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

JASON KNOX

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

JASON KNOX

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

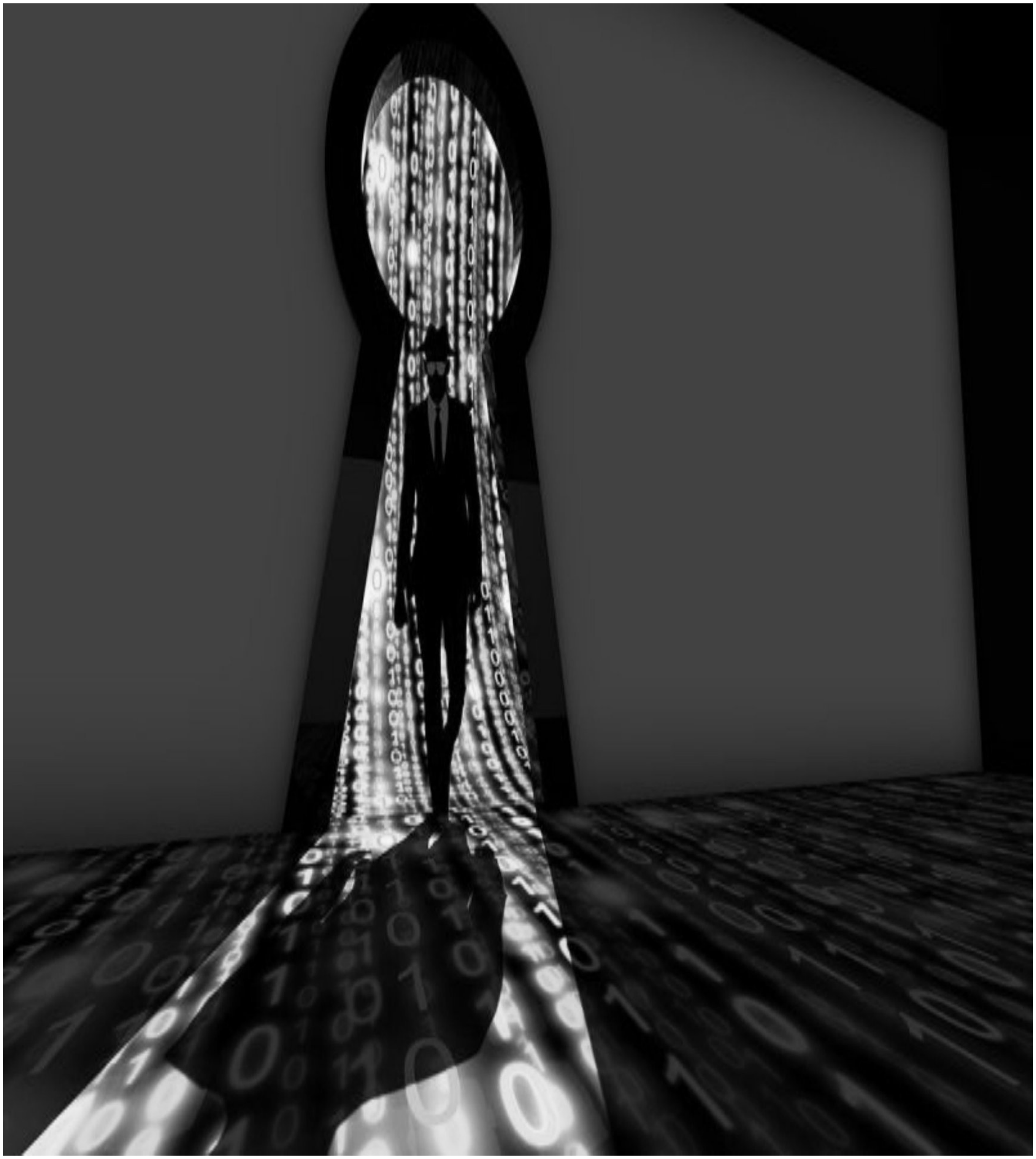
Table of Contents

Introduction

Congratulations on purchasing *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,* and thank you for doing so. The book covers the numerous tools in Kali Linux that you can use for performing penetration tests. You will also be able to learn the operations of the various utilities in this Debian distribution. To use this book effectively, you will require prior knowledge of basic Linux administration, computer networking and the command utilities but on a minimum. This will help you to comprehend the various subjects that have been covered herein.

You will get to know how hackers are able to gain access to your systems and the methods they use to steal information. Furthermore, you will also learn the countermeasures required to safeguard yourself against the numerous hacking techniques. To this end, the books cover topics that include: an Introduction to Kali Linux, 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 some basics on Web Security you will need to know in your journey to be a professional hacker.

By the time you flip the last page of this book you will have mastered both theoretical and practical concepts on the basic techniques that you require to become a hacker. You will have the techniques needed for penetration of computer networks, computer applications alongside computer systems. Let me say that we have numerous books that cover this topic, but you have decided to pick this one up. Many thanks for that. No efforts have been spared in ensuring that the content in this book is relevant and refreshing to you. Have fun reading!



Chapter 1: Introduction to Kali Linux

In this chapter you will be introduced to a diverse area of ethical penetration testing. It is also referred to as ethical hacking and is defined as a technical procedure and methodology which gives professional hackers a platform to simulate the techniques and actions that real-life hackers would use in the exploitation of an information system or a computer network. We are going to learn the steps that are usually followed by the penetration tester right from the understanding and analysis of a select target to the actual break-in. The book also covers topics dealing with the numerous tools that are used in the penetration testing exercise. These are briefly introduced in this chapter but will be covered in depth in chapter 4. The reader will get to understand the practical applications of Kali Linux in the real world besides knowing how to download and install this distribution of Linux. So, let us get into it without further ado.

History of Kali Linux

Offensive Security is the company behind this wonderful distribution. Kali Linux is the company's latest release. Kali is a live disk security distribution having over 300 penetration testing and security tools. If you have prior experience with the operating system, you may have noticed that the tools have been categorized into groups that are commonly utilized by penetration testers and any other entities doing the assessment of information systems. Kali Linux utilizes Debian 7.0 distribution as its base, unlike the earlier distributions that were released by Offensive Security. The operating system is of the same lineage as its predecessor, Backtrack Linux. It is worth noting that it is also supported by the same team.

The name change to Kali Linux, according to Offensive Security, implies that this operating system is a total rebuild of the Backtrack distribution. The major improvements that were made meant that it was not just a new version of Backtrack but a new operating system altogether. Going down memory lane, you will remember that Backtrack itself, just like Kali, was an upgrade that was derived from White Hat and SLAX, abbreviated as

WHAX alongside Auditor. Technically speaking, Kali is the most recent incarnation of the information security industry penetration and auditing assessment tools.

Tool categories in Kali Linux

Kali Linux comes prepackaged with plenty of tools we can use for carrying out penetration testing. As we have said previously, the tools in Kali Linux are categorized in a fashion that helps with the penetration testing exercise. Below are the broad categories:

1) **Information gathering tools:** In this category, we have numerous tools that are used in the information gathering process. Normally, a penetration tester would be interested in information about DNS, operating systems, IDS/IPS, SSL, network scanning, routing, voice over IP, SMB, e-mail addresses, VPN, and SNMP.

2) **Vulnerability assessment tools:** Here, tools that are used in the scanning of vulnerabilities, in general, are located. We have tools that are utilized for the vulnerability assessment of the Cisco network and database servers. We also have several fuzzing tools in this category.

3) **Web applications:** Just like the name, tools in this category relate to web applications. They include database exploitation, content management system scanner, web vulnerability scanners, web crawlers, and web application proxies.

4) **Tools for password attacks:** Tools that you can use to carry out both online and offline password attacks are found under this category.

5) **Exploitation tools** : You will find tools for the exploitation of the vulnerabilities unearthed from a selected target environment. Here, you will get exploitation tools you can use for databases, the Web, and the network. Also, under this category, you will find tools for carrying out social engineering attacks. The tools will give the user information about the exploits carried out too.

6) **Tools for sniffing and spoofing:** The tools here are used for sniffing web traffic and the network traffic. We also have network spoofing tools, for example, Yersinia and Ettercap.

7) **Tools for maintaining access:** A penetration tester will use the tools found here to maintain their access to a target machine. Obviously, you require the highest level of privilege to install tools located in this category. We have tools that can be used for backdooring web applications and the operating system. Tools used for tunneling are also found in this category.

8) **Tools for reporting:** Tools that are used for documentation of the penetration testing methodology and the obtained results and recommendations are found in this category.

9) **System services:** We have numerous services which are necessary during the penetration testing exercise in this category. Examples include: the Metasploit service, Apache service, SSH service, and MySQL service.

10) **Wireless attacks:** Here, we have tools for carrying out attacks on wireless devices, RFID/NFC and Bluetooth devices.

11) **Reverse engineering:** Tools in this category are normally used for debugging programs or carrying out disassembly of executable files.

12) **Stress testing** : If you want to carry out stress testing of your network, VOIP environment, wireless and Web, you will find all the tools relevant in this category.

13) **Hardware hacking:** If you are interested in working with Arduino and Android applications, all the tools you need are found here.

14) **Forensics:** The forensics category contains numerous tools normally utilized in digital forensics. Examples of forensics include the acquisition of hard disk images, carving of files and, more

importantly, analyzing the image retrieved from the hard disk. To do these tasks properly, a user is required to go to the Kali Linux Forensics menu then select the No Drives or Swap Mount from the booting menu. This way, the operating system will not automatically mount the drives. This implies that the integrity of the drives will be maintained.

Hold onto this information for now as we will look at some of it in chapter 5.

The Lifecycle for Penetration Testing

Today, we have various lifecycle models of penetration testing that are being used. So far, the lifecycle and the methodology defined and used by the EC-Council Certified Ethical Hacker program is the one that is widely used. This penetration testing life cycle is made up of five phases, including Reconnaissance, Scanning, Gaining Access, Maintaining Access and finally Covering Tracks in that order. Later in the book, we will look at each of the stages above in detail.

General Penetration Testing Framework

We have said before that Kali Linux provides us with the versatility we need in the process of penetration testing and security assessment from the numerous tools it possesses. A penetration tester who does not follow a proper framework is likely to get unsatisfactory results emanating from unsuccessful testing. This means that it is therefore essential for managers and technical administrators to ensure that the security testing is in harmony with a structured framework: the goal of the test is to provide useful findings.

What you are going to learn here is a general testing framework that is normally used by both the white box and black box approaches. From it, you will get an elementary understanding of the typical phases that a penetration tester or a security auditor should progress. The frameworks, however, need to be adjusted appropriately basing on the target being assessed. The following are steps that need to be followed so that the assessment procedure is successful.

- Scoping of the target
- Gathering Information
- Discovery of the Target
- Target Enumeration
- Mapping out Vulnerabilities
- Social engineering
- The exploitation of the Target
- Escalation of Privilege
- Maintenance of access
- Reporting and Documentation

1. Scoping of the Target

This is usually the first step prior to beginning the technical assessment of the security. It is essential that observations are carried out on the target network environment so that the scope is well understood. It is also possible to define the scope for a given set of entities or a single entity that is given to the auditor. Examples of typical decisions normally made in this step include;

- What element requires testing?
- How will it be tested?
- What are the parameters that will be applied when conducting the test?
- What are the limiting factors of the test process?
- How long will the test take?
- What objectives are intended to be achieved?

For any penetration testing exercise to be successful, the tester must have a good understanding of the technology being assessed, its basic operations together with the way it interacts with the network environment. What this means is that an auditor's knowledge is what determines the success of the penetration testing procedure.

2. Information gathering

After scoping has been done, the next phase is the reconnaissance phase. Here, the penetration tester will make use of resources that are available publicly to get a better understanding of their target. One can get valuable information from sources on the Internet, which include:

- Social networks
- Articles
- Forums
- Blogs
- Bulletin boards
- Commercial or non-commercial websites
- Newsgroups
- Search engines, for example, MSN Bing, Google, among others.

Additionally, Kali Linux has several tools that you can use to get a target's network information. The tools use crucial data mining techniques for gathering information from DNS servers, e-mail addresses, traceroutes, phone numbers, Whois database, personal information, and user accounts. Chances of having a successful penetration test increase with the amount of information that is gathered.

3. Target discovery

Here, key activities are the identification of the network status of selected targets, its OS and, if possible, the target's network architecture. Such information gives a penetration tester a comprehensive outlook of the interconnected devices or current technologies in the network. That means that they will be able to enumerate the numerous services running within the network. It is possible to do all this (determination of hosts on the network that are live, the running OS on the hosts and the characterization of each of them based on their roles in the network system) using the Kali Linux advanced network tools. The detection techniques employed by these tools can either be active or passive. This is done on top of network protocols and can be manipulated in a fashion that will yield useful information. An example of this information is the OS fingerprinting.

4. Target Enumeration

This phase advances the previous efforts by finding open ports on the systems being targeted. After the identification of open ports, enumeration of the ports will be done for the running services. Employing port scanning techniques like stealth, full-open, and half-open scan can assist a hacker, or a penetration tester checks the visibility of ports. This is possible for hosts that are behind an Intrusion Detection System or a firewall. To help penetration testers or hackers discover existing vulnerabilities in a target network's infrastructure, an investigation of the services which are mapped to the open ports can be done. This means that we can use target enumeration as a platform for unearthing vulnerabilities present in the various devices on the network. Through the vulnerabilities, one can penetrate the network. A security auditor can utilize Kali Linux’s automated tools to do target enumeration.

5. Vulnerability mapping

By now, we will be having enough information about the target network. We will now need to analyze the identified vulnerabilities basing on the services and ports we have discovered. We have automated vulnerability assessment tools for applications and the network in Kali Linux that can help us achieve the objectives of this phase. It is also possible to do vulnerability mapping manually. The only downside is that it requires expert knowledge and consumes plenty of time. The best approach to this is to combine the two so that a security auditor can have a clear vision that will enable them to investigate vulnