Kevin Kirk

Kali Linux

Copyright © 2023 by Kevin Kirk

All rights reserved. No part of this publication may be reproduced, stored or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise without written permission from the publisher. It is illegal to copy this book, post it to a website, or distribute it by any other means without permission.

First edition

This book was professionally typeset on Reedsy
Find out more at reedsy.com

Contents

Kali Linux

Introduction

Chapter 1: Introduction to Kali Linux

Chapter 2: The Fundamentals of Kali Linux

Why You Should Use Kali Linux

Chapter 3: The Hacking Process

Chapter 4: Hacking Wireless Networks

Chapter 5: Kali Linux Uses and Applications

Chapter 6: Introduction to Cybersecurity

Chapter 7: Network Management and Scanning

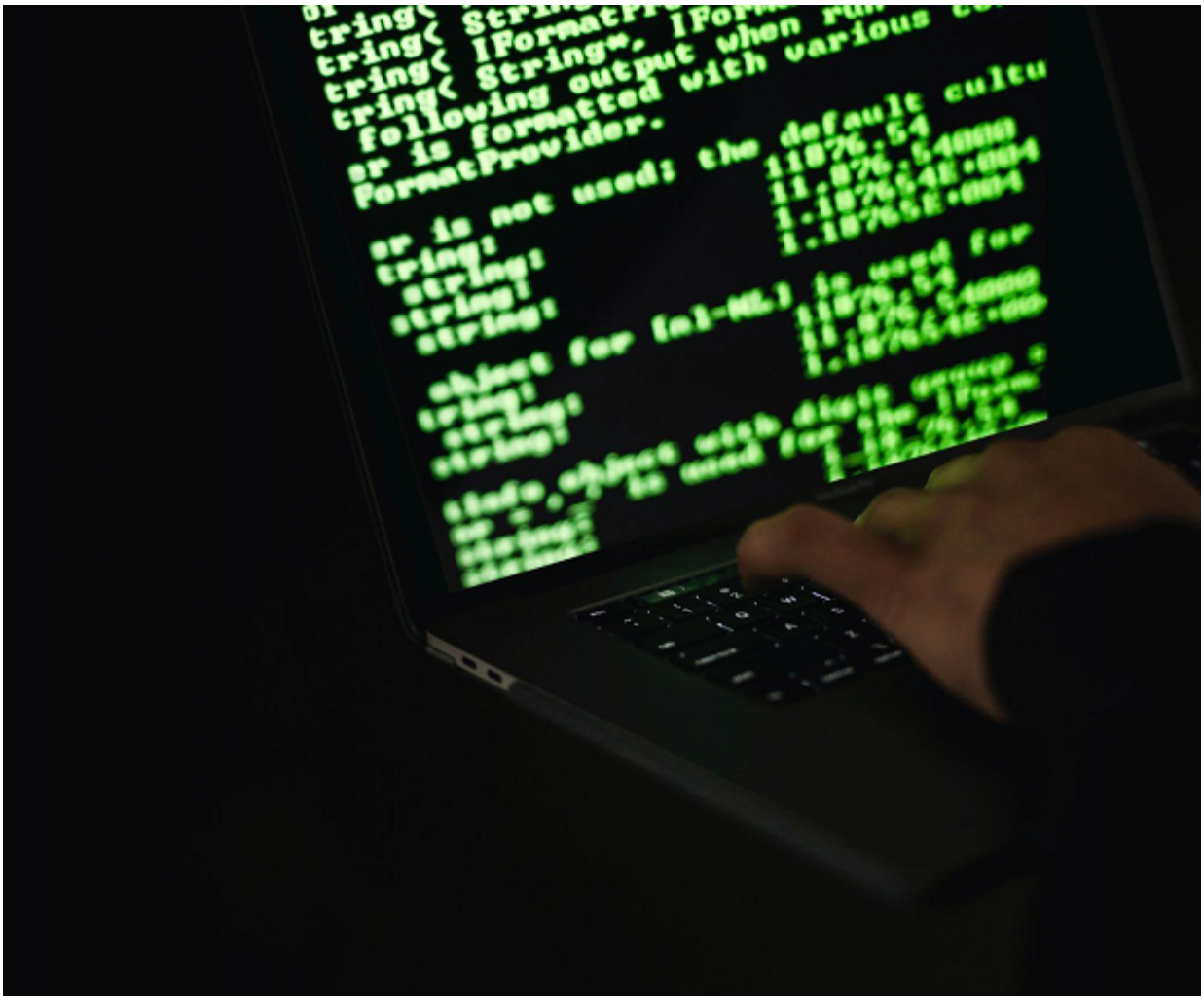
Chapter 8: Web Security

Conclusion

Kali Linux

The Basics of Cybersecurity and Ethical Computer Hacking:

A Complete Step-by-Step Beginner's Guide, Including Wireless Penetration Testing Tools to Secure Your Network



Introduction

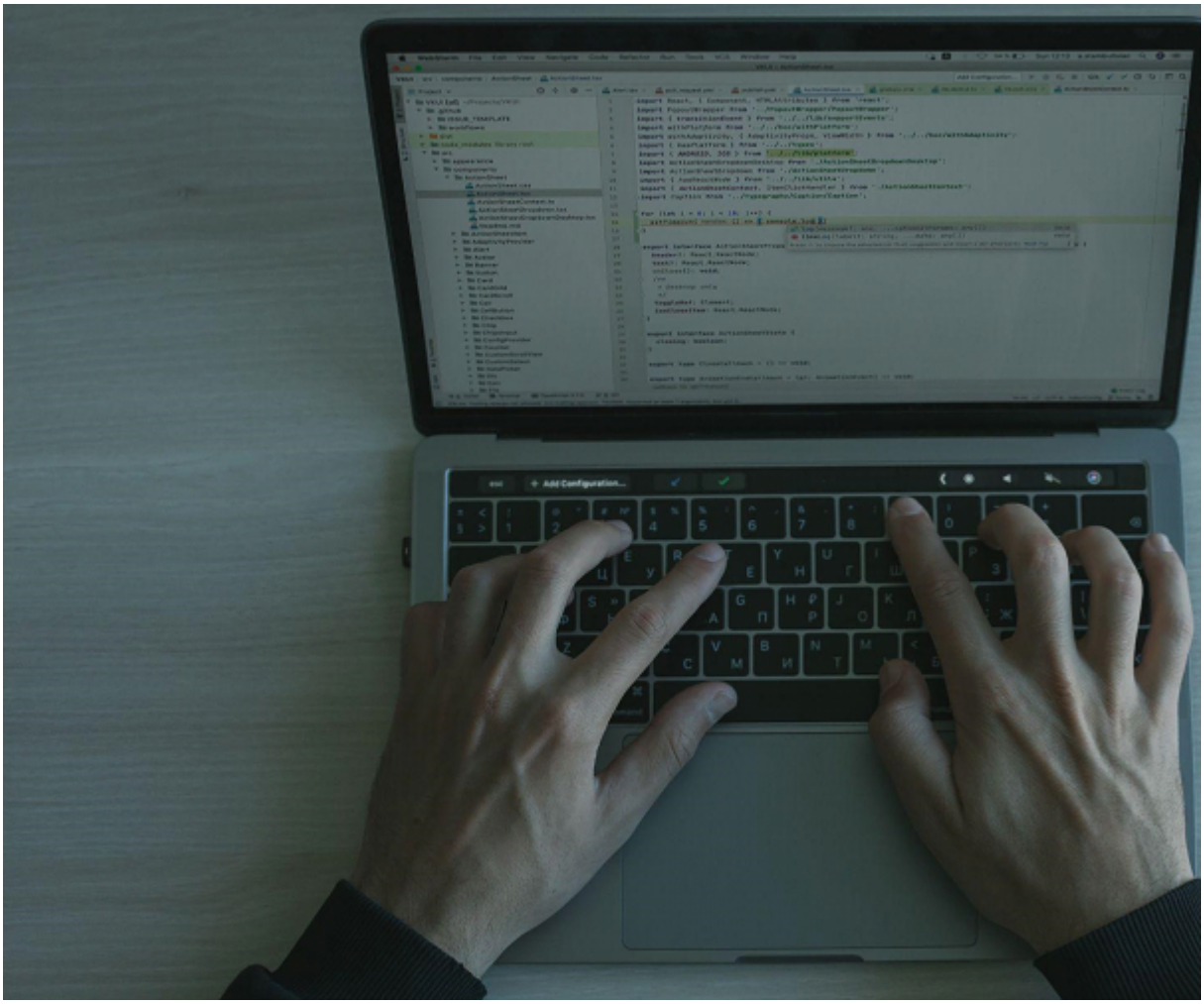
We sincerely appreciate your decision to buy Kali Linux: A Comprehensive Step-by-Step Beginner's Guide to Learn the Basics of Cybersecurity and Ethical Computer Hacking, Including Wireless Penetration Testing Tools to Secure Your Network. The book discusses all of the tools available in Kali Linux for conducting penetration tests. Additionally, you will be able to discover how the various utilities in this Debian installation work. You will need at least a basic understanding of command utilities, computer networking, and Linux administration in order to use this book effectively. This will make it easier for you to understand the range of topics addressed here.

You will learn how hackers sneak into your systems and the techniques they employ to steal information. you will learn the defenses necessary to defend against the various hacking strategies. In order to accomplish this, the books cover a variety of subjects, such as an introduction to Kali Linux, the basics of Kali Linux, the hacking process, wireless network hacking, uses and applications of Kali Linux, an introduction to cybersecurity, network scanning and management, and some fundamentals of web security that you will need to understand on your path to becoming a professional hacker.

You will have mastered both theoretical and practical principles on the fundamental hacking techniques by the time you turn the final page of this book. You will be equipped with the methods required for breaking into computer systems, applications, and networks. Let me remark that even

though we have several books that cover this subject, you choose to read this one.

I’m grateful for that. Every effort has been made to make the information in this book useful and enlightening for you. Enjoy your reading!



Chapter 1: Introduction to Kali Linux

You will learn about a variety of ethical penetration testing topics in this chapter. It is also known as ethical hacking, and it is described as a technical process and approach that provides professional hackers with a platform to model the methods and techniques that actual hackers would use to exploit an information system or computer network. We will discover the procedures that a penetration tester typically follows, starting with the comprehension and evaluation of a particular target and ending with the actual break-in.

The book also addresses issues related to the various tools employed in the penetration testing process. These are introduced in this chapter, but Chapter 4 will go into further detail.

Along with learning how to download and install Kali Linux, the reader will also gain an understanding of the real-world applications of this Linux distribution. So without further ado, let's start.

Offensive Security is the firm that created the excellent distribution known as Kali Linux.

The latest offering from the company is Kali Linux. Over 300 security and penetration testing tools may be found in Kali, a live disk security distribution. If you're familiar with the operating system, you might have observed that the tools have been divided into groups that penetration testers and other organizations that evaluate information systems frequently use. In contrast to past editions made available by Offensive Security, Kali Linux uses the Debian 7.0 distribution as its foundation.

The operating system shares a family tree with Backtrack Linux, which it replaced. It is important to note that the same team also supports it.

According to Offensive the name change to Kali Linux implies that this operating system is a complete rebuild of the Backtrack version. The significant upgrades made meant that it wasn't just a new version of Backtrack but an entirely new operating system. If you think back, you will recall that Backtrack was an upgrade that came from White Hat and SLAX, also known as WHAX and Auditor, just like Kali.

Technically speaking, Kali is the most recent iteration of the tools used for penetration and auditing assessments in the information security sector.

Tools available in different categories in Kali Linux

Kali Linux is preloaded with a variety of tools that can be used for penetration testing. The tools in Kali Linux are grouped in a way that facilitates the penetration testing exercise, as we have previously stated.

The basic categories are listed below:

1) Information-gathering tools:

This category includes a variety of tools used in the information-gathering process. A penetration tester is typically curious about knowledge of DNS, operating systems, IDS/IPS, SSL, network scanning, routing, voice over IP, SMB, email addresses, VPNs, and SNMP.

2) Tools for vulnerability assessment:

These are tools that are located here and are generally used to scan for vulnerabilities. We have tools that are used to evaluate the Cisco network and database servers for vulnerabilities. We also offer a number of fuzzing tools under this heading.

3) Web

As implied by the category's name, these tools are related to web apps. They consist of web crawlers, web application proxies, content management system scanners, database exploitation, and scanners for web vulnerabilities.

4) Tools for password attacks:

This category includes tools that can be used to conduct both online and offline password attacks.

5) Exploitation tools:

These are tools for exploiting the flaws discovered in a particular target environment.

You may find exploitation tools for databases, the Web, and networks here. Additionally, you can find tools for launching social engineering assaults in this area. The user will receive information from the tools about the exploits that were used as well

6) Sniffing and spoofing

These tools are used to snoop on network and web traffic. Additionally, we offer network spoofing tools like Yersinia and Ettercap.

7) Access-maintenance tools:

A penetration tester will utilize the tools listed below to keep access to a target computer. It goes without saying that you need the highest degree of privilege to install the tools in this category. We have tools that can be used to backdoor OS systems and online apps. This category includes tunneling equipment as well.

8) Reporting Tools:

This category includes tools for recording the penetration testing technique, as well as the outcomes and recommendations.

9) System services:

This category includes a wide range of services that are required for the penetration testing operation. The Metasploit service, Apache service, SSH service, and MySQL service are a few examples.

10) Wireless attacks:

This section contains techniques for attacking Bluetooth, RFID, and wireless devices.

11) Reverse engineering:

This category of tools is typically used for troubleshooting software or performing executable file disassembly.

12) Stress testing:

You can discover all the necessary tools in this category to perform stress tests on your network, VOIP environment, wireless network, and Web.

13) Hardware hacking:

This page has all the tools you need to work with Arduino and Android applications.

14) Forensics:

This category includes many tools that are typically used in digital forensics. The acquisition of hard disk images, file carving, and—most significantly—the analysis of the image extracted from the hard disk are examples of forensics. A user must choose the No Drives or Swap Mount option from the booting menu in Kali Linux Forensics in order to do these procedures correctly. In this manner, the operating system won't mount the drives automatically. This suggests that the drive's integrity will be preserved.

Keep this knowledge in mind since Chapter 5 will examine some of it.

The Penetration Testing Lifecycle There are several different lifecycle models for penetration testing that are utilized today. The methodology and lifespan outlined and used by the EC-Council Certified Ethical Hacker program are currently the ones that are most popular. The five phases of the penetration testing life cycle include reconnaissance, scanning, gaining access, maintaining access, and covering tracks, in that order.

We shall examine each of the aforementioned stages in more detail later on in the book.

General Penetration Testing Framework As we have previously stated, Kali Linux's extensive toolset gives us the adaptability we require for penetration testing and security assessment. Without a good framework, a penetration tester is more likely to receive unsatisfying results from failed testing. As a result, it is crucial for managers and technical administrators to make sure that security testing is in line with a defined framework because the test's objective is to produce valuable discoveries.

This article will teach you a general testing framework that both the white box and black box methodologies typically

You will learn the fundamentals of the normal steps that a penetration tester or security auditor should take from it. However, the frameworks must be suitably modified based on the objective being evaluated. The following actions must be taken in order for the assessment process to be successful.

Target scoping Information gathering Target discovery Target enumeration Target mapping out Vulnerabilities Social engineering Target exploitation Privilege escalation Access maintenance Reporting and documentation 1. Prior to starting the technical examination of the security, the target is often scoped. In order to fully comprehend the scope, observations must be made on the target network environment. Additionally, the auditor may be given a specific group of entities or a single entity to establish the scope for.

Typical decisions that are typically made in this step include things like:

- What element needs testing?
- How will the testing be done?
- What are the criteria that will be used when the test is run?
- What are the constraints on the testing procedure?
- How much time will the exam take?
- What goals are meant to be attained?

Any successful penetration testing exercise requires the tester to have a solid grasp of the technology being tested, its fundamental workings, and how it interacts with the network environment.

1. This means that the effectiveness of the penetration testing process depends on the auditor's knowledge.

2. Information collecting The reconnaissance step comes after scoping is complete. In this case, the penetration tester will use freely accessible sites to learn more about their target.

Social networks, articles, forums, blogs, bulletin boards, business or non-commercial websites, newsgroups, and search engines like MSN

Bing, and Google are just a few of the online resources one can use to find relevant information.

Kali Linux also comes with a number of tools that you can employ to get network information about a target. The programs collect data from DNS servers, email addresses, traceroutes, phone numbers, the Whois database, personal information, and user accounts using essential data mining techniques. The more data that is acquired, the higher the likelihood that a penetration test would succeed.

3. Target discovery critical actions include determining the network state of chosen targets, their operating system, and, if practical, their network architecture. Such details provide a penetration tester with a thorough understanding of the network's connected devices or cutting-edge technologies. As a result, they will be able to list all of the various services that are now active within the network. Using the Kali Linux advanced network tools, it is feasible to perform all of these tasks (identifying the live hosts on the network, identifying the OS that each host is running, and characterizing each host according to their functions in the network system). These instruments might use active detection methods or passive detection methods. This is carried out on top of network protocols and is manipulatable to produce meaningful data. The OS fingerprinting is an illustration of this information.

4. Finding open ports on the systems being targeted at this part of the process, or "target enumeration," boosts earlier efforts. Following the detection of open ports, the ports used by active services will be listed.

A hacker or penetration tester can help by using port scanning techniques including stealth, full-open, and half-open scan to check the visibility of ports. For hosts protected by a firewall or an intrusion

detection system, this is conceivable. An examination of the services that are mapped to the open ports can be carried out to assist penetration testers or hackers in finding existing vulnerabilities in the infrastructure of a target network. This indicates that we can use target enumeration as a base to find vulnerabilities in the various network devices. One can enter the network through the vulnerabilities. Target enumeration can be carried out by a security auditor using Kali Linux's automated tools.

5. Vulnerability mapping At this point, we should have sufficient knowledge on the target network.

On the basis of the services and ports we have identified, we must now examine the vulnerabilities that have been found. We may accomplish the goals of this phase with the help of Kali Linux's automated vulnerability assessment tools for networks and apps. Manual vulnerability mapping is an additional option. The main drawback is that it takes a lot of time and requires specialized knowledge. The best strategy is to mix the two so that a security auditor may have a clear understanding that will allow them to look into network system vulnerabilities that are either known or undiscovered.

6. Social engineering is a sort of attack that employs people as its attack vectors. Humans are typically seen as the weak point in information security configurations—the gateway via which an attacker can access a system. A target network can be breached by an attacker, who can then run malicious code to do harm and, occasionally, open a backdoor for later use. All of this will have been made feasible by tricking the administrators or users of a certain network. There are many distinct types of social engineering.

For instance, a phone-based attacker may impersonate a network administrator to ask a user for their account information.

Email phishing scams are another type of social engineering that malevolent users use to acquire your bank account information.

A person can physically impersonate a legitimate user to enter a physical space. Also social engineering. These illustrations demonstrate the vast possibilities for reaching a necessary objective. Understanding the human psychology is a talent that will enable the tester or attacker to improvise appropriately in their targeting, which is essential for the success of any penetration testing activity. Because most nations have rules governing this, it is important to be aware of them before taking any action lest you land in jail.

7. Target exploitation Using the many forms of exploits that are readily available, we can attack our target after studying the vulnerabilities we have discovered. To guarantee that existing exploits function as planned, tweaks or further research are frequently required.

Of course, the task is intimidating. However, Kali Linux already includes cutting-edge exploitation tools that can make the process easier. Additionally, a tester is free to use client-side exploitation techniques in addition to a small bit of social engineering to provide them access to a target system. By now, a discerning reader should be able to notice that this phase focuses more on the target acquisition process. Target exploitation includes three main categories. These are the three stages of exploitation: pre-, exploitation, and post-.

8. Privilege escalation The penetration experiment will be considered successful once the target has been acquired. Depending on their access rights, the penetration tester or auditor will now be allowed to go throughout the system. A tester is able to elevate these privileges by using

local exploits that are compatible with the system's environment. A hacker or penetration tester will now be able to obtain system-level or super-user capabilities after these exploits are used. A tester can now launch further assaults on the computers connected to the local network. This technique can be either non-restricted or restricted depending on a target's scope. Cracking passwords to various services, observing network traffic, and using spoofing techniques on local networks are other ways to learn more about a compromised target. This suggests that obtaining the highest level of access to the targeted system is the primary goal of privilege escalation.

9. Access preservation In some cases, a client may ask a penetration tester to continue having access to the system for a predetermined amount of time. This can be used to demonstrate to network administrators how unauthorized access to the system can be accomplished without the need for further penetration methods. Additionally, it helps to reduce the amount of time, money, and resources needed to get access to the system in order to evaluate its security. One can select to use end-to-end connection methods, proxy protocols, or hidden tunneling techniques. By doing so, a tester can build backdoor access that will help them stay present in a target system for however long is necessary. This method of entering the system shows us how an attacker might remain present in a targeted system without drawing attention to themselves.

10. Reporting and Documentation Without presenting the vulnerabilities that were discovered during the penetration test, the exercise is not complete. Vulnerabilities that have been verified and exploited ought to be adequately reported, displayed, and documented.

This is essential ethically since it will enable network and system managers and administrators to focus their resources on plugging any security gaps in their infrastructure.

Depending on the requirements of the various contracting organizations, the reports will have varying perspectives. Technical personnel and enterprises will be able to identify and analyze any weak places in their IT infrastructure with the help of the customized report. Additionally, the reports can be utilized to compare a target system's integrity before and after the infiltration process.

Let's take a look at the ethics We have rules of engagement to make sure that everything remains lawful. The auditors and other information security experts must abide by these.

These guidelines specify how penetration testing should be provided, how testing is to be carried out, how legal negotiations and contracts should be determined, how to define the testing scope, how to prepare a test plan, how the test should proceed, and how to manage a consistent reporting structure. Each of these topics has to be carefully examined. Throughout the duration of the engagement, official procedures and practices need to be followed.

These guidelines comprise the following, without being exhaustive:

1. It is important to choose a test schedule that won't interfere with or disrupt a business' regular operations. It is wise to plan ahead and not include the regular working hours.

2. The procedures that must be followed during the testing exercise are outlined in the rules governing the test process. The managers and technicians of the organization contribute to the creation of these

regulations in order to limit the testing procedure with its inhabitants and surroundings.

3. It is prohibited to offer testing services to a client after breaking into their systems without first creating a legal agreement. This is similar to unethical marketing, and depending on the norms and laws of the country, it may result in the collapse of regular business operations and painful legal implications.

4. Without the express consent of the customer, it is completely forbidden to conduct a penetration test outside of its intended parameters or outside of any other restrictions.

5. The parties concerned should agree on a legally enforceable contract that limits the liability of work until there is proof of illegal activity. The details of the test technique, the emergency contacts, the job description, and any potential conflicts of interest must all be stated in plain detail.

6. The contractual entities and any limitations placed on them during the process should be explicitly identified in the penetration test's scope.

7. Reports and results must be presented in a consistent and understandable manner once the testing is complete. All known and unknowledgeable vulnerabilities should be covered. Additionally, it must be supplied in confidence to only approved persons.

Terminologies We will come across words that are frequently used in the penetration testing industry in this book. We need a working definition of the terms because members, technicians, and professionals all have

various perspectives on how they are used in their respective fields. The terms we'll be utilizing are listed below along with their definitions.

Penetration according to our definition, is the methodology, process, and procedures used to try to get beyond an information system's built-in security measures and other safeguards. Normally, the entire procedure adheres to predetermined rules. Examining a system's administrative, technical, and operational settings and controls is the focus of penetration testing. A specific information system's security is evaluated during testing exactly as it is set up. It's possible that the targeted network's system administrators and workers are unaware that such an exercise is taking place.

Performing an assault on computer or network systems for a company or a specific owner of the information system is the primary responsibility of an ethical hacker, a professional penetration tester. You'll see that the terms "ethical hacking" and "penetration testing" are used interchangeably in this book.

White Hat This phrase refers to a computer security expert or an ethical hacker who specializes in the security testing of information systems in order to either improve or add security where it is needed.

A person who uses their IT expertise to circumvent the security of information systems without authorization is referred to as a "black hat" in this parlance. Black hats typically intend to commit computer crimes. Members of the Red Team and penetration testers frequently use Black Hat techniques in their job. This is done in security testing to imitate hostile individuals performing valid tests or activities.

Grey Hat In life, there are good guys, bad guys, and people who fall in the middle. Grey hats represent the midway ground in hacking. In most circumstances, they will attempt to bypass the security measures of an information system without authorization. They typically do this to alert the system administrators to any holes they have found. They often are not in it for the money. They are illegal since they don't ask permission from the owners first before engaging in their operations.

Vulnerability Assessment/Analysis

This activity is used to assess a system's security settings. The types of evaluations that can be done include assessing the security patches that have been installed on a system and the ones that are missing. Vulnerability assessment teams can either be external or internal to an organization's IT department.

Malicious User Testing

In this case, the assessor will behave maliciously as though they were an insider. Of course, their insider status makes them a reliable source.

The assessor will be provided with authentic login information belonging to an authorized user; this will be a test account. They will then use the credentials to try to go beyond security measures that have been put in place. They can achieve this by altering settings that shouldn't be altered, viewing settings and documents that the account isn't allowed to view, and elevating their permissions and privileges over what the test account ought to have. In conclusion, a malicious user test tries to mimic

the activities that an untrustworthy insider could perform using their trusted credentials.

Phishing In this kind of attack, efforts are made to persuade the targets to divulge private data such as passwords, account numbers, and user names. Typically, fraudulent emails with authentic-looking subject lines are used to do this. The emails may come from companies, banks, or customer service representatives. Users are encouraged to click on bogus hyperlinks in a different kind of phishing assault. By doing this, harmful software could be secretly installed on the target system without the owner's awareness. Following this, the malware can be used to target other computers or to steal data that is stored on them. Phishing assaults are by their very nature non-targeted. Targets can include everyone on a mailing list or those whose email addresses have a particular extension, such as "@kali.com."

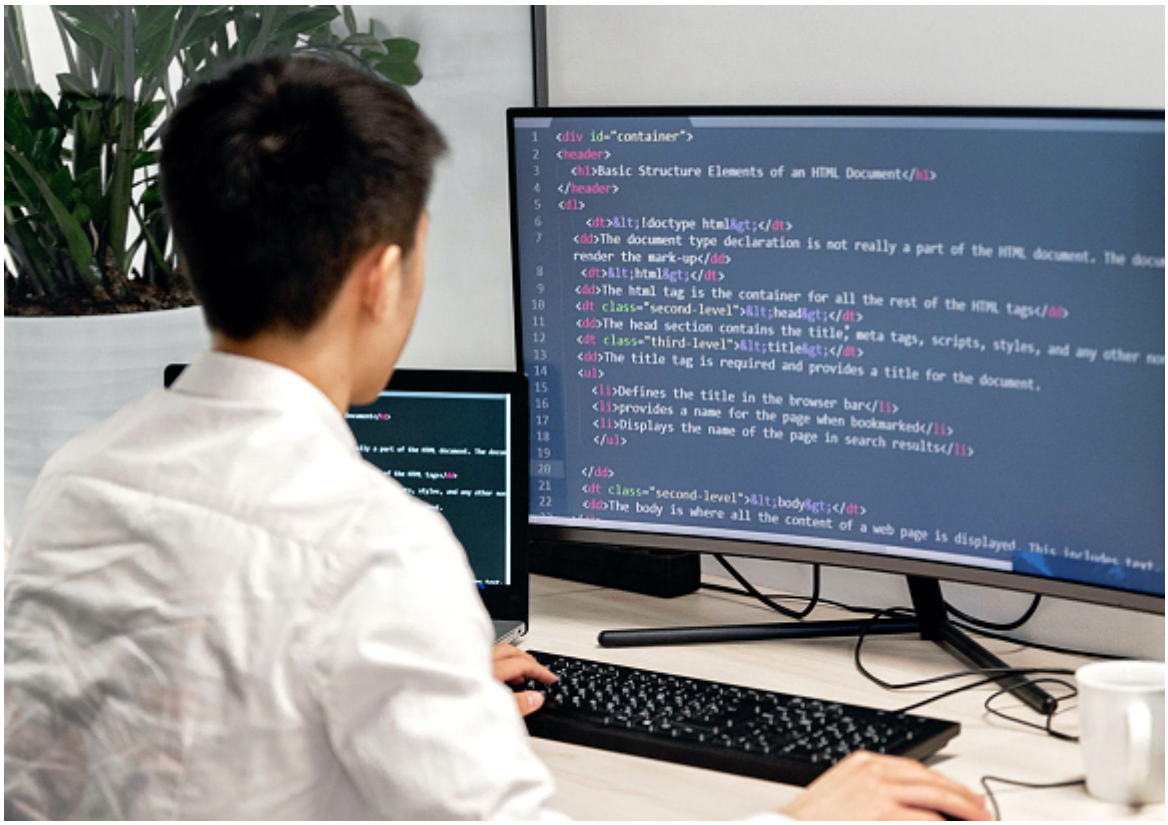
Spear phishing is a kind of phishing attempt in which the targets are narrowly defined. For instance, an attacker could conduct reconnaissance to find the email addresses of an organization's top executives. The phishing assault can now be launched specifically against these people.

Container diving

Using this method, the penetration tester will try to search through a system's trash. Any user, as well as the system administrators, could be the source of this garbage. Any knowledge gleaned from this will be very beneficial in comprehending a certain target. Information describing network diagrams, system settings and configurations, the hardware components, and the software versions that are being used might be found by a penetration tester. On a good day, one might even obtain user

credentials, including user names and passwords. The act of entering a large trash bin is referred to as “dumpling.” Additionally, little workplace trash cans frequently contain valuable information.

The words “LiveOS,” “Live Disk,” and “Live CD” are all used to describe an optical disk that contains an entire operating system. Live disks are a valuable tool for penetration testers and assessors since they may be tailored to the situation at hand. They can be customized to have particular settings, resources, and software elements. Even though there have been several Microsoft Windows versions developed over the years, the majority of live CDs in distributions are typically Linux-based. In the majority of assessments, an assessor merely has to deliver a live disk. The systems being evaluated can be booted directly to the live disk, essentially using the resources of the information systems against the system itself.



Chapter 2: The Fundamentals of Kali Linux

Obtaining Kali

As we mentioned in the introduction, Kali Linux is a Linux distribution that is available for download as an ISO file. You'll have to download it from a different computer, then you'll need to create a disk and install it from there. Download this intriguing Linux distro by visiting http://www.kali.org/downloads/. You may find the documentation for setups, sophisticated operations, and special cases on http://www.kali.org/official-docs/ to learn how to install it. We have a vibrant community where you may ask any questions or offer assistance to other people in need if you require any more aid. These community boards are controlled by Offensive Security, and new users must register in order to access them.

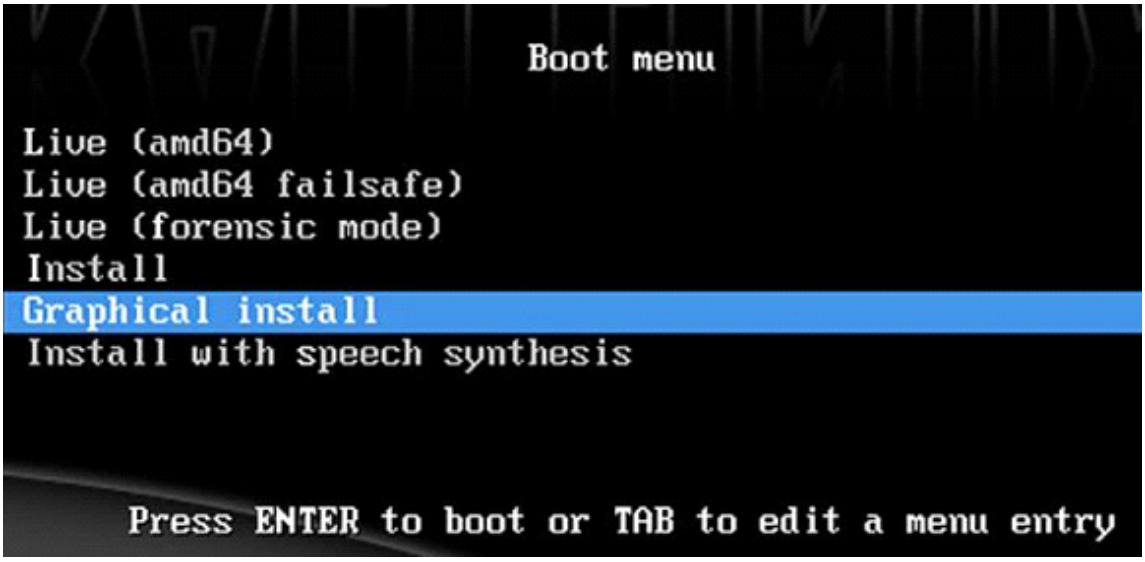
The Kali Linux developers are the security firm. about the occasion, Offensive Security will send out messages with information about their products, community news, and upgrades. Make careful to choose the appropriate architecture for your machine (either amd64564-bit or i386532-bit) when downloading Kali Linux. Since the knowledge of Kali Linux images is adequately covered in the resources I've supplied, I won't discuss them in this book. To pick and download the image, click on the appropriate link. If you're using Microsoft Windows, you'll need to burn the image using Burn ISO or another program (Ruxus comes to mind). Burning should continue until it is finished. Similar to Windows users, Linux users can convert the ISO image using a disk-burning program (like K3b).

Kali Linux installation on a hard drive

You will discover how to install this operating system both graphically and textually. The graphical user interface has been made as uncomplicated as feasible. You must set up your Basic Input Output System (BIOS) so that it can boot from the produced optical disk. Start by inserting Kali's optical disk or flash drive into the PC. There is the possibility for sophisticated users to employ virtualization software like Oracle's VirtualBox or VMware's Player.

Kali Linux booting for the first time

The PC in the screenshot below has successfully booted from the Kali Linux disk. In this book, 64-Bit Kali Linux 1.0.5 has been utilized. You will eventually notice that Kali Linux versions downloaded at various periods will appear slightly different from one another. Apart from that, graphical installs are comparable.



You may access the most recent guidelines for all Kali Linux releases at http://www.kali.org/. As a result, it's crucial to visit this website before

performing an installation. In addition to being installed on a computer's hard drive, Kali Linux can also be launched directly from the disk containing the converted image. A live CD is what we refer to as this.

The operating system can now boot thanks to this. The Kali tools will also be put to use. The only thing to keep in mind is that the live CD's operating system is not permanent. By using this word, it is meant that any memory, documents, saved settings, and any other important research or work are likely to be lost when the computer is turned off. Running Kali Linux in a nonpersistent state is an excellent approach to learning how to use it. Your present operating system won't be impacted in any way either. You can see that we have a Speech Synthesis installation option. We won't get into the finer points of that, but you should be aware that it is a recent upgrade feature for Kali and the Debian operating system. If their hardware can enable speech synthesis, users can voice-control the installation process. How thrilling! As I've already indicated, let's focus on the graphical installation for the time being. Scroll to and select Graphical Install using the directional keys, then press the Enter key.

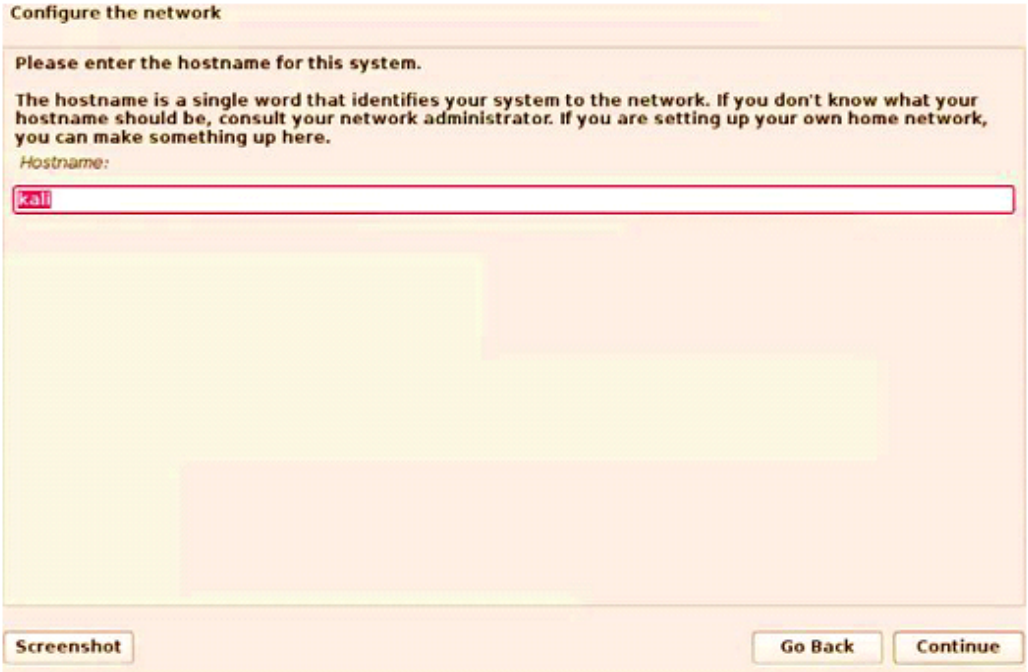
Defaults are being set

The following few panels will ask you to choose default options for your region, keyboard layout, and language. Click continue to move on to the next stage after making the necessary selections. As the machine starts the real Kali installation, you will see numerous progress bars on the screen throughout the process. For the majority of selection displays, selecting the default options is a wise move.

Setup of the Initial Network

See the picture below. You must perform a fundamental configuration and initial setup of your main network interface card at this point. Choosing a hostname. Enter this information easily by typing in the box provided, then click the continue button to move on. To prevent several machines on the same network with the same hostname, choose a unique hostname.

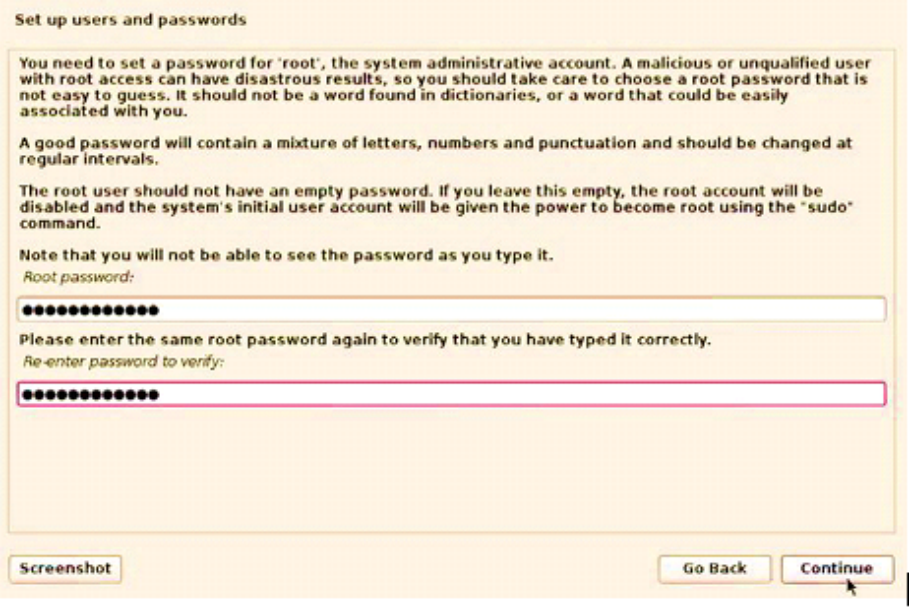
This will lessen networking-related issues. Click the Continue button to continue after deciding on a hostname. You must provide an FQDN, or fully qualified domain name, on the following screen. Unless you want to join a domain environment, this is not required for the majority of lab environments. Let's leave it empty for the moment. To continue, we will click the Continue option.



Configuring Passwords

The following screen will ask you for a root-level password. The default password in Kali Linux is too. I advise you to come up with a new password that is difficult to guess, strong, and untraceable to the user. Tap the Continue button after entering the password twice to go to the next step.

Do you still accompany me? Now let's set the system clock.



setting up the system clock

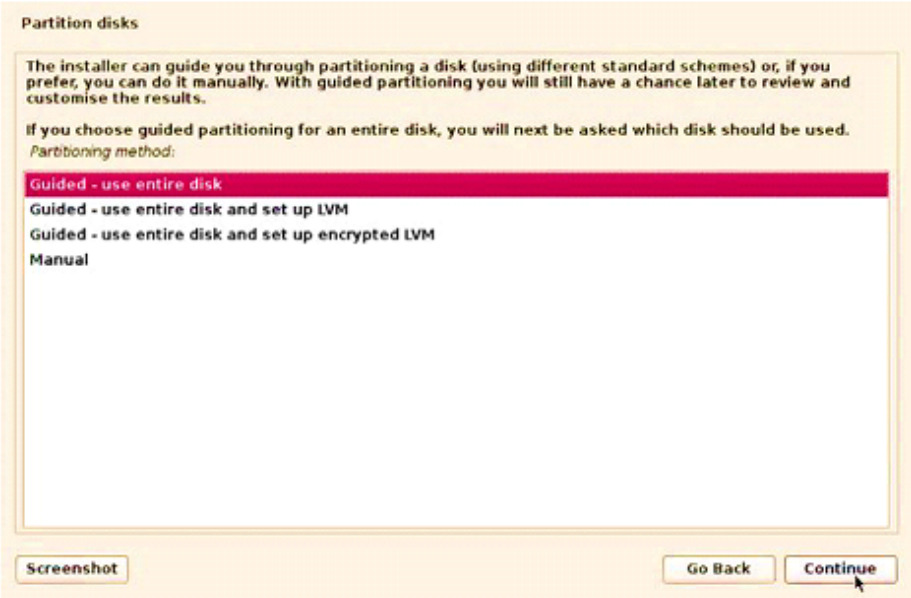
In the manner seen in the image below, you will be asked to choose a time zone. To move on to the next installation phase, choose the relevant selection and then click the Continue button.

Configuration of the clock.

Disk Partitioning

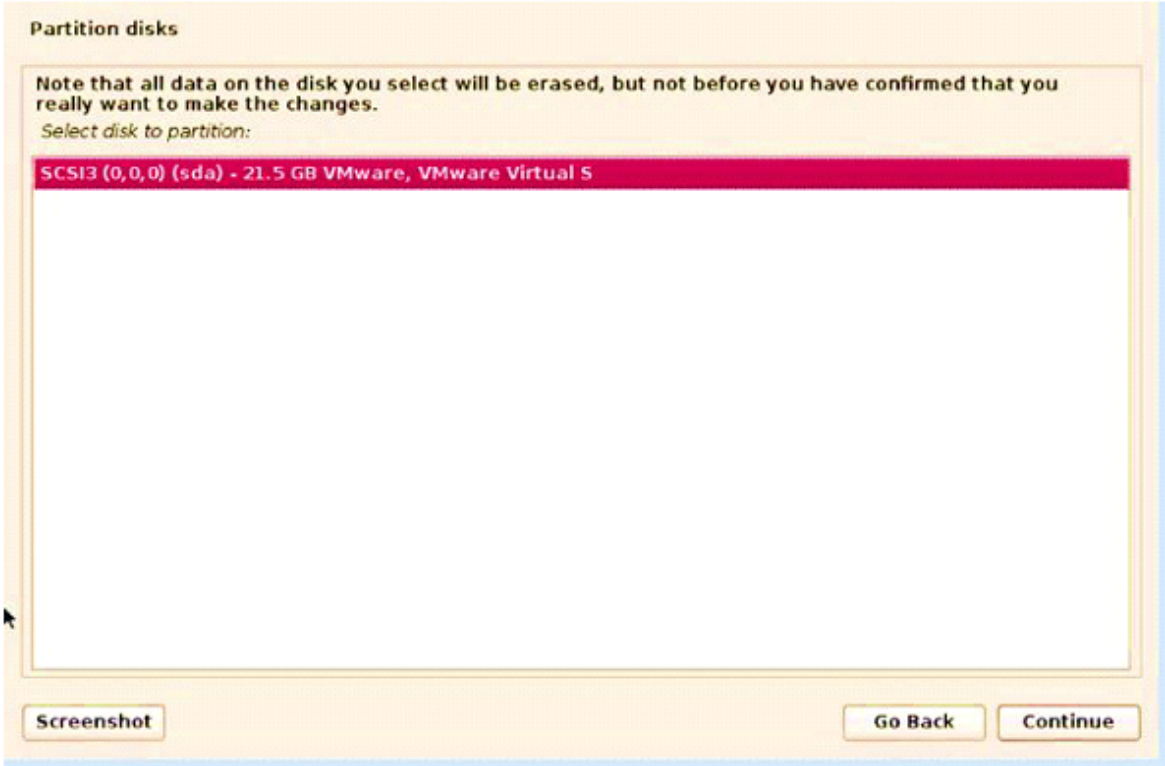
We can build up a Linux OS in a number of different ways by configuring partitions. The most fundamental installation, Guided Partitioning, is what we'll concentrate on. The settings that are typically highlighted by default are shown in the figures below. Up until the partition disks - 5 figure, nothing needs to be selected. Simply keep clicking the proceed button until partitioning is finished. Allow me to take a moment to explain what occurs at each stage of the installation wizard.

The several options you have for partitioning your computer's hard disks during installation are listed below.



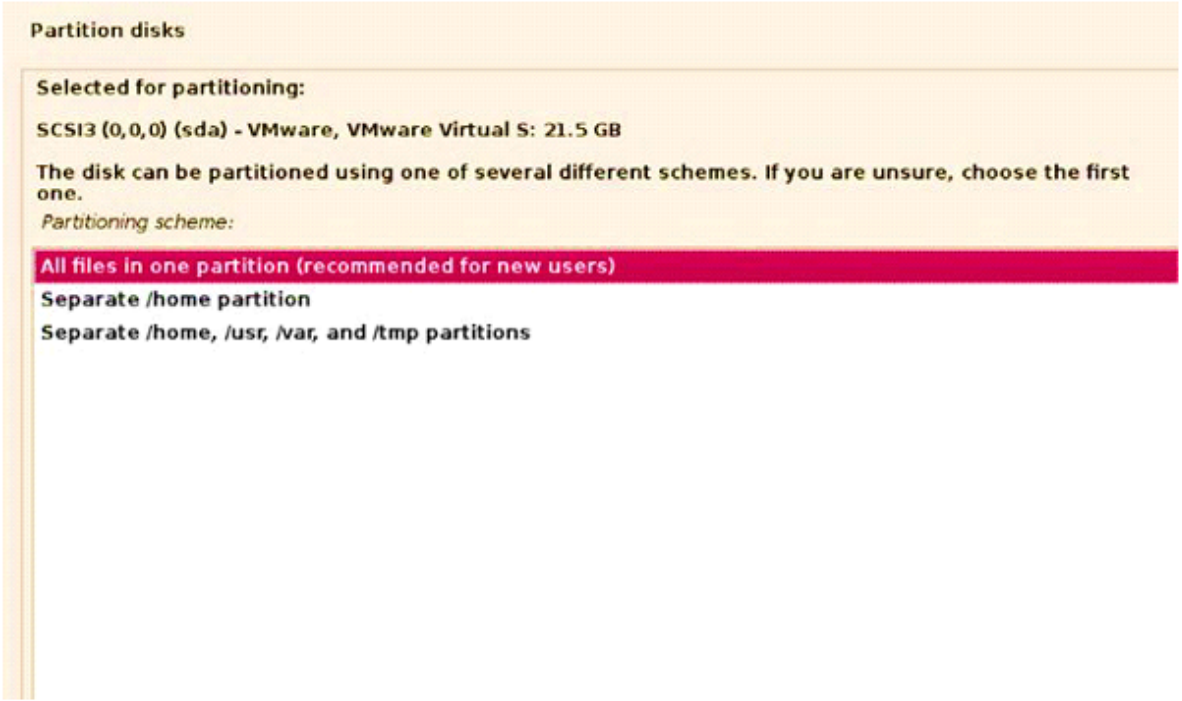
Partition disks - 2.

Choose "All files in one partition (recommended for new users)" if you are a new Kali Linux user. The greatest choice for you is this. To continue with the installation, click the Continue button.



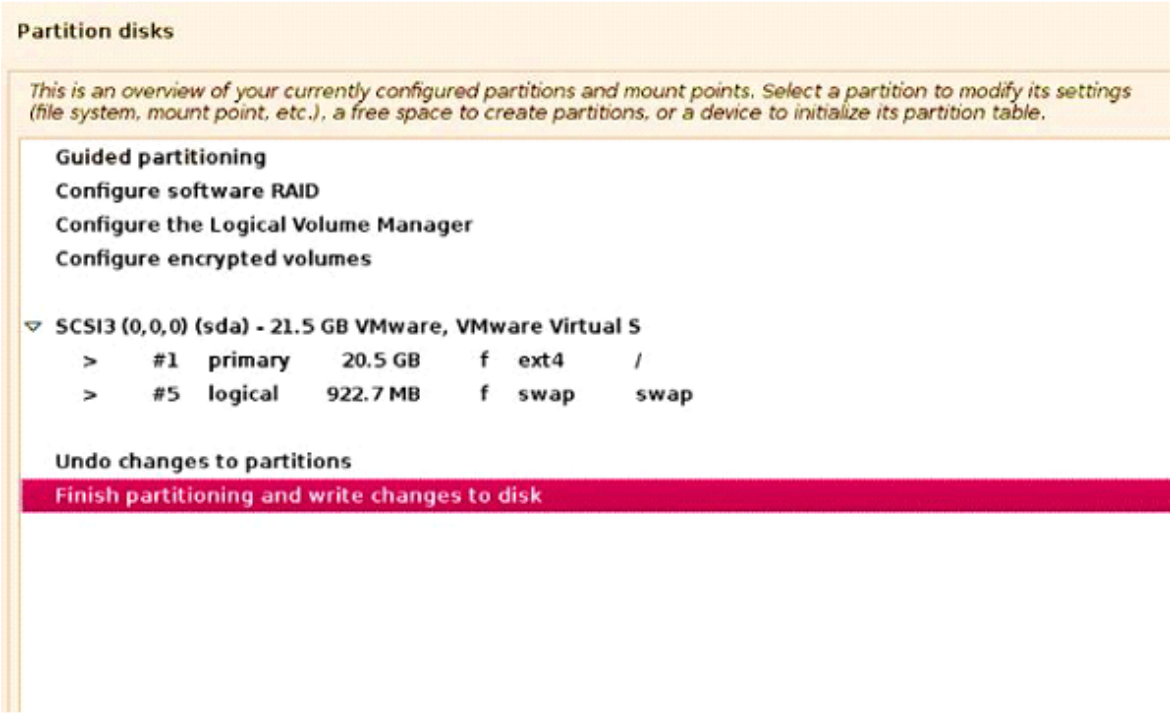
Partition disks - 2.

Choose “All files in one partition (recommended for new users)” if you are a new Kali Linux user. The greatest choice for you is this. To continue with the installation, click the Continue button.



Partition disks - 3.

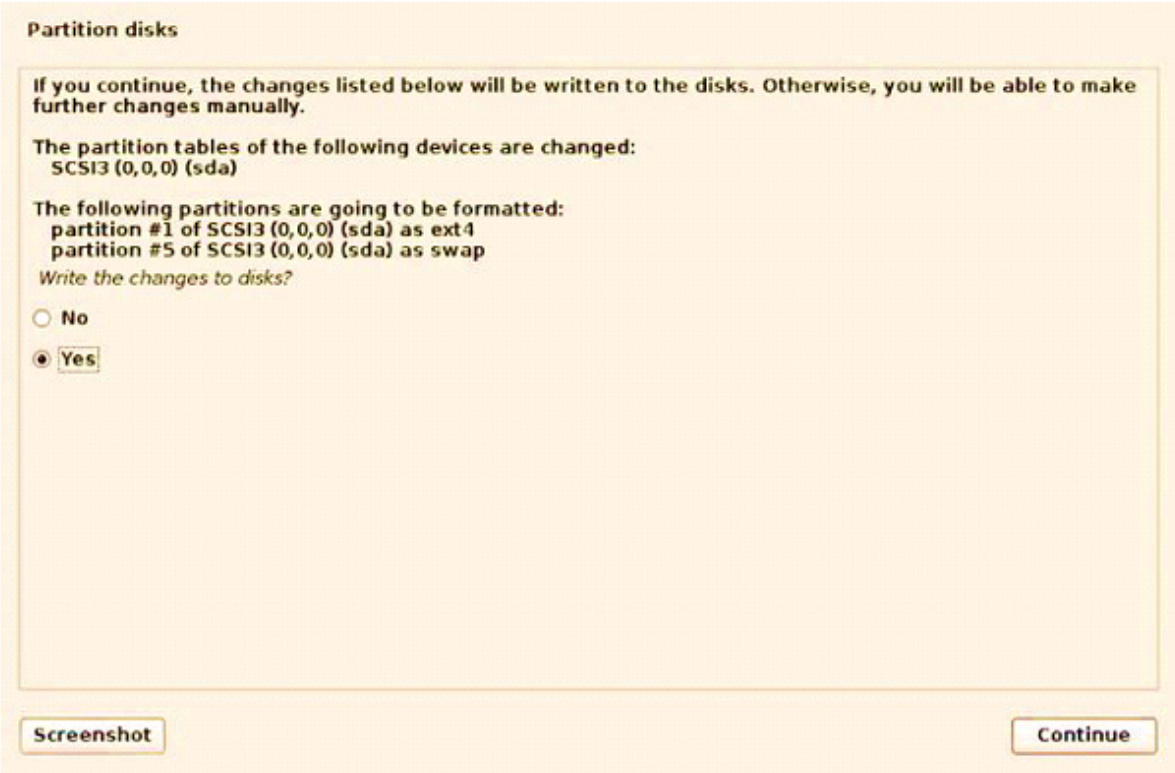
To continue the installation, keep pressing the continue button



Partition disks - 4.

After guiding you through the aforementioned stages, the wizard will provide you a screen for your evaluation. The primary partition will now be formed as a single partition and contain all of the system, scripting, and user data. For swap space, a second partition will be created. This system's virtual memory is used to page files to and from the central processing unit and random-access memory of the computer. All Linux-powered computers are advised to have swap space. The swap area is typically set up to be 1.5 times, if not exactly, the amount of installed physical random-access memory (RAM) for the machine.

You'll arrive at a screen that looks like this.



Partition disks - 5.

In the graphic above, you will be prompted to "Finish partitioning and write changes to disk." To start the installation procedure, select Yes and

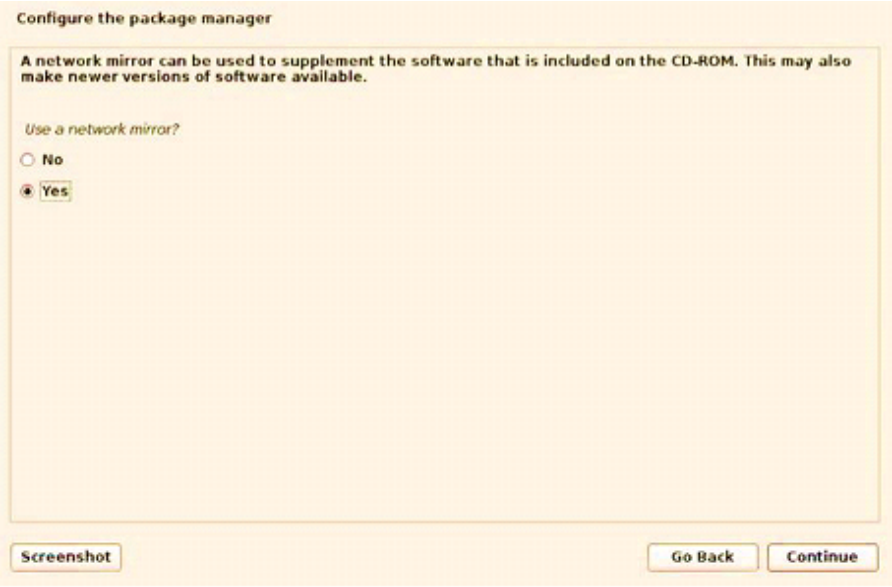
press the Continue button. Be aware that this will be your final opportunity to review your partitioning choices before the operating system is installed on the hard drive. It is still feasible to change the partition's sizes if the necessity arises in the future. However, if the partition sizes are changed improperly, your operating system could be completely destroyed.

After you click proceed (at the figure at partition disks - 5), the installation and partitioning of the hard drive will start. Depending on the hardware in your computer, the installation could take an hour or perhaps a few minutes.

Putting the package manager together

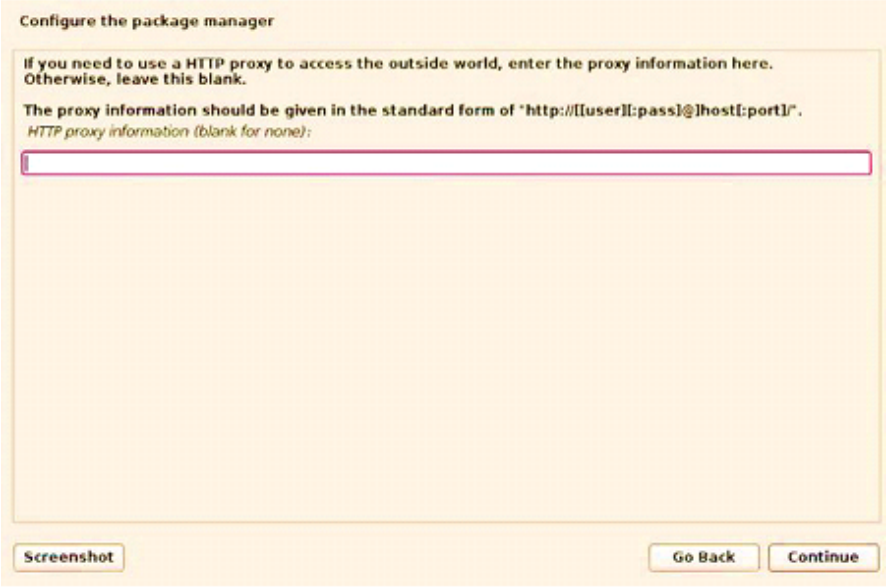
Your operating system will get its security updates and fixes from this update repository. The package manager is therefore crucial to the operation of the operating system.

The network mirror that is included with the Kali Linux image can be used. Since it includes the most recent package management sources, using it is advised. You will automatically select the "YES" option, as illustrated in the figure below. By selecting the Continue option, continue with the installation.



Configuration of the package manager.

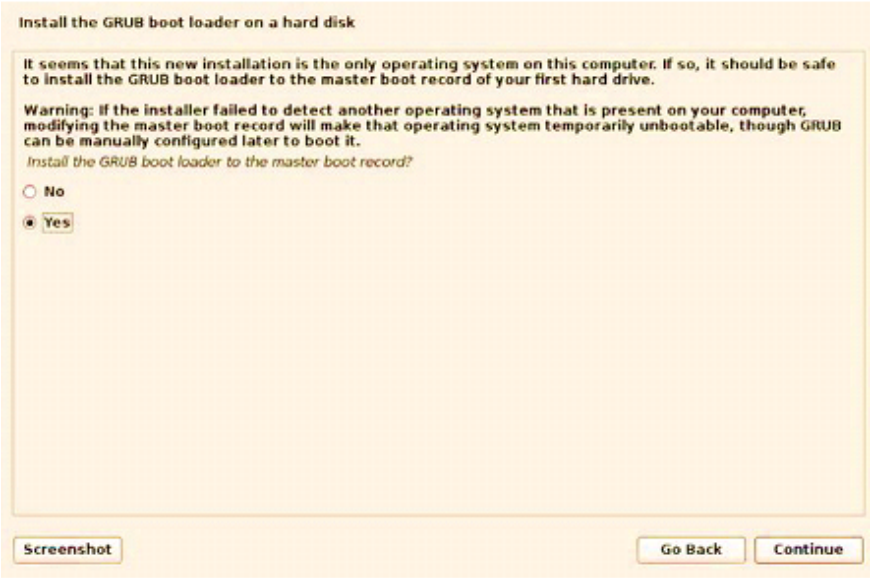
If you use a proxy, you will need to enter the configuration data at the following prompt the installation wizard will display. As shown below, you can leave it empty. To start the GRUB loader installation, click the Continue button.



Configuring a proxy.

Install the GRUB Loader

The Grand Unified Bootloader, also known as GRUB, is the name of the main screen that appears when a computer is turned on. GRUB offers a platform where a user may check particular boot-up options, make adjustments as needed, and modify settings before the operating system loads. GRUB is strongly advised for the majority of Linux installs, despite the fact that some sophisticated users may not necessarily need it. The "YES" option has been selected for you to install GRUB, as seen in the figure below. Click the Continue button to move on to the next installation phase.

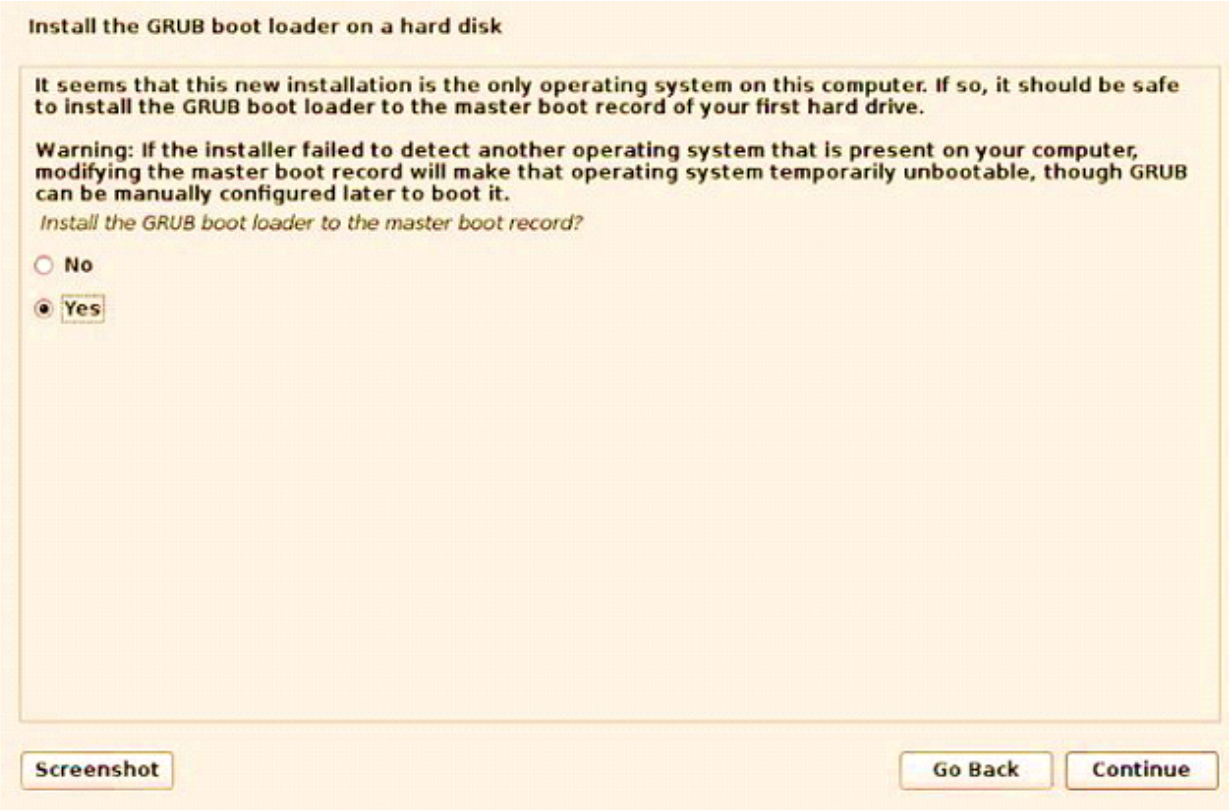


Installing the GRUB loader.

Kali Linux Installation is Now Complete

Your installation is now finished. Restart the computer after removing the flash drive or optical disk. You will be prompted to restart the computer. To finish your installation, click the Continue button. See the illustration

below. You will get a welcome screen after rebooting that asks you to log in. Use the login information you created before. It will end there. Greetings from Kali Linux!



Completing the installation.

Why You Should Use Kali Linux

As we've already mentioned, Kali Linux comes pre-installed with nearly all of the tools needed for any of the aforementioned tasks. Security auditors, forensic investigators, penetration testers, and researchers favor it for this reason.

In addition to hacking networks and websites, Kali may also be used to run Open Source Intelligence on an entity. In addition to ethical hacking, Kali Linux has tools that can be used for forensic inquiry. This area of security is quickly becoming to be just as crucial because it primarily gathers information, analyzes it, and then uses the findings to track down cybercriminals. The use of forensic investigation enables the detection and elimination of malicious byproducts of malevolent activity. It is also helpful in managing and calculating the loss that results from a cyberattack. The stealth Live mode, which is mostly used in forensics and does not leave traces (fingerprints and footprints) on a host's system, is a crucial component of Kali.

A terminal

Opening the terminal, which is the command-line interface we'll be using in this book, is the first thing you should do when using Kali. The terminal icon can be seen at the bottom of the desktop in Kali Linux.

Press CTRLALTT or double-click this icon to launch the terminal. The terminal launches the shell, a command-line environment that enables you to run scripts and run commands on the underlying operating systems. The bash

shell, which is the default shell in Kali and many other Linux distributions, is the most widely used of Linux's many distinct shell environments. The command password can be used to modify your password.

Basic Linux Commands

Let's start by taking a look at some fundamental Linux commands that will get you started.

Finding Yourself with pwd

Unlike Windows or macOS, the Linux command line does not always make it clear which directory you are currently in. You often need to be aware of your location in order to browse a new directory. Your position inside the directory hierarchy is returned by the pwd command, which shows the current working directory. To find out where you are, type pwd into your terminal: kali >pwd /root In this case, Linux responded with /root, indicating that I am in the root user's directory. You should also be in the root user's directory, which is located one level below the top of the disk hierarchy (/) since you logged in as root when you began Linux. Pwd will instead return the name of the directory you are currently in.

Using Whoami to Check Your Login

The sole "all-powerful" superuser or system administrator in Linux is known as the root, and it has all the privileges required to add users, modify passwords, alter permissions, and other things. Naturally, you do not want just anyone to have this authority; you want someone you can rely on and who is familiar with the operating system. You might wish to log in as root because, as a hacker, you often need all those privileges to execute the

programs and instructions you require. Using the “whoami” command, a Linux user can determine which user they are currently logged in as, as seen below: kali >whoami root In this case, the user is logged in as root.

A crucial Linux skill is being able to navigate the filesystem from the terminal.

You must be able to navigate in order to seek programs, files, and directories that are housed in other folders in order to complete any task. The directories can be seen visually in a GUI-based system, but when using a command-line interface, the structure is purely text-based, and using the filesystem requires typing certain commands.

Using the cd Command to Change Directories

To change directories from the terminal, use the cd command. Here’s an example of how to switch to the /etc directory.

the location where configuration files are kept: kali >cd /etc root@kali:/etc# The prompt now reads root@kali:/etc, indicating that we’ve entered the /etc directory. directory. To verify this, type pwd root@kali:/etc# pwd.

/etc We use cd followed by double dots (..) to move up one level in the file structure (toward the root of the file structure, or /), as displayed here: root@kali:/etc# cd..

This raises us one level above /etc, root@kali:/# pwd / root@kali:/#. to the /root directory, but you can advance any number of levels. Simply use as

many double-dot pairs as levels you wish to move, for example, you would use. to ascend a level.

You would employ. .. two levels higher.

You would employ. .. .. three layers higher, and so forth.

In order to advance two levels, for instance, type cd followed by two sets of double dots and a space: kali >cd. ..

By using cd /, where / denotes the filesystem's root, you can easily advance to the root level of the file hierarchy from any location.

Listing the Contents of a Directory Using the ls (list) Command We can use the ls (list) command to view the files and subdirectories that make up a directory. This is extremely comparable to the Windows dir command.

```
kali >ls
bin   initrd.img      media     run     var
boot  initrd.img.old  mnt       sbin    vmlinuz
dev   lib             opt       srv     vmlinuz.old
etc   lib64           proc      tmp
home  lost+found      root      usr
```

This command displays a list of the directory's files and folders. By adding the directory name after the command, for example, ls /etc, you can use this command on any specific directory in addition to the one you are presently in. shows the contents of the /etc.

directory. You can add the -l switch after ls (the l stands for long) to acquire extra details about the files and directories, including their permissions, owner, size, and when they were last edited.

The long listing is another name for this. See the illustration below:

```
kali >ls -l
total 84
drw-r--r--   1   root   root   4096   Dec   5   11:15   bin
drw-r--r--   2   root   root   4096   Dec   5   11:15   boot
drw-r--r--   3   root   root   4096   Dec   9   13:10   dev
drw-r--r--   18  root   root   4096   Dec   9   13:43   etc
--snip--
drw-r--r--   1   root   root   4096   Dec   5   11:15   var
```

Getting Help

In Linux, almost every command, program, and utility have a specific help file that describes how to use it. For instance, if I needed assistance with the best wireless cracking program, aircrack-ng, I could enter kali >aircrack-ng —help. Note the double dash here. In Linux, it is customary to use a double dash (—) before word options like "help" and a single dash (-) before options with just one letter, like "-h." When you input this command, you ought to receive instructions for using the tool as well as a brief description of it. You may be able to use either -h or -? to access the help document. For instance, kali > nmap -h would be entered if I required assistance using Nmap, the best port scanning tool for hackers. Unfortunately, even while many applications accept all three options, there is no guarantee that the one you are using will. So kindly try a different option if the first one doesn't work.

Finding Files

Navigating around Linux can be tedious until you get used to it, but learning a few fundamental commands and tricks will make the command line much more user-friendly. You can use the following commands at the terminal to find stuff.

Locate is probably the most user-friendly command for searching. This command, when used with a keyword specifying what you're looking for, will search your whole filesystem for that term anywhere it appears. Enter the following, for instance, to search for aircrack-ng:

```
kali >locate aircrack-ng
/usr/bin/aircrack-ng
/usr/share/applications/kali-aircrack-ng.desktop
/usr/share/desktop-directories/05-1-01-aircrack-ng.directory
--snip--
/var/lib/dpkg/info/aircrack-ng.mg5sums
```

However, the locate command is not faultless. The information you receive from locate's results may occasionally be too much to handle.

locate uses a database that is typically only updated once per day, so if you recently generated a file, it could not appear in this list until the following day. Knowing the drawbacks of these fundamental commands can help you choose when to use each one.

Using the where is command to find binary files

If you're looking for a binary file, you can use this command to find it. If they are available, this command also returns the binary's source code and home page in addition to the binary's location. Here's an illustration:

```
kali >whereis aircrack-ng
aircarck-ng: /usr/bin/aircarck-ng /usr/share/man/man1/aircarck-ng.1.gz
```

Using the which Command to Locate Binaries in the PATH Variable

The which command is even more specific: In Linux, it only returns the location of the binaries that are present in the PATH variable. For instance, when I run the command line program aircrack-ng, the operating system consults the PATH variable to determine which directories to search for the program. In this case,

kali >which aircrack-ng
/usr/bin/aircrack-ng

It was successful in locating a single binary file in the PATH variable's listed directories. These directories typically contain /usr/bin as a minimum, but they may also contain /usr/sbin and maybe a few more files.

Using the Find Command to Conduct More Powerful

The find command is the most robust and adaptable of the searching utilities. It can start your search in any specified directory and look for a number of different criteria, including the filename of course, but also the owner, the group, the rights, the size, and the date of creation or modification.

The fundamental syntax for find is as follows: find directory options expression

Filtering with grep

You may frequently want to search for a certain term while using the command line. To do this, you can narrow your term search using the grep command. When output is piped from one command to another, the grep command is frequently utilized.

```
kali >ps aux | grep apache2
root  4851 0.2 0.7 37548  7668 ?  Ss  10:14  0:00  /usr/sbin/apache2 -k start
root  4906 0.0 0.4 37572  4228 ?  S   10:14  0:00  /usr/sbin/apache2 -k start
root  4910 0.0 0.4 37572  4228 ?  Ss  10:14  0:00  /usr/sbin/apache2 -k start
--snip--
```

The command in the aforementioned example will list all the services that are currently active before passing the result to grep. Grep searches the received output for the term we specified in the command. The keyword in our situation is apache2. Grep will proceed and output just the results that are pertinent. Saving time with this command.

After you've located the folders and files you were looking for, you might need to perform a number of operations on them. We'll learn how to create directories and files, copy and rename files, as well as delete files and folders.

File Creation

There are other ways to create files under Linux, but for now, let's look at two straightforward techniques. The first is the cat, which is short for concatenate and refers to the act of combining components rather than your

beloved household cat. The cat command can produce tiny files in addition to often being used to display a file's contents. It's preferable to enter the code in a text editor like Vim, emacs, leafpad, gedit, or kate and then save it as a file when developing larger files.

Concatenation with the cat command

The cat command followed by a filename will display the contents of that file, but to create a file, we add a redirect, indicated by the > symbol, and the name of the file we want to create after the cat command. Here is an illustration:

kali > cat > kalilinux

Using Kali Linux for hacking!

File Creation

Using Touch Touch is the second command for creating files. Originally, the purpose of this command was to allow a user to edit a file's metadata, such as the creation or modification date. But by default, this operation creates the file if it doesn't already exist.

Let's use the touch command to create newfile:

kali >touch newfile

Afterwards, when I run ls -l to view the directory's long list, I can see that newfile has been created as a new file. Because the newfile is empty, take note that its size is 0.

Making a Directory In Linux,

the command to make a directory is called mkdir, which stands for make directory. Enter the command below to create a directory called new directory:

```
kali >mkdir newdirectory
```

Enter the following to access this recently created directory:

```
kali >cd newdirectory
```

Copying a File

The cp command is used to copy files. By doing this, the old file is kept in place and a duplicate of it is created in the new location. Here, we're going to use touch to create the file oldfile in the root directory and copy it to /root/newdirectory while renaming the original oldfile to remain in place:

```
kali >touch oldfile
kali >cp oldfile  /root/newdirectory/newfile
```

You can choose to rename the file by simply appending the name you want to it to the end of the directory path. The original name of the file will be retained by default if you don't rename it when you duplicate it. When we

next navigate to newdirectory, we can see that newfile is an exact duplicate of oldfile:

kali >cd newdirectory
kali >ls
newfile oldfile

Renaming a File

Regrettably, unlike Windows and some other operating systems, Linux lacks a dedicated command for renaming files. However, it does have the mv (move) command. The mv command can be used to rename an existing file or directory or relocate them to a different location. You would input the following to rename newfile to newfile2:

```
kali >mv newfile newfile2
kali >ls
oldfile newfile2
```

Now that newfile2 has been renamed, you may see it when you list (ls) that directory but not newfile. The same is possible with directories.

Delete a File

To delete a file, use the rm command as follows:
kali >rm newfile2

You can verify that the file has been deleted by running a long listing on the directory.

Removing a Directory

The rm command for removing files has the appended dir (for directory) parameter, as shown below:

```
kali >rmdir newdirectory
rmdir:failed to remove 'newdirectory': Directory not empty
```

It is crucial to remember that rmdir will not remove a directory that is not empty, as you can see in this example, but will instead notify you that the directory is not empty. Before you remove the directory, you must first remove all of its contents. This will prevent you from inadvertently removing items that you did not mean to. If you do want to remove a directory and its content all in one go, you can use the -r switch after rm, as shown below:

kali >rm -r newdirectory

Just a word of caution, though: be wary of using the -r option with rm, at least at first, because it is straightforward to remove valuable files and directories by mistake. For instance, using rm -r in your home directory would delete every file and directory there; this is undoubtedly not what you intended.

Finding tools and packages

Before you download a software package, you can check to see if it is already present in your operating system's repository, where data is kept. The search feature of the apt tool allows you to see if the package is already installed. Simple syntax is used here:

```
apt-cache search keyword
```

Keep in mind that to search the apt-cache—the location where it keeps package names—we use the apt-cache command. For instance, you would execute the command indicated below to look for the intrusion detection system Snort.

```
kali >apt-cache search snort
fwsnort - Snort-to-iptables rule translator
ippl - IP protocols logger
--snip--
snort - flexible Network Intrusion Detection System
snort-common - flexible Network Intrusion Detection System - common files
--snip--
```

As you can see, the word “snort” appears in numerous files, but in the center of the output, we find the phrase “snort - flexible Network Intrusion Detection System.” That is what we’re trying to find.

Installing Software

You can use apt-get to get the program now that you are aware that the snort package is available in your repository. Use the apt-get command, the keyword install, followed by the name of the package you wish to install in the terminal to install software from the default repository of your operating system. The format is as follows: apt-get install package name Let’s test this out by setting up Snort on your system. As seen below, type the command apt-get install snort.

```
kali >apt-get install snort
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
snort-doc
The following NEW packages will be installed:
snort
--snip--
Install these packages without verification [Y/n]?
```

You may learn what is being installed by the output you see. If everything appears to be in order, press Y to continue with the software installation.

Software Removal

To uninstall software, use apt-get with the remove option and the name of the program to be deleted. Here is an illustration.

```
kali >apt-get remove snort
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer
required:
  libdaq0 libprelude2 oinkmaster snort-common-libraries snort-rules-default
--snip--
Do you want to continue [Y/n]?
```

You will once more watch the tasks being completed in real time and be prompted to decide whether you wish to proceed. You can press Y to uninstall, but because we'll be using Snort again, you might want to keep it.

The delete command does not remove the configuration files, so you won't need to reconfigure if you reinstall the same package in the future. You can use the purge option, as displayed below, to remove the configuration files along with the package if you do so.

```
kali >apt-get purge  snort
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libdaq0 libprelude2 oinkmaster snort-common-libraries snort-rules-default
--snip--
Do you want to continue [Y/n]?
```

To continue removing the software package and configuration files, type Y when prompted. Many Linux packages are divided into software pieces that may be used by numerous different programs in order to keep things compact and modular. When you installed Snort, you also installed a number of dependencies or libraries that Snort needs in order to function.

These other libraries or dependencies are also removed since Snort is being uninstalled and they are no longer required.

package updates

New software or updated versions of existing software will be added to software repositories on a regular basis. You must ask them to apply these updates to your system because they do not come to you automatically. Upgrading differs from updating in that upgrading brings a package up to date with the repository's most recent version whereas updating changes the list of packages that are accessible for download. By using the apt-get

command and the term update, you can upgrade your system. This will look through every package on your system to see if there are any updates. The updates will download if that is the case. See the illustration below.

```
kali >apt-get update
Get:1 http://mirrors.ocf.berkeley.edu/kali kali-rolling InRelease
[30.5kb]
Get:2 http://mirrors.ocf.berkeley.edu/kali kali-rolling/main amd64
Packages
[14.9MB]
Get:3 http://mirrors.ocf.berkeley.edu/kali kali-rolling non-free amd64
Packages
[163kb]
Get:4 http://mirrors.ocf.berkeley.edu/kali kali-rolling/contrib amd64
Packages [107kB]
Fetched 15.2 MB in 1min 4s (236 kB/s)
Reading package lists… Done
```

Done Your system's software repository will now refresh with a list of available programs. Reading package lists will be displayed on your terminal if the update was successful. It's finished, as you can see above. Please take note that the repository name, values, time, size, and other factors may vary on your system.

Package Upgrades

Use apt-get upgrade to update the installed packages on your system. You must be logged in as root or use the sudo command before doing an apt-get upgrade since updating your packages could trigger modifications to your software. This command will upgrade all of your system's packages that apt

is aware of, which only includes those that are kept in the repository, as illustrated in the example below.

You might not be able to use your system for a while while it is being upgraded because it can take some time.

```
kali >apt-get upgrade
Reading package lists... Done
Building dependency tree... Done
Calculating upgrade... Done
The following packages were automatically installed and no longer required:
--snip--
The following packages will be upgraded:
--snip--
1101 upgraded, 0 newly installed, 0 to remove and 318 not upgraded.
Need to get 827 MB of archives.
After this operation, 408 MB disk space will be freed.
Do you want to continue? [Y/n]
```

Your system should estimate how much hard disk space is required for the software package, as you can see in the result. If you want to proceed and have enough hard disk space for the upgrade, press Y.

Chapter 3: The Hacking Process

In defense hacking for businesses and organizations, which includes the discovery of possible threats on a computer or network, is known as ethical hacking, carried out by white hat hackers.

Ethical hacking follows a similar set of distinct phases to all good initiatives. Making a planned ethical hacking attack aids hackers. The process of ethical hacking is described in various ways in security training books, however in my experience, it may be divided into the following six phases:

reconnaissance.
Scannable.
Gaining Access.
Preserve Access.
Make your tracks clear.
Reports

Reconnaissance

Reconnaissance: What is it? It is a preliminary survey that is conducted to gather information, according to the dictionary definition. The exploratory surveys that militaries carry out on enemy territory serve as an illustration. Reconnaissance in the context of cyber security is the process of learning more about a target using a variety of methods.

An ethical hacker is interested in three types of information throughout this exercise:

1. The Network.
2. The Host

3. Users/Participants.

How to Perform a Reconnaissance Exercise in Steps.

The first phase in ethical hacking is typically intended to aid a penetration tester in comprehending their targets. This falls within the umbrella of the category of information gathering.

Underneath, we have something called reconnaissance, which we characterize as being a collection of methods and procedures used in learning and gathering vital details about a target. They consist of scanning, counting, and fingerprinting. Following the seven steps outlined below, an ethical hacker attempts to learn as much as they can about a target system during a reconnaissance exercise;

Gathering preliminary data.
Establish the range of a network.
Determining which machines are on.
Learning about available open ports and access points.
Fingerprinting of operating systems.
Checking for services that are active on different ports.
Maps of the network.

There are two main categories for reconnaissance.

Active Reconnaissance: Information obtained through active reconnaissance is accurate because it includes making direct contact with your target's computer system. There is a chance of being discovered engaging in active reconnaissance without authorization. But the majority of hacking tasks demand active reconnaissance.

Passive Reconnaissance: You won't be directly connected to a computer system during this process. Without ever engaging with the target systems, this approach is used to obtain crucial data.

Enumeration

Enumeration, in its truest sense, is the systematic listing of everything in relation to the objects in a collection. Making a list of policies, user accounts, shares, and other resources is known as enumeration. This process comes right after scanning and before vulnerability evaluation. This aids the attacker in developing the most effective access-gaining plan.

You may use enumeration to learn more about:

Users and Groups
Shared pathways and networks
Hostnames
Route Diagrams
Service Configurations
SNMP port scanning

Applications and banners use DNS details.

These tools can be used for enumeration. In the Windows Operating System, a variety of tools are used with commands like "Net accounts," "Net config server," "Net config workstation," and "Net view" to enumerate NetBIOS names.

<u>Scanning</u>

This process is used to find the services, running hosts, and open ports that the target application is using. Let's imagine you want to find a system's weak points. To do this, you'll need to attack a system point. Network scanning is used in ethical hacking to discover these spots. Black Hats use these locations to break into a system. The pertinent teams will focus their efforts on system improvement after identifying these issues. We are aware that every organization has a network.

They might even be linked to the internet or internally. In order to break into these networks, you must first identify a weak spot where you can employ attacks. We use a technique called network scanning to find these sites within a network.

Goals of Network Scanning

It aids in the identification of open ports, active hosts, and the victim's IP address.

Network scanning enables the identification of the services active on the host computer.

It also helps in identifying the target's operating system and system architecture.

We can find and fix vulnerabilities by scanning Live hosts.

What distinguishes network scanning from reconnaissance?

I'm going to utilize this analogy to assist you comprehend the differences between the two. Assume you are an army commander who has been given the order to go with your squad and carry out an attack on a terrorist camp. We're going to presume that you already know where the camps are and what's in their immediate neighborhood. Now, this kind of knowledge is

typically gathered through reconnaissance. To begin your attack, you will still need to locate a point of entry inside the terrorist camp. We now refer to this as network scanning. We can state with confidence that reconnaissance is a method you'll employ to gather data so you can learn more about your target. On the other hand, network scanning is a method you'll use to find any potential weak spots in the network. A targeted network can be accessed through these points.

Network scanning can be separated into two categories based on the data obtained from the scan: a port scan

Velocities Scanning

We can infer from the name that port scanning is a technique for locating active ports on a network. The way a port scanner operates is by sending client requests to the set of targeted ports on a network. After saving the port-specific information, a reply will be sent back. This is how active ports are discovered, good readers. After obtaining a target's IP address (by scanning the UDP and TCP ports of the victim organization), the hacker will move on to map the network of the target company.

Port scanning techniques

SYNScan: The TCP three-way handshake method is not finished in this mode of scanning. Here, a victim will get the SYN packet from a hacker or penetration tester. The target will establish a connection and the port will be able to listen if a SYN/ACK response frame is received. If you get a RST from the destination, the port might not be open or it might be closed. This form of scan has the advantage that only a few IDS systems would report it as an attack or a connection attempt.

XMASScan: The scan sends a packet with the flags PSH (for push), URG (for urgent), and FIN (for completion). Assume we have an open port; we do not anticipate a response; if the port is closed, the target will respond with a RST/ACK packet. (RST=reset)

FINScan: With one exception, this scan is virtually analogous to an XMAS scan. Only the FIN (finish) flag is transmitted in packets sent via FINScan.

The other two flags (URG and PSH flags) are not present in the scan.

The reaction is comparable to an XMAS scan. The limits of the two scans are comparable as well.

IDLEScan: This type of scan determines the responses from the port scan along with the IP header sequence number in order to transmit a SYN packet to the target using a fake IP address. Depending on the scan's outcome, the port is either regarded as open or closed.

TCP Inverse Flag Scan: In this scenario, a hacker will send TCP probe packets with or without a TCP flag (FIN, URG, PSH). If there is no response, the port is open, and RST indicates that the port is closed.

ACK Flag Probe Scan: In this kind of port scanning, a hacker sends TCP probe packets to a location where an ACK flag is set to a distant device that is utilized for header information analysis.

This data consists of the WINDOW and TTL fields. One utilizes the RST packet to determine whether the port is open or closed. This scan can also be

used to examine a target's filtering setup.

Velocities Scanning

In essence, we utilize this kind of network scanning to look for vulnerabilities in a network. Vulnerability scanning identifies weaknesses that may occur as a result of network configuration errors or bad programming. Let's look at a few tools used for network scanning before moving on.

tools for network and port scanning

Utilizing Nmap, data such as operating systems, types of packet filters and firewalls, active hosts on a network, services, and operating system versions can be extracted.

This tool, called Angry IP Scanner, can be used to look up IP addresses on systems that are accessible inside each input range.

Superscan is a potent instrument created by McAfee. It may be used to ping in addition to being a TCP port scanner.

ZenMap: This scanner comes with a very potent GUI tool that can be used to identify the type of OS version, perform port scanning, OS, ping sweep, etc.

A collection of several applications and programs used for web rippers, port scans, mass emails, and floods is referred to as the Net Scan Tool Suite Pack. Although there is a sample version of the tool, there are also commercial versions available.

Famous and potent tools used for listening to network traffic include Wireshark and Omnipeak. A network analyzer can be created using either tool.

measures to prevent scanning

System administrators can configure IDS and firewalls to block all probing efforts in addition to detecting them.

Using unique rules to secure the network and block any undesirable ports.

To check whether the firewall accurately detects any port scanning activity, a user might utilize tools for port scanning.

Anti-spoofing and anti-scanner rules must be correctly configured, and security experts must ensure this.

System and network administrators must make sure that routers, IDS, and firewall firmware are all current.

How to Access

Access is the most important part of an attack by far. I'm speaking in terms of possible harm. In order to harm a system, malicious actors do not always need to gain access to it. A denial-of-service attack, for instance, can be launched remotely and has the potential to abruptly terminate any services that are already running on the target or, in some situations, deplete all available resources. Processes can be killed to terminate service. A logic/time bomb can be used to do this. A system crash and reconfiguration both have the same effects.

Local network resources may run out due to overloaded outbound communication lines. Such exploits can be used for fraud or theft locally,

remotely across a LAN or the Internet, or offline. Here are a few instances of these:

Session espionage

Stack-based denial of service and distributed denial of service caused by buffer overflows

Spoofing is a technique used by sophisticated attackers to exploit a target's system by pretending to be other systems or outsiders.

They can send a bug-filled, faulty packet using this method. The target system has vulnerabilities that this bug will try to exploit.

One method for remotely stopping the availability of critical services is packet flooding. Smurf attacks are a distinct subtype of our attacks. These attacks try to get the available network users to respond. The victim will then be inundated using their actual addresses. The following factors are crucial to an attacker's ability to successfully enter a target system:

- the first degree of access received.
- The attacker's level of expertise and
- the target system's architecture and configuration.

The distributed denial-of-service assault is the denial-of-service attack that does the most damage. This occurs when an attacker launches a coordinated, widespread denial of service assault using zombie malware that is installed on numerous computers connected to the Internet.

Maintaining Access

Once a hacker has gained access to the target system, he or she must put up considerable effort to make sure their boat, to use an analogy, stays afloat. The hijacked machine may be used by the attacker to stealthily exploit it, serve as a launchpad for additional assaults like DDoS or spam operations, or be used to scan for and attack other systems. All of these behaviors may be harmful. Let me give you a real-world illustration. Sniffer software can be developed by hackers to assist in the capture of all network traffic, both inbound and outbound. Telnet conversations with other systems and file transfer protocols can be a part of the traffic, allowing them to convey the collected data to any location. It will be necessary for those who don't want to be found to perform actions that will mask their presence. We can do this using a variety of methods. The preferred technique involves installing covert channels, rootkits, Trojan horses, and backdoors to provide the hacker unrestricted access to such systems.

Tools and Techniques

One approach to gaining rapid access to a system that has already been compromised is through the use of a Trojan or backdoor. A Trojan horse gives a hacker access at the application level. The drawback of the approach is that a target system must first have the Trojans locally installed. Trojans have the ability to set up shop on Windows-based computers as a service. They will then have access to administrative functions. They are thus capable of functioning as a local system. These Trojans can be used by a hostile person to steal login information, passwords, and any other sensitive data from the system. The backdoors that attackers typically install have built-in download and upload functionality, just like with remote access Trojans. This method uses port 80 for HTTP, port 443 for HTTPS, and port 53 for DNS to mask their traffic.

A Covert Channel

In this scenario, data is transmitted using covert communication tunnels. These routes include VoIP, HTTP, DNS, and ICMP tunnels, as well as others. Be aware that you can also send encrypted data through the covert channels we outlined. Covert channels may be discovered. Only that the victim must put out a lot of effort. Anomalies in the traffic leaving the network can be detected using tools like flow data analysis, protocol analysis, and network signatures. To find these, specialized tools are needed. Be aware that although identifying a hidden route is one thing, blocking it is another. You can use a few of the following strategies.

Blocking requests for DNS-related information from servers outside of corporate networks; prohibiting outbound ICMP at the corporate information border. You can schedule a delay in the delivery of voicemails in cases of exfiltration tunneling using VoIP RTR. This will allow for sending the voicemail to an audio processor for the examination of every packet to find any encoded data, similar to how antispam software works. Requests can be made for internal DNS servers, HTTP tunnels dissipating through the use of Web proxies, and voicemail delivery delays.

Rootkits

This type of malware is very good at hiding from a computer system. This characteristic set rootkits apart from other types of malware. They can get beyond security precautions that have been put in place on the computer thanks to their enhanced ability to conceal. The fact that they are difficult for standard malware detection software to identify is the fundamental motivation behind their creation. Trojan horses are typically used to install rootkits on the targeted platform starting with “user” level access. Once inside the target system, rootkits will observe login information like passwords in order to get “administrator” level access. This is a privilege escalation, as

keen readers will point out. That is accurate. Despite this, maintaining access is the rootkits' primary area of expertise.

Rootkits have a propensity to linger around a targeted system, gradually degrading it. Ordinary viruses, on the other hand, are typically built to do the most harm in the shortest amount of time. The crucial word here is secrecy. For instance, keyloggers with rootkits are specifically designed to record every word unaware victim types into their keypad. For as long as it goes unnoticed, it will gather private data. Due to this, identity theft is very likely. A parasite that enters the body through a variety of channels makes an excellent analogy. It will remain inactive for an extremely long time. It will now erupt after it has gathered enough strength to defeat the body's immune system.

Three fundamental layers can be found in a computer system.

These are the hardware level, the kernel, and the operating system.

In a nutshell, the operating system's kernel serves as its structural foundation. User-level rootkits frequently use low-priority processes to compromise the software responsible for protecting a computer. Kernel-level rootkits are more sneaky and harmful rootkits. This is primarily because it has repeatedly been shown to be challenging to remove rootkits at the kernel and boot levels.

Normally, rootkits that have settled in the kernel memory leave no traces on the hard drive. In order to make themselves "reboot resistant," these rootkits frequently modify the kernel, files, and various disk components.

Kernel-level rootkits can run even before the operating system starts. This category of rootkits can bypass encryption by creating secret channels to give them unrestricted access to the compromised system. Rootkits can conceal their presence by adding their code to kernel sectors.

When rootkits are installed at the kernel level, they gain full administrative access to the systems that are being attacked. Unlike Trojan horses, rootkits typically establish a direct path to the operating system level.

Getting rid of rootkits

The conventional security methods, such as antivirus software, are insufficient to completely eradicate rootkits. As an alternative, you can remove rootkits from your system using apps designed for the purpose, such as Malwarebytes Anti-rootkit, TDSSKiller, Sophos Anti-Rootkit, and GMER. Keep in mind that the rootkit may not always be completely eliminated from your machine. The aforementioned tools can only lessen the negative consequences that the rootkit leaves behind on your system. A user has the option to start the clean slate process in addition to employing tools to deal with rootkits. Here, the crucial files are backed up, and the operating system is completely reinstalled. In most cases, this will guarantee that the rootkit is eliminated from your computer. Once more, this does not imply that the removal will be 100% successful. Although they are uncommon, BIOS-level rootkits can survive a re-install. Regardless of how hard rootkits try to conceal themselves, there will always be indicators that they are present in a system. This is significant because they are made to prevent an assailant from the outside from entering the building.

Data exfiltration is the unlawful movement of data to a system or device outside of the organization. The data may come from a computer system or

from IT servers. The procedure can be carried out manually (by copying and pasting) or automatically (by malware). The security company McAfee stated in 2015 that the majority of data exfiltration cases (about 60%) involved direct electronic methods. The remaining 40% involved tangible media, such as snatching a laptop or downloading data using a USB drive. It's interesting to note that a sizable percentage of that 40% involves cell phones. Personal health information, personally identifiable information, financial information, and intellectual property were the data types that were most frequently exfiltrated. The electronic exfiltration of data uses various tunneling protocols, file transfers, web protocols, or email transfers. We are aware that the file transfer protocol is a widely used network protocol designed to facilitate file transfers. It can be helpful in campaigns including data exfiltration.

It is possible to rig peripheral devices on the targets and other devices, including microphones and webcams, to make it possible to watch the target's movements. The hacker can utilize HTTP file transfers or the Tor network to remain anonymous. Early detection is crucial to preventing hackers from stealing your data and protecting yourself from Advanced Persistent Threats. Organizations must have a functional threat intelligence strategy in place to help them spot suspicious data exfiltration-related activity. Keeping up with the most recent developments in the security industry will be made easier by connecting the local threat intelligence system to the global threat intelligence network. Let me mention a few noteworthy signs of data exfiltration. These could serve as the basis for a thorough investigation. They are:

<u>Unauthorized/unsanctioned port activity.</u>

Multiple emails sent to non-corporate domains Abnormally high email sending rates by hosts

User activity on the web uploading. Typically, non-corporate websites will receive the uploads.

As I wrap up this section, you now know that an attacker must spend some time circling their targets in order to gather useful information. That suggests that you will need to master the “Maintaining Access” cycle of the hacking process.

It’s simpler to say than to do. There are many tools included with Kali Linux that can assist you in keeping control of a targeted system. Maintaining access is the equivalent of breaking into someone else’s home without their consent. You’ll soon understand that entering the house is merely the first step. Another is continuing to be present but avoiding detection. It can be even more challenging than the first challenge.

Cleaning Up Our Traces

In this stage, we’ll discover how hackers hide their identities in order to remove any digital evidence they may have left behind. It is clear that this is a bad thing to do. Simply expressed, it has to do with erasing records of the activities that occurred throughout the hacking process. This subtopic will be covered in great length because it is so crucial for readers who want to become skilled hackers. After clearing tracks, there is one more procedure that involves drafting reports, which consists primarily of paperwork. We can carefully inspect digital signs left behind by an intruder to determine whether a system has been targeted. A hacker should remove any evidence of their activity that might lead to them. You may have noticed that a penetration tester or hacker was able to evade firewalls and intrusion detection systems in the earlier phases. However, the goal of this stage is to hide any clues that could reveal the nature of the hacker’s actions.

Covering/clearing rails mostly involves:

Anti-Forensics measures aim to obstruct the gathering of digital evidence during a potential post factum investigation.

1) Anti-Incident Response methods try to prevent real-time detection.

Anti-Incident Response The fundamental goal of anti-incident response is to impede, perplex, and outwit the targeted company's incident response team. A hacker or penetration tester may also be able to establish a long-term foothold inside their target even after they have been discovered through actions falling under this category.

Antiincident response can be used to carry out important activities like:
•discreetly deploying backdoors;
•configuring infrastructure to allow for agility in lateral movement;
•and continuously updating the number of infected hosts.
•Additionally, their numbers shouldn't be excessive.

utilizing numerous types of malware on the network.

by cranking up the pace, you're preventing responders or investigators from keeping up with what's happening.

Busy file servers can also be utilized as a means of data staging. They make the ideal cover for internal hop-points.

In some circumstances, using a VPN for communication could get beyond network monitoring controls.

The efforts made to prevent the rapid identification of an ongoing, or continuous, cyberattack are what matter when it comes to how anti-incident response functions. This includes disguising the source of malware transmission. Anti-forensics, on the other hand, is intended to hinder the investigators' ability to obtain sufficient digital evidence that will be presented before a court of law during later stages. It contrasts with the deliberate actions taken by hackers or penetration testers to destroy any evidence present and cause a digital investigation to die out during the initial stages. This suggests that anti-incident reaction operations are urgent since a significant amount of the action takes place on a live, running system in real-time. When compared to investigators in a prospective future digital probe, incident responders are likely to be far more time-constrained in their countermeasures.

Anti-Forensics

Before we dive into this subject, let's first define forensics. We define computer forensics as a science whose fundamental goal is to make it possible for forensic professionals to gather, preserve, analyze, and present digital evidence in a court of law. We describe anti-forensics as a field that includes any method and technology currently in use for erasing, altering, or concealing digital data. The modification, deletion, or destruction of digital evidence is the primary goal of anti-forensics. One can tell from the name that this is concerned with the methods or actions that are intended to obstruct an eventual digital investigation and to reduce both the quantity and quality of evidence. Antiforensics has also been defined by some as the "Attempts made to negatively compromise the quality, amount, and existence of evidence from a crime scene or to complicate the examination and analysis of evidence so that it is impossible or difficult to conduct." Anti-forensic tactics and tools are frequently used by cybercriminals such as online pedophiles, hackers,

counterfeiters, cyberterrorists, and other cyber criminals. It is clear that they want to get rid of any evidence that can implicate them.

Evidence Removal

Some of us are so concerned that we've spent money on disk cleaners and privacy protection software just to erase the information we don't want others to see. It is thought that everything on the hard drive can be permanently deleted with these programs. Users can wipe files using the "secure delete" option, and the following types of data can be specifically deleted: registry items, thumbnails, jumplists, Skype chat sync, and so forth. Web browser history and cache are also among the types of information that can be deleted.

Many of these clean-up procedures can be defeated by a forensic specialist using specialized forensic instruments. For instance, images that a forensics expert would find interesting can be recovered. This is due to the fact that Windows Thumbnails will remain contain a smaller version of this image even after the original image has been deleted. By performing what we refer to as "file carving," we can still restore the thumbnail even after it has been deleted.

Jumplists can also provide details on the photographs, programs, papers, and various other kinds of files that the user has used. Even for files that are accessed from the outside, jumplists are typically established.

Whether the original file has been erased or the external device has been taken away, it will continue to exist. These lists often include a MAC address, the name of the item being viewed, the path to the file being accessed, the application being used to view the file, the name of the computer, and the time and date of the access. This suggests that jumplists provide great proof of access. Manually deleting the "chat sync" folder's internal data will not

remove any Skype history. You can find tidbits of user interactions in the folder's content. Despite the method's flaws (deleting), when done correctly, it can permanently delete evidence, leaving forensics specialists without any evidence.

Even though some wrongdoers can use this technique to avoid detection, hiding, moving, renaming, or altering files may come across as naive. Here, trails can be hidden by renaming or relocating files that contain chat histories or by changing file extensions. My friends, this is not a simple task. There are programs available that can be used to partition big files into smaller ones. The ends of other files can obscure these divisions. A hacker can use the unused file space, also known as slack space, by using specialized tools to hide important data from view. Additionally, a hacker may bury a file inside another (stenography, perhaps). With executable files, this technique functions perfectly.

Timestamping Investigators frequently don't look through every file on a computer system. Most of the time, they arrange the data in chronological order so they may focus their search for possibly pertinent data. When an attack is known, they will want to see the information right after it happened. Criminals will often make an effort to thwart this strategy by altering the metadata of the files they need. The times and dates each file was last visited, last modified, and created are often changed. Time stamping is a deceptive forensic method. The computer or device will believe that the file is a different one once modification or transformation has been made. Changing the name of an mp4 file to make it appear like a.gif, for instance.

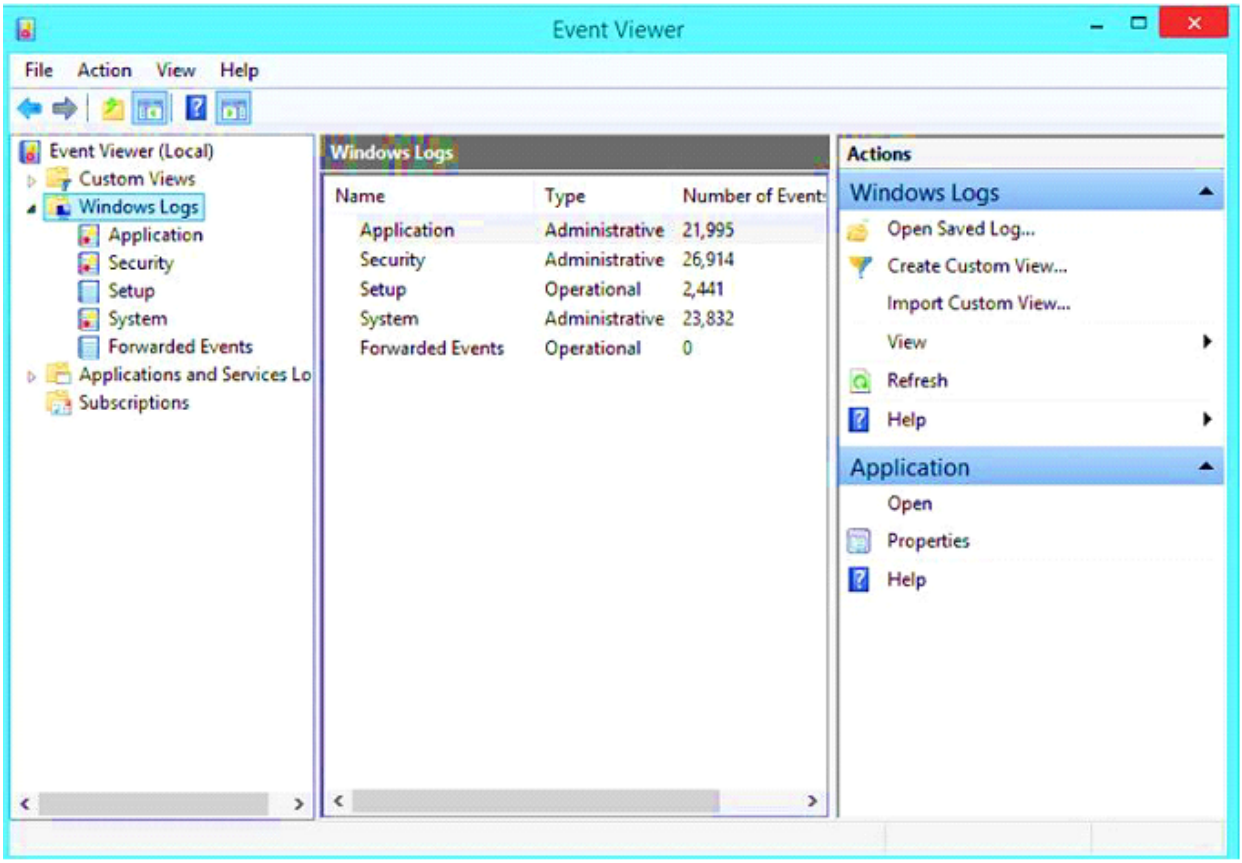
to locate moved or renamed files, forensic investigators typically rely on their experience and expertise. Additionally, we have information forensics techniques that can automatically check hard drives for unusual discrepancies. Data carving is an illustration of such a strategy. This

technique is employed to do a thorough and sequential scan of the material. Data carving works well because it can easily read low-level data from the media. It is independent of how the file locations and names are displayed on the file system. For instance, an mp3 file's identification is dependent on the actual data stream that it contains rather than the file's name.

The final security mechanism a hacker can use is encryption. Encryption is a headache in terms of digital forensics. By using a powerful encryption method, the data may become unreadable and so useless to the investigators.

Log Tampering

Log files are commonly saved in the event viewer on Windows-based PCs. It is simple to find using the "Search" bar. The /var/log directory houses the logs in the majority of Linux and UNIX operating systems.



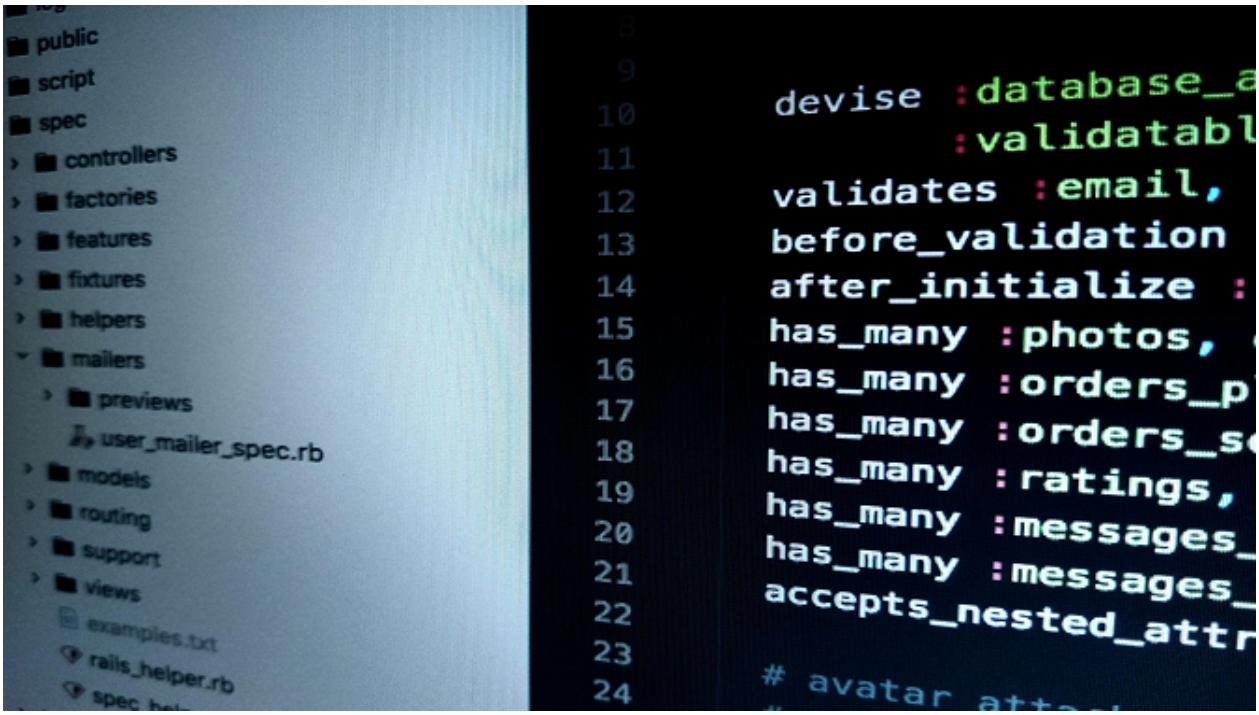
Simply by looking at the log files, system administrators can see any harmful activity that has taken place in their systems. There are two different kinds of log files: system- and application-generated log files. When manipulating logs, a hacker often has two choices. The logs can be deleted entirely in one method, and their contents can be changed in another. In order to prevent any signs of a cyber incursion from being seen, a hacker can also replace the system binaries with malware like Trojans.

Normally, it’s not a good idea to delete log files because doing so will leave a gap in the logs and raise questions. The detection of harmful actions can be done using the log files. They can serve as a method for alerts regarding the condition and actual state of a system. It’s possible that any anomalies in the records may attract unwanted attention. An astute attacker will probably launch his attacks when there is little chance that log data will be seen, such as on weekends or at night.

To tamper with the data in log files, an attacker would need root access. A hacker can change the log data related to their activity within the log file itself after increasing their level of privilege. Therefore, any investigation by a system administrator won't reveal any strange activities. Prudent system administrators typically configure their system so that all log files are sent to a distant server.

Being sneaky is one requirement for success, to sum up. Therefore, it is insufficient to avoid discovery while hacking. Even after the actual attack has been carried out, the procedure should continue.

Any errors are likely to trigger the radar detection, and the forensics team will be dispatched right away to locate the assailant. This suggests that the last stage of covering tracks is extremely important and shouldn't be taken lightly. Keeping a low profile is a crucial ability that you will need to possess if you want to hack into complex systems. We can claim that hackers use covert operations as a fail-safe method to keep them out of danger. The issue may arise right away or later, for example, during an investigation.



Chapter 4: Hacking Wireless Networks

Wireless Espionage

The use of wireless networking has various benefits. However, there are a number of risks and weaknesses that this type of technology has that hackers can exploit. Compared to wired connections, information is easier for hackers to intercept because it is transmitted over the air via radio waves. This is especially true if the data being delivered is not encrypted or if the encryption mechanism is insecure.

Basic components of wireless networks include:

- a wireless access point that connects to the network;
- data being broadcast over radio frequencies;
- and client devices, such as laptops, tablets, and other computing devices.

Users A hacker could focus on any one of these components to undermine at least one of the three main goals of a secure network, availability, integrity, or secrecy.

Attacks on wireless networks

1. Accidental hacking A wireless network could be hacked unintentionally. Sometimes wireless networks overlap, making it possible for any user to unintentionally enter a different network. This might appear innocent, but a bad hacker could exploit it to get data that shouldn't have been made available in this way. If the overlapping networks are

owned by businesses, the link can be exploited to steal confidential information.

2. Malicious Association When a malicious hacker uses their own device to enter a private network rather than the authorized access point (AP), the malicious association takes place. A “soft AP,” which a hacker can construct using software to trick a laptop’s wireless network card into thinking it’s an actual access point, is possible. This enables the hacker to send consumers Trojan horse programs, attack computers, and steal passwords.

Every computer that connects to the fictitious network is effectively under the hacker’s total control.

3. Ad-hoc Networks These networks connect two wireless computers together without an access point in between. Such networks rarely have effective defenses, making them very vulnerable to assault.

4. Non-traditional networks These include barcode readers, Bluetooth devices, wireless printers, and handheld PDAs. Since the focus is typically on laptops or access points, IT staff rarely safeguard these types of networks. They are therefore vulnerable to nefarious hackers.

5. MAC spoofing is a type of identity theft in which a hacker examines network traffic to determine which computer has access to the network. The goal is to obtain that computer’s network MAC (Media Access Control) address. Many wireless networks contain a MAC filter that restricts access to and use of the network to just certain computers with certain MAC addresses. To identify these permitted computers and their

IDs, a hacker may purchase software that can “sniff” the network. The hacker may then use this software in conjunction with other tools to enable the usage of these stolen MAC addresses on the hacker’s own computer.

6. Attacks by “Man-in-the-Middle”

This happens when a hacker tricks other users into using their laptop by setting it up as a soft access point. The hacker then uses a different wireless card to connect the soft access point to the real access point, making it necessary for users to pass through the false AP in order to access the real one. The hacker may now sniff out whatever information from the traffic they choose. Software like AirJack and LANjack have made this kind of assault simpler. This kind of attack works well on wireless hotspots because there isn’t any security on those networks.

7. Attacks known as denial of service (DoS) occur when a hacker repeatedly sends a large number of requests, commands, and messages to a single access point, either to cause the network to crash or simply to keep legitimate users from connecting to the network.

8. Network Injection Attack An access point that doesn’t filter traffic is attacked by a malicious hacker who injects phony networking reconfiguration commands into it. These bogus orders force a reboot or reprogramming of every networking device by taking down the entire network of switches, routers, and hubs.

Wireless Network Authentication Wireless networks are made to be accessed by any device that supports wireless. Because of this, passwords are typically used to secure networks. WEP and WPA are two widely used authentication methods.

In order to give users the same amount of privacy as wired networks, WEP, which stands for Wired Equivalent Privacy, was developed. It complies with IEEE 802.11 WLAN requirements. Data sent over a network is encrypted with WEP to prevent eavesdropping.

WEP design faults This type of authentication method has several serious design flaws:

1. In order to check the integrity of packets, it employs Cyclic Redundancy Check 32. The issue with CRC32 is that it only takes two packets to be captured for a hacker to get access to the network. In order to force the system to accept the packet, they can also change the checksum and encrypted stream.

2. It creates stream ciphers with an Initial Value (IV) and a secret key using the RC4 encryption technique. The secret key can be anywhere between 40 and 104 bits long, but the IV length is set at 24 bits. The network becomes more vulnerable to hacking if a secret key with a shorter duration is utilized.

3. A hacker can use a dictionary attack since it uses a password-based authentication method.

4. It lacks a central key management mechanism, making key changes in large networks extremely challenging.

WEP has lost favor and been replaced by WPA as a result of various security issues.

How to hack WEP networks

Passive attacks or active cracking can both be used to exploit the numerous security holes in a WEP network. The network traffic is not impacted by a passive attack until the WEP authentication has been broken. This makes it more difficult to find. Active cracking is more efficient but also more difficult to detect because it tends to put more strain on the network.

There are several tools available for breaking WEP, including Aircrack, a network sniffer that may be obtained from www.aircrack-ng.org.

Kismet – This versatile tool has the ability to sniff network traffic, find both visible and hidden networks, and even spot intrusions. WebDecrypt — It uses a dictionary attack to break WEP keys and produces its own keys. It can be downloaded from www.kismetwireless.net/ WEPCrack — This open-source utility can crack secret keys and can be downloaded from www.wepcrack.sourceforge.net/. Get it from www.wepdecrypt.sourceforge.net WPA Wi-Fi Protected Access is referred to by the acronym WPA. It was largely created to counteract WEP's shortcomings. WPA employs an IV that is 48 bits higher than WEP. Temporal keys are used to encrypt packets.

weaknesses in WPA

1. Denial of service attacks makes it simple for hackers to get around it.

2. Because its keys depend on passphrases, a dictionary attack can be conducted if weak passphrases are used.

How to break WPA networks

Because WPA relies on passphrases to verify user logins, it is susceptible to a well-coordinated dictionary attack, especially if short passphrases are employed. The following programs can be used to decode files that have been sniffed by other applications like Wireshark: Cain and Abel.

CowPatty is a program that uses brute force to break pre-shared keys. How to break network WPA and WEP keys can be downloaded from wirlessdefenc.org/Contents/coWPAttyMain.htm.

To unlock a wireless network, you will need the appropriate devices, software, and patience. The quantity of user activity inside the network you have targeted will, however, determine if you are successful in doing so.

Based on Linux, Backtrack is a fantastic security operating system. It has a lot of well-known tools that are excellent for gathering information, identifying vulnerabilities, and taking advantage of networks.

Metasploit, Ophcrack, Wireshark, Nmap, and Aircrack-ng are a few of these tools.

A wireless network adapter with packet injection capabilities is necessary for cracking network authentication keys.

•Download Backtrack OS from backtracklinux.com.

•Proximity to the network radius is org/downloads.

•enough understanding of the Linux operating system and the Aircrack routines.

•Have patience because there may be forces beyond your control.

Keep in mind that this will operate more quickly the more individuals actively using the network.

How to carry out MAC spoofing

You must get over the target network's MAC filtering in order to do MAC spoofing. MAC filtering is frequently used to prevent MAC addresses from connecting to a wireless network if they have not been given permission. This normally works well to block network access for anyone who might have obtained the password in some way. However, MAC filtering is ineffective as a security mechanism to keep hackers out.

You may easily spoof the MAC address of a client that is permitted to connect to the network by following the procedures below.

The monitoring mode of the Wi-Fi adaptor is required. The MAC address will be retrieved using Kali Linux's Airodump-ng program. Following that, the Macchanger program will be used to perform the spoofing, get over the filter, and establish a network connection.

Instructions:

1. Ensure that monitoring mode is selected on your Wi-Fi adapter. Enter the following command to discover the specified wireless network and any clients connected to it: Airodump-ng—c [channel]-bssid [target router MAC Addres]-l wlan0mon A window displaying a list of clients connected to the network will open. Their MAC addresses on their whitelist will also be displayed.

To access the network, you must spoof these addresses.

2. To fake your own address, choose one of the whitelisted MAC addresses from the list. Remove the monitoring interface first, then carry out the spoofing. Type Airmon-ng stop wlan0mon 3 into the command line. The following action is to disable the wireless interface for the MAC address you want to forge. Type ifconfig wlan0 down 4 into the command line. After that, you modify the address using the Mcchanger program.

Macchanger —m [New MAC Address] wlan0 is the command to enter. Keep in mind that in step 3, you have disabled the wireless interface.

It's time to bring it up again right now. Use the following syntax: ifconfig wlan0 up

Test to determine if the network will confirm your connection now that the MAC address of your wireless adapter has been updated to that of an authorized user. The wireless network ought to be accessible to you.

The three main risks from transmission hacking on wireless networks are disruption, alteration, and interception. You can employ signal-hiding techniques to stop malicious hackers from listening in on wireless transmissions. A malicious hacker must first find the wireless access point

in order to intercept wireless broadcasts. A company can make this more challenging by turning off the SSID (service set identifier) that the access point is broadcasting, giving the SSID a mysterious name, reducing signal strength to provide only the necessary coverage, or positioning access points away from exterior walls and windows. There are also more advanced but more expensive methods, such as using TEMPEST (a method to prevent the emission of wireless signals) or directional antennas to confine the signal to a certain area.

Stronger encryption of all wireless traffic — This is crucial, especially for businesses that need to safeguard the privacy of their data being transmitted wirelessly. The likelihood of a man-in-the-middle assault is decreased by this measure.

Stronger authentication processes – Both users' devices and users themselves should be covered by this. Man-in-the-middle assaults are reduced as a result.

Countermeasures against Denial of Service Attacks

Although malicious hackers may occasionally try to take down an organization's servers, a DOS attack may occasionally be accidental. To reduce the dangers of this type of assault, the following actions can be taken:

doing thorough site surveys to locate signals coming from other devices. When determining where the access points should be placed, consider this as a guide.

conducting routine audits of network activity and performance to identify trouble spots. If there are any disruptive devices, they need to be taken out. Additionally, steps should be taken to improve signal strength and coverage in troubled areas.

Wireless access points that are improperly set up provide a serious vulnerability and may give hostile hackers unauthorized access to sensitive data. The following countermeasures must be implemented in order to secure wireless access points: Get rid of any rogue access points – Using 802.11i is the best approach to accomplish this. Ix to stop unauthorized devices from connecting to the wireless network via the USB port.

Make sure that all valid access points are correctly set up. Since default settings are made available to the public, hackers can easily take advantage of them.

Use 802.11 to authenticate each device. Strong authentication measures in the Ix protocol will stop unauthorized devices from installing backdoors. Prior to giving any device an IP address, this protocol makes sure that strict authentication is ensured.

Devices There are two ways to evaluate security risks posed by wireless devices: theft/loss and compromise.

Since laptops and PDAs frequently contain important and secret data, they must be secured against theft and loss.

When a malevolent hacker gains access to the device's data storage, wireless client devices are also susceptible to intrusion. The tool can be used by hackers to attack other networks and systems.

The most effective method for securing a wireless network is network encryption.

The majority of base stations, access points, and wireless routers have built-in encryption algorithms that allow network traffic to be scrambled. Make sure the router you purchase has an encryption feature at all times. Make sure to manually activate this option before using your router since most manufacturers leave it off.

Make sure your wireless network is safeguarded the same way a cable connection is by installing anti-spyware, anti-virus, and firewall software. Keep all of your software up to date, and make sure your firewall is constantly turned on.

Turn off your router's identifier broadcasting. A wireless router utilizes this feature to announce its presence to nearby devices. However, if people are already aware of a network, there is no need to make an announcement about its existence. Malicious hackers frequently look for broadcast identification to narrow focus on potential targets.

Change the default identifier — The manufacturer of each router assigns it a default ID. Even if you have the identifier broadcaster turned off, hackers can still target the network if they know the default ID, which is made available to the public.

Don’t forget to configure the new ID into your computer after changing the identifier.

Alter the default password — The manufacturer assigns a default password to each router. This is for initial device configuration reasons. Because it’s simple to locate these default passwords, be sure to change your router’s password to something far more difficult to guess. Make an effort to extend the length of your password as well.

Establish the devices that are permitted to connect to the network – Set your router to only permit connections from certain Mac addresses. Do not, however, rely solely on this method because Mac spoofing is still a possibility.

When not in use, turn off any wireless networks. Ensure that any wireless networks are turned off when not in use.

As a the window of opportunity that hackers have to break into the network will be reduced.

Be cautious in Wi-Fi hotspots – Most people like using free Wi-Fi at hotels, airports, and other public locations. Do not assume that these wireless networks are safe as this is rarely the case.

The Users Educating and training every user is the best way to secure a wireless network. Users include not just those who connect to the network but also administrators and IT staff. Teaching individuals appropriate behavior is crucial to maintaining the wireless network’s security. This user education and training must be a recurring project.

Let’s not hide it. It is impossible to totally remove all dangers associated with wireless networks. A hacker will eventually succeed.

A decent level of general security can be maintained, nonetheless, by taking certain steps. Using methodical risk appraisal and management procedures, this is feasible. When developing defenses against malevolent hackers, every aspect of a wireless network must be taken into account.

Chapter 5: Kali Linux Uses and Applications

Kali Linux has several applications. I've listed and discussed a few of them below. You are welcome to obtain the documentation from the Chapter 2 links. Let's now get to the important things.

Testing for penetration

Organizations use this approach to evaluate the reliability of their security infrastructure. In this scenario, security experts will assume the role of attackers and work to identify system faults and vulnerabilities before the nefarious individuals do. Finding and reporting vulnerabilities to businesses and organizations is one of the main goals. Many large firms are starting to outsource security services as organizations grow more security concerned and the cost of security breaches climbs significantly. Penetration testing is one of these vital security services. A penetration test is essentially a legitimate hack that is ordered to show how vulnerable a company's network and systems are.

In order to identify any potential vulnerabilities in their network, operating systems, and services, businesses typically start by conducting a vulnerability assessment. I put the word "potential" in quotes since there were a lot of things that were recognized as vulnerabilities but weren't, according to this vulnerability scan. The penetration tester's job is to make an effort to exploit these vulnerabilities. Only then can the company decide whether to spend time and money to close the vulnerability and determine whether the weakness is real.lo

military and espionage

Cyber espionage is the act of gaining access to information and trade secrets without the consent or knowledge of the targets. They could be common people, adversaries, rivals, rival groups, governments, or even enemies. These goals are rather general. They may have a military, political, economic, or even personal component. Diverse approaches are also employed. To accomplish their stated goals, hackers might utilize a variety of tools, including malicious software, cracking techniques, and proxy servers. Professionals can conduct espionage online from their workstations, or it can be done through infiltration utilizing trained moles and traditional spies. It may occasionally be carried by novice programmers and hackers who have malevolent intentions. It is well known that every country on the planet engages in clandestine cyber espionage or even cyberwarfare. Hacking has increased the efficiency of gathering intelligence about foreign military operations. Therefore, a hacker will have it tough in any country's protection systems.

Forensics: Forensic Linux Live Boot environments have grown in popularity over the past few years. This distribution contains a large number of forensic tools that are based on Linux. With Kali, forensic experts may perform all tasks associated with their trade, from initial triage and data imaging to case administration and thorough analysis.

Reverse engineering: Recently, this talent has become essential in many fields, including law enforcement. One of the main techniques for locating weaknesses and creating exploits is reverse engineering. On the offensive end of things, that is.

Reverse engineering can be used to analyze malware that has been used to attack a specific system defensively.

Here, determining a piece of tradecraft's capabilities will be the main goal.

Wireless Attacks: A wide variety of wireless hacking tools are supported by Kali. Wireless networks are widely used, which makes them a frequent target for attacks. A hacker's preferred option for launching attacks against various wireless network types, Kali Linux also supports a variety of wireless devices.

Password assaults: Where a user comes across an authentication system, Kali Linux can be used to conduct password assaults. Numerous helpful tools and utilities are included with the OS for this reason. For dealing with hashing and encryption systems, Kali Linux users have access to both offline and online password assault tools.

Database Evaluation: Kali Linux is capable of conducting database attacks like SQL injection and credential stealing. The tools available in Kali's extensive repository, which can be used to test attack vectors ranging from data extraction and analysis to SQL injection, make all of this possible.

Again, Kali Linux contains a ton of tools that a skilled hacker or aspiring one can use to access data as it is being transferred over the network, including tools for sniffing and spoofing. If you want to acquire and evaluate data that has just been captured, you can use sniffing tools after using spoofing tools to pretend to be a network's authorized user.

When used in conjunction, these tools are deadly.

Stress Examining

You run a stress test on your system to see if it is stable. In this case, you'll create more traffic than usual by using the many options Kali Linux offers. You will be able to understand the limitations of your system in this way. The tools used for stress testing might either be closed-source or proprietary. Knowing every instrument used to test the availability of a system is a need for an expert.

Hardware theft

Hardware hacking is another way Kali Linux is used. The following tools are included with Kali Linux and can be used for this task.

The Android SDK gives you the API libraries and developer tools required to create, test, and debug Android apps.

A tool for reverse engineering locked, binary, third-party Android apps is called apktool. It allows for the step-by-step debugging of Smali code and can decode resources to almost their original form before rebuilding them after certain alterations. Additionally, the project-like file structure and automation of some repetitive operations, such as creating apks, etc., make using the program easier.

Arduino is an open-source platform for electronic prototyping. It is founded on adaptable, simple-to-use hardware and software.

Sakis3G: Sakis3G is a modified shell script that should automatically establish a 3G connection with any operator or modem combination. Your USB or Bluetooth modem is automatically configured, and it might even detect operator settings. When everything else fails, give it a shot.

Smali is an assembler/disassembler for the dex format used by dalvik, the Java VM implementation used by Android.

The syntax supports all of the dex format's features, including annotations, debug information, line information, etc. It is roughly based on Jasmin's/dedexer's syntax.

Chapter 6: Introduction to Cybersecurity

We define cybersecurity as the defense against digital attacks on computer networks, computer systems, and the programs connected to them. Cyberattacks are frequently conducted with the aim of obtaining access to, altering, or even destroying sensitive information. They aim to disrupt a company's regular operations and also attempt to extort money from its victims.

Confidentiality, availability, and integrity

The phrase "CIA triad" is often used to refer to the trio. It can be characterized as a model meant to direct information security policy within a certain organization. We sometimes refer to the triad as the AIC triad to avoid confusion with the American Central Intelligence Agency. The three components are the most important ones for security. In our situation, we can say that availability is defined as a guarantee of dependable access to information by individuals with authorization, confidentiality is said to be a set of protocols used to restrict access to information, and integrity is the undertaking given to demonstrate that the information at hand is both accurate and reliable.

Confidentiality:

This roughly equates to privacy. It is necessary to take serious precautions to ensure that there is secrecy while ensuring that the appropriate individuals may access crucial information. The data in

question should only be accessible by those who are allowed to see it. It is common practice to categorize data according on the kind and scope of harm that could arise from it getting into the hands of unauthorized individuals.

Depending on these categories, strict measures can be used in certain cases and not in others. For those who are authorized to view or use the data, specialized training may be necessary to protect its secrecy. Security concerns that might affect that information are typically present. Without a doubt, it can aid those with the required authorization in learning about the numerous risk elements and preparing them with defenses. The training may also cover social engineering techniques and best practices for password-related issues.

Even if they may have motives that we may define as altruistic, this will assist them avoid violating laws controlling data processing, which could have terrible repercussions. For instance, one excellent way to guarantee confidentiality is to utilize a routing number or an account number. To ensure that there is confidentiality, we can also use data encryption. The typical technique of two-factor authentication, which is becoming increasingly popular, includes passwords and user IDs. There are various choices. They consist of biometric authentication and security tokens (sometimes known as soft tokens or key fobs).

Additionally, it is the users' responsibility to exercise caution in order to limit the number of times and locations where their information must be sent in order to complete a transaction. When we have important data, more precautions can be required. Such efforts could entail keeping the data on air-gapped computers with unconnected storage devices, or even just keeping hard copies of it.

Integrity:

This part of the triangle is making sure that data is reliable, consistent, and accurate over its entire life cycle.

The integrity of data while it is in transit must be maintained at all costs.

Effective measures must be made to prevent unauthorized individuals from altering the data. For instance, when there is a breach of confidentiality. User access restrictions and file permissions can be used as countermeasures in this case. Version control can be used to avoid inadvertent deletion or incorrect changes by authorized users. Mechanisms must be in place to aid in the detection of data changes that may be caused by non-human events, such as a server crash or an electromagnetic pulse. Checksums and cryptographic checksums can be used to aid in the data integrity verification process. Finally, it could be required to include redundancies and backups of some kind to aid in the restoration of the system to its prior state.

Availability:

The consistent upkeep of all the hardware guarantees that the services provided by it will always be available.

To maintain a stable operating system environment free of any software conflicts, failing equipment should be fixed immediately and adequately. The update of all essential system components is another aspect of maintenance that should be done. Additionally, it will need to

ensure that communications have enough bandwidth and that blockages are rare.

High-availability clusters, redundancy, RAID, and even failovers can be used to mitigate the effects of hardware failures.

Disaster recovery that is both quick and flexible is crucial for worst-case scenarios. The established catastrophe recovery strategy must be thorough in order for this to be feasible.

Unpredictable events must be taken into account while preventing data loss or connection lapses. Natural calamities and fire are a couple of such examples. To prevent data loss as a result of such events, backup data copies can be safely kept at a geographically remote site. These locations also need to be fire and water resistant. We can utilize additional security equipment, such as proxy servers, firewalls, and software, to prevent problems like network intrusions, downtime, and data inaccessibility caused by denial-of-service assaults.

Concerns related to the CIA

Big data presents significant challenges to the CIA paradigm. This is primarily due to the enormous amount that needs to be protected, the variety of data formats, and, lastly, the abundance of the sources from which the data originated. Duplicate data sets and disaster recovery plans all drive up the already high cost.

Since gathering data and using it to create some form of meaningful interpretation is big data's primary goal, oversight is sometimes inadequate as well. We are all familiar with the man, Edward Snowden, who made this problem public. Across the globe, security agencies acquire a vast amount of personal information on individuals. We have unique considerations known as the Internet of Things privacy to protect personal information from exposure in the IoT ecosystem. To enable autonomous communications over a network, including the Internet, practically every logical or physical entity can be given a special identifier.

It's not always the case that the transferred data from a certain endpoint leads to privacy problems. The problem is that sensitive data can be retrieved when the fragmented data from several endpoints are accessible, collated, and analyzed. The Internet of Things, which includes many other Internet-enabled devices besides computers, presents a significant security risk in and of itself. These devices are frequently configured with weak default passwords, or they may even be unpatched in some circumstances. IoT might either be used as a separate attack vector or integrated into a thingbot if it isn't appropriately safeguarded. In recent times, researchers have shown that all it takes to compromise a network is the use of a Wi-Fi light bulb. We must take into account the security of the many network-capable products that are now being developed.

Encryption

As a mechanism for converting plaintext or other data types from their currently readable form to an encoded one, encryption is what we refer to as. The data can only be decoded by a party with access to a decryption key. This crucial step is typically taken to offer complete data protection across networks.

On the internet, encryption is frequently employed as a preventative security measure to safeguard sensitive user data that is transferred between servers and browsers. Private data including payment information, passwords, and other personal data are examples of what may fall under this category. Encryption is a security measure that can be used by both individuals and businesses to protect sensitive data that is kept on computers, servers, and mobile devices.

How to use encryption

A combination of an encryption algorithm and an encryption key is used to encrypt plaintext data, sometimes referred to as unencrypted data.

This produces a ciphertext that can only be seen in its original form when decrypted with the right key. Decryption, on the other hand, is the opposite of encryption. The procedures for encryption are carried out backwards. There are two encryption algorithms that are widely utilized in the present era. Both symmetric and asymmetric encryptions are used.

A single key is used for encryption when using the symmetric encryption process. Among symmetric-key ciphers, the Advanced Encryption Standard (AES) is frequently employed. Its main purpose when it was designed was to safeguard governments' secret information. In comparison to asymmetric encryption, this approach is quicker. The recipient must, however, have access to the sender's encryption key.

A secure method of key management is required. Most of the time, this use an asymmetric algorithm.

On the other asymmetric cryptography is available. Additionally, it is known as public-key cryptography. Here, two distinct keys are employed. However, they are mathematically related. The keys are as follows, with one being private and the other being public. The public key can frequently be distributed to everyone. It is required to keep the private key private. The RSA encryption algorithm is one that is frequently used in asymmetric cryptography. The two keys can, to some extent, encrypt a message, which implies that the key required to decrypt it is the opposite of the key used for encryption. With the use of this function, we can make sure that electronic conversations and data are authentic, unreliable, and intact in addition to being confidential.

Gains from Encryption

Encryption safeguards the confidentiality of digital data that is stored on computer systems or transmitted over the internet or any other computer network. Sensitive data must be encrypted, according to organizations like Payment Card Industry Data Security Standard (PCI DSS), in order to prevent unauthorized parties from accessing the information. Additionally, there are several standards that suggest or call for data encryption. Today's encryption algorithms play a crucial part in ensuring that communications and IT systems are secure and possess the following critical security characteristics in addition to confidentiality:

- Authentication: A message's origin should be able to be confirmed.

- Integrity: This has to do with maintaining the integrity of the message. In other words, since a message was sent, its contents have not been changed or removed.

•Non-repudiation: In this context, non-repudiation refers to the inability
of a specific sender to deny sending the communication.

Protection and redundancy

In most cases, we use backup, where copies of the data are made in case of a severe loss. However, redundancy encompasses much more than just data storage. Redundancy attempts to maintain service levels no matter what happens. Data redundancy makes ensuring that data is stored in a variety of different places. We also have a concept known as “network redundancy” in which a network is set up with a lot of backup systems. No matter what happens, the alternate systems maintain service continuation.

Redundancy in Data

First and foremost, it is crucial for any firm to quickly resume regular operations following a security compromise.

As soon as feasible, data should be able to be rebuilt. Businesses have developed a number of strategies to ensure data redundancy as a result. It is widely recognized that these techniques have advantages in terms of cost-effectiveness, speed, and management. The most typical method is to use off-site tape backups. This technique stores a complete bit-for-bit replica of a storage volume on magnetic tapes. The tapes can be moved to an off-site storage location where they are conveniently accessible in the event of a catastrophic failure. Additionally, we can employ cloud backup to protect data from losses.

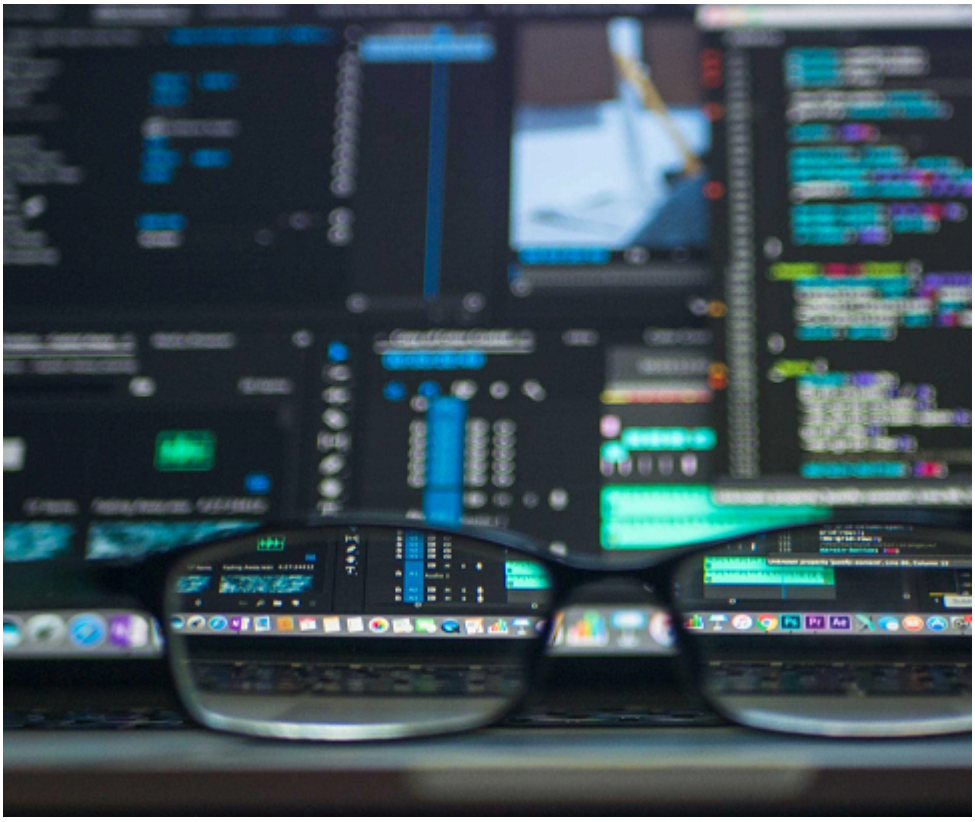
System Redundancy

The majority of the infrastructure that supports our networks is incredibly unstable. For instance, if a router burns out for any reason, the network will be unavailable for an extended length of time. Businesses take precautions to mitigate this by ensuring that the networks they utilize have sufficient redundancy so that they can function and offer services in an emergency.

Network redundancy essentially means that a network will continue to function no matter what kind of failure takes place. We can accomplish this by configuring additional network devices, such as hubs, routers, and switches, to take the place of a failing one. We also have ISP redundancy, when a network gateway is connected to multiple distinct ISPs. One ISP will take over anytime there is a failure, just like with the devices. When a network is operating well, we can use the ISPs to share the traffic, which reduces network congestion. This is referred to as load sharing.

preventing a single point of failure from occurring. We do not want a system to become completely inoperable due to the breakdown of a single crucial component. Any strategy must reduce this occurrence. Redundancy can decrease or even get rid of a single point of failure.

This will ensure that no one element can interfere with a system's correct operation.



Chapter 7: Network Management and Scanning

The key to being a good hacker is having the capacity to search for and connect to other network devices from your system, and with wireless technologies like WiFi and Bluetooth becoming the norm, being able to locate and manage WiFi and Bluetooth connections is essential. A wireless connection can be hacked, giving an intruder access to a device and private data. Of course, learning where to discover these devices is the first step. The two most popular wireless technologies in Linux that we will be looking at in this chapter are WiFi and Bluetooth.

Network scanning

As the name suggests, is the process of using a computer network to gather data on IT systems. We perform network scanning primarily to assist with system maintenance or a security evaluation. Before starting an attack, hackers might also perform a network scan.

Some of the reasons we scan networks

•Identifying the current TCP and UDP network services, which may be running on the targets.

•to learn about the filtering systems that lie between the user and the targeted hosts.

•By examining their IP answers, determine the OS systems that are being used.

•Analyze a specific host that is being targeted for its TCP sequence number predictability. This will enable attack sequence prediction and TCP spoofing.

Vulnerability scanning and network port scanning are the two main components of network scanning. The latter refers to a method of transmitting data packets through a network to a system's unique port numbers. Finding network services that are present in that specific system is the aim. It is a great approach to identifying problems with a certain system. In this manner, the issues can be resolved and the system's security is ensured. We utilize a technique called vulnerability scanning to find known flaws in network systems. Weak points in the operating system and application software can be found using it. These vulnerabilities are typically used to infiltrate computer systems.

Network port scanning and vulnerability scanning can both be referred to as information-gathering strategies. On the other hand, when they are used by unidentified entities, they can represent a precursor to an attack. These entities typically have bad motives. Another method for network scanning is inverse mapping. It is helpful for gathering IP addresses that are not associated with active hosts. By doing this, it will help in directing attention to addresses that are important to pay attention to—that is, those that are realistic.

There are three steps that can be taken to obtain information.

The second stage of footprinting. the third stage of scanning. This suggests that network scanning is one of the essential stages an attacker must do in order to be able to acquire information.

Ifconfig is a crucial tool for inspecting and dealing with active network interfaces, and it can be used for network scanning.

By typing ifconfig into the terminal, you may use it to check the status of your active network connections.

Using the ifconfig command to Scan Wireless Networks

If you have a wireless adapter, you can use it to obtain vital data for wireless hacking, like the adapter's IP address, MAC address, what mode it's in, and more. When using wireless hacking tools like aircrackng, the information you can learn from this command is quite crucial.

Changing your network information

Being able to modify your IP address and other network information will allow you to access other networks while presenting yourself as a reliable device on those networks, which is an important skill. For instance, you can spoof your IP in a denial of service (DoS) attack to make it appear as though the attack is coming from a different source, enabling you avoid having your IP captured for forensic analysis. The ifconfig command is used in Linux to complete this rather easy process.

Changing Your IP Address

Type ifconfig, the interface you wish to reassign, and the new IP address you wish to be allocated to that interface to change your IP address. For instance, to give interface eth0 the IP address 192.168.181.115,

you would type:
Kali >ifconfig eth0 192.168.181.115

kali >

If you did this successfully, Linux will return to the command line and say nothing. This is advantageous! Following that, you should see that your IP address has changed to the new IP address you just assigned when you check your network connections once again using ifconfig.

Changing Your Network Mask and Broadcast Address

The ifconfig command also allows you to alter your network mask (netmask) and broadcast address. For example, you would input the following if you wanted to give the same eth0 interface the netmask 255.255.0.0 and the broadcast address 192.168.1.255:

Kali >ifconfig eth0 192.168.181.115 netmask 255.255.0.0 broadcast 192.168.1.255
kali >

Again, assuming everything went according to plan, Linux will reply with a fresh command prompt. Enter ifconfig once more to confirm that all of the options have been adjusted correctly.

Spoofing Your MAC Address

You can also modify your MAC address using the ifconfig command. Because it is globally unique, the MAC address is frequently employed as a security mechanism to prevent hackers from accessing networks or

tracking them down. It’s almost simple to change your MAC address and impersonate a different MAC address, which defeats those security procedures. As a result, it serves as a useful tool for getting around network access controls. Use the down option of the ifconfig command to shut down the interface (in this case, eth0) in order to fake your MAC address. Next, type the ifconfig command, followed by the name of the interface (hw for hardware, ether for Ethernet), and the newly created fake MAC address. In order for the modification to take effect, you must finally bring the interface back up using the up option.

IP Addresses Assignment Linux has a DHCP (Dynamic Host Configuration Protocol) server that executes a daemon, a background process, known as dhcpd or the DHCP daemon. All of the systems connected to the subnet will have their IP addresses assigned by the DHCP server. Additionally, it maintains track of which machine is currently assigned which IP address in a log. This makes it a valuable tool for forensic investigators to identify hackers following an attack. Because of this, it’s helpful to comprehend how the DHCP server functions. Usually, you need a DHCPassigned IP in order to connect to the internet from a LAN.

you must come back and obtain a new DHCP-assigned IP address after setting a static IP address. You could always reboot your PC to accomplish this, but I’ll teach you a different method of getting a fresh DHCP without doing so. All that is necessary to request an IP address through DHCP is a dhclient call to the DHCP server, followed by the interface to which you want to give the address. Different DHCP clients are used by various Linux distributions. For instance, Kali utilizes dhclient and is based on Debian.

Hackers can find a wealth of information about a target by manipulating the Domain Name System (DNS) of that target. Although it's intended to convert domain names to IP addresses, this essential component of the internet can also be used by hackers to gather information about their targets.

A domain name like google.com is translated to the correct IP address using the dig DNS service. Your system will know how to access it this way. Without DNS, we would have to keep track of the tens of thousands of IP addresses that are associated with the websites we routinely visit. One of the commands that any aspiring hacker should know is to dig. It provides a means to compile DNS data on a target domain. Before attacking, obtaining the DNS storage data might be a vital part of early reconnaissance. This information can comprise the target's email server's IP address, nameserver (the server that converts the target's name to an IP address), and possibly any subdomains. By including the mx option (short for mail exchange server), you can also use the dig command to learn more about the email servers associated with a domain. Attacks against email systems require this information to be available.

Changing Your DNS Server

There may be times when you need to utilize a different DNS server. You will achieve this by making changes to the system's /etc/resolv.conf plaintext file.

In a text editor, open that file. After that, on your command line, type the exact name of your editor, followed by the file's location and name.

Let's start by taking a look at WiFi networks. Here is a brief introduction to the various WiFi security protocols that are typically utilized before doing so. Wired Equivalent Privacy (WEP), the original, had serious flaws and was easily breached. WiFi Protected Access (WPA), which took its place, was a little bit more secure. Finally, almost all WiFi APs (with the exception of enterprise WiFi) now use WPA2PSK, which is far more secure and employs a preshared key (PSK) that all users share.

Basic Wireless Commands

ifconfig

In Unix-based operating systems, ifconfig is required to configure a network interface. The system contains this tool for administration. Ifconfig offers tools that are used for configuring, exploring, and managing the TCP/IP interface's parameters. Ifconfig can be used as an interactive tool to display and examine network interface settings.

In conclusion, ifconfig performs the following tasks: enabling the viewing of network settings; carrying out the enabling and disabling of a network interface; allocating a broadcast to a network interface; assigning an IP address, a netmask, and a broadcast to a network interface; and changing the MTU for a network interface.

Altering the MAC address of the network interface; turning on and off promiscuous mode; adding and removing new aliases from the network interface.

RTNetlink socket-received wireless events are shown via the iwevent command. Each line displays a unique Wireless Event that details what

occurred on the chosen wireless interface. The arguments for this command are not accepted.

The iwlist command can be used to search for wireless networks that are available and to display any further information about the wireless networks that the iwconfig command does not display. Iwlist is used to generate a list of neighboring wireless access points, together with their SSIDs and MAC addresses.

iwspy

This command is used to keep an eye on network nodes. It can also be utilized to monitor the nodes' link quality.

Using a variety of static criteria to assign names consistently to each interface, the ifrename command is used to rename wireless network interfaces. Typically, interface names are dynamic by nature. This command aids users in selecting the network interface's name.

This is used to report the NWID, ESSID, or address of the wireless network's access point that is currently in use. The devices' ESSID will be shown by iwgetid by default. If it isn't available, it will output its NWID in its instead. The data supplied matches the data displayed by iwconfig. In contrast, integrating into different scripts is simpler.

Identifying and using Bluetooth Nearly all modern gadgets, systems, and devices come equipped with Bluetooth. Computers, iPods, smartphones, speakers, game controllers, keyboards, and tablets are just a few examples of the gadgets that can be used. If a device is controlled and

a platform is acquired to send privileged information from and to the device, among other things, the ability to break into Bluetooth networks can result in the compromise of the information on the device. Therefore, in order to fully utilize Bluetooth, we must comprehend how it operates.

You can learn some fundamental skills from this book that will be helpful while scanning for and connecting to Bluetooth devices in order to hack them.

How Bluetooth Works

Bluetooth is a wireless communication technology that allows for the wireless transmission of audio or data between devices.

This occurs over a fairly small area. This technique was developed to take the place of the commonplace cables that were used to link gadgets while maintaining the security of the communications between them. Pairing is the process of connecting two Bluetooth devices. If two devices are in a discoverable mode, they can almost always pair. A Bluetooth device will broadcast the following details about itself when it is in the discoverable mode: Technical information Name List of services Class When two Bluetooth devices pair, they exchange a link key. In order to identify the other device during subsequent pairings, the devices will save the key. Every gadget has a distinctive identity and typically a name given to it by the manufacturer. When we wish to locate and access a gadget, these will be helpful pieces of information.

We will search for Bluetooth signals using BlueZ, an implementation of the Bluetooth protocol stack provided by the Linux program Bluetooth

Scanning and Reconnaissance. The majority of Linux distributions, including Kali Linux, come with it as a standard feature out of the box. BlueZ has tools that can be used to manage and scan Bluetooth-capable devices. The utilities are illustrated by the following examples: hciconfig, a Bluetooth-specific version of Linux's ifconfig.

We utilize a tool called hcitool to do inquiries. The device's name, class, ID, and even its clock information may be requested. This makes the devices more synchronized.

hcidump: Since this tool does Bluetooth communication sniffing, it enables us to record data that is being transmitted via the Bluetooth signal.

Checking whether the Bluetooth adapter on the system we are using is recognized and enabled allows us to utilize it to scan for other devices as the first scanning and reconnaissance phase with Bluetooth.

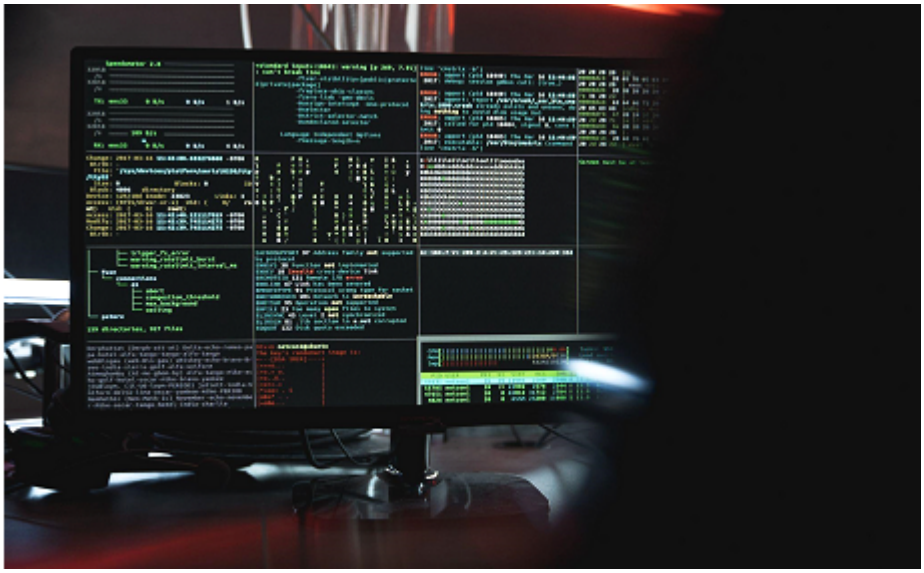
Using hcitool to Scan for Bluetooth Devices

Now that we are aware that our Bluetooth adapter is operational, we can use hcitool, a different BlueZ suite tool, to search for nearby Bluetooth devices.

We can identify Bluetooth devices that are communicating using their discover beacons by using the straightforward scan command. In other words, the gadgets in discovery mode. You will most likely come across Bluetooth hacking tools that use these commands in a script. These commands should allow you to build your tools using Python or even bash script.

The service discovery protocol, or SDP as it is more commonly known, is a Bluetooth protocol used to search for Bluetooth services (Bluetooth is a suite of services). BlueZ kindly offers the sdptool tool for browsing a device for the services it offers. It's also crucial to remember that the device need not be in discovery mode in order to be scanned. Following the collection of the MAC addresses for all nearby devices, we can use l2ping to send pings to these devices to see whether they are reachable, regardless of whether they are in discovery mode. The syntax is as follows: sdptool browses MACaddress. This enables us to determine whether they are present and active. The l2ping command, with the syntax: l2ping MACaddress, is used to transmit a ping. Wireless gadgets are the future of communication and hacking.

In order to scan and connect to Wi-Fi APs, Linux has created specialized commands. This is the first step in hacking those systems. The wireless hacking tools in the aircrack-ng package, airmon-ng and airodump-ng, allow us to scan and acquire crucial data from in-range wireless devices. The BlueZ suite comprises hciconfig, hcitool, and other information-gathering tools that are necessary for scanning and hacking Bluetooth devices nearby. There are other additional tools that are worth investigating.



Chapter 8: Web Security

Web Safety

Web apps and websites are equally susceptible to having their security systems and protocols broken as are real stores, houses, and government buildings. Strong and trustworthy security measures are required to combat cybercrimes and the compromise of web applications.

This is exactly what web security does. A practical definition of web security for us would be that it is a collection of protocols and safety measures used to secure your website and online apps from hacking and unauthorized personnel entering your system without authorization. Web services, websites, and web apps can all be protected by the essential division of information security.

This offers essential security for anything done on the Internet.

there are a number of factors to take into account while discussing web protection and/or web security. An online application or website must be supported by a number of methods and checkpoints to ensure its security in order to be deemed secure. We always have security requirements that must be met. These standards are to be highlighted and put into practice by OWASP. Experienced web developers usually follow OWASP guidelines and pay close attention to the Web Hacking Incident Database in order to understand the vulnerabilities that result in website hacks and how they happen.

common dangers to website security

Websites can come under assault in a variety of ways. We must first comprehend some typical dangers to the security of websites before moving forward.

During the planning of security measures, we will try to prevent these and be ready for them. Among many more, some of the issues include spam, malware and viruses, WHOIS domain registration, and DDoS attacks.

How to make your website secure

Let's now concentrate on how to prevent typical security threats after learning about them. It is incorrect to assume that your website is secure. There is a good probability that it can be assaulted if you have not put in place any protective measures. You must take the following actions to increase the security of your website:

limits on file uploads

Allowing users to upload files to your website is dangerous. The uploads can include a script designed to take advantage of holes in your website. Every upload must be viewed as a potential risk to the website's security.

using the HTTPS protocol

This signals to website visitors that they are, in fact, working with a reliable server. The literal translation of this is “no one can intercept the interactions they are having or the content they are viewing.”

Safeguard your computer.

With you, security begins! It is crucial that you maintain your devices’ security. Your computer may be used by hackers as a portal to your website. Make sure your antivirus program is current with definition updates. This will shield you from a variety of malicious attacks, including those that come from file downloads. Malware can potentially be injected into websites using stolen FTP login information. It’s crucial that you constantly scan your devices for viruses and spyware.

Modify your CMS’s default settings.

We have observed that many attacks today are typically automated. Bots are created by malicious individuals to assist them find websites that are still utilizing their default settings. Create obstacles for them. When installing a CMS that you own, change any default settings that are present:

Settings for comments, User-required Controls, Information Visibility, and File Permissions

You can immediately change the parameters listed above.

program upgrades

The software must always be current. This covers, among many other things, the CMS, plugins, and Word Press software. The updates provide enhanced functionality, security patches to close security holes, bug and software glitch repairs, and other improvements.

Choose a secure web hosting package

Shared web hosting packages are more likely to be compromised. Although the potential cost savings make them enticing to users, the levels of security are decreased. They are not a safe choice as a result. Don't forget: cheap is dear!

User access restrictions

The bulk of cybersecurity threats are the result of human error. Reducing or limiting the number of humans can significantly help with error reduction. Not every employee has to have access to your website. Visitors, web designers, and consultants are all ineligible for automatic access. To secure your website, the least privilege concept must be used.

Change your password.

Changing passwords often is a big boost for web security.

Change your password, then. Making a habit of regularly changing your password is far more important than simply changing it once.

Check your security.

Online, you can find tools to help you keep an eye on the security of your websites. These tools can assist you in conducting security audits, which can help to identify potential weaknesses. By doing this, you can start countermeasures prior to an assault.

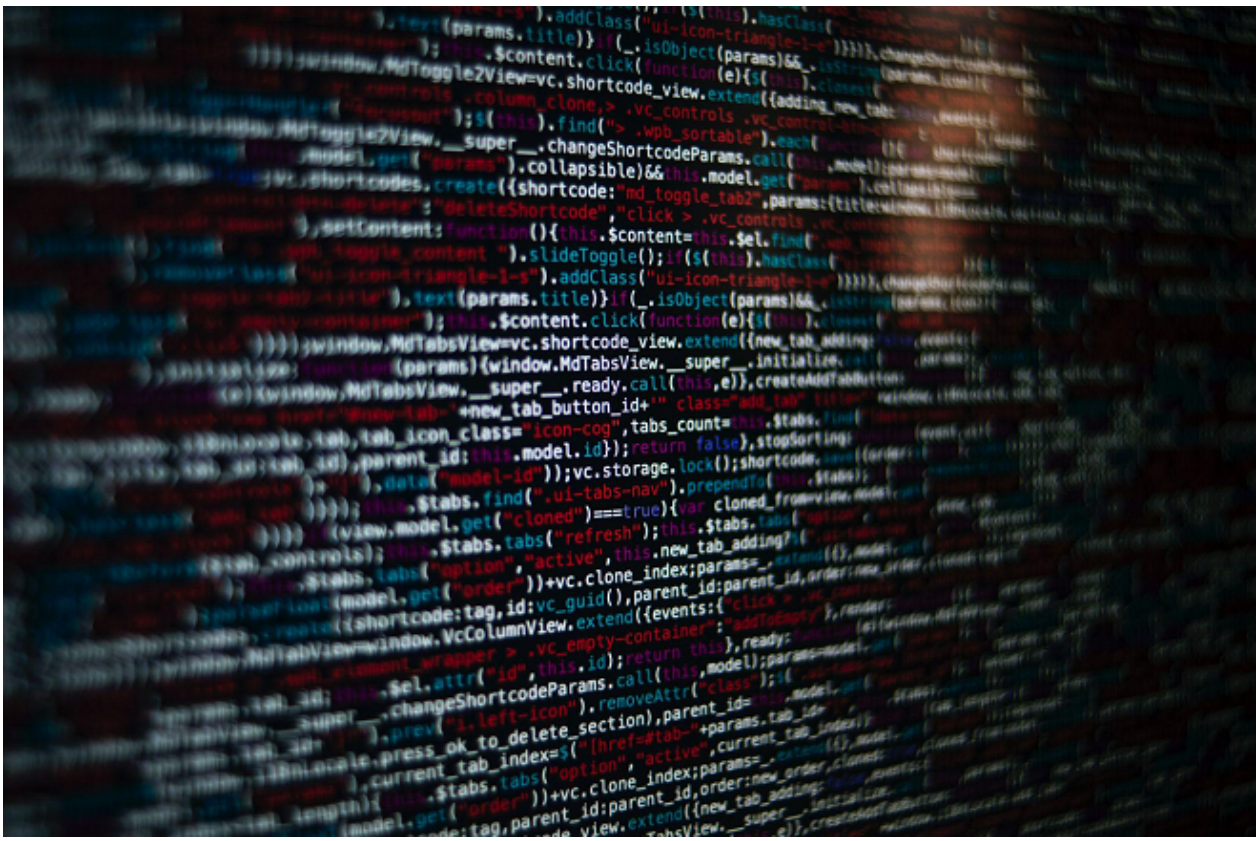
Create a website backup.

It is said that you should arm yourself when you have been warned. Being constantly ready for the worst is a good idea. The worst that can happen in this situation is that your website might be compromised. A backup gives you piece of mind because it prevents data loss in the case of a compromise.

Conclusion

Please allow me to take this time to thank you for persevering through this educational book, Kali Linux. I'd like to think that it was instructive and that you are now well-equipped to tackle issues relating to hacking. I also hope you have acquired the necessary knowledge to launch your hacking career or advance your abilities if you already have one. From the first topic, Introduction to Kali Linux, all the way through The Basics of Kali Linux, The Hacking Process, Wireless Network Hacking, Uses and Applications of Kali Linux, Introduction to Cybersecurity, Network Scanning and Management, and Web Security, I sincerely hope you have enjoyed turning the pages. I hope that by reading this book, you have gained a wealth of practical knowledge that will help you become an accomplished hacker.

By this you must have had access to a substantial body of theoretical information about the different kinds of attacks that might be launched against your systems, the motivations behind them, and the defenses you can put in place to prevent them. These are the initial steps you need to do to become a skilled hacker. The book discusses current topics including penetration testing, cyberattacks, and wireless network threats, among others. It follows that you are now well-positioned to identify network attack methods that manifest in the real world and recommend effective countermeasures.

I've also provided you with a few security steps you can use to protect your networks. You can grasp the need of protecting your networks because of the format's user-friendly terminology. The next stage is to start putting the ideas you have learned from this book into practice. As they say, practice makes perfect, and utilizing Kali Linux in particular, practicing will help one

become an expert hacker. Put to use the knowledge you have learned from the book.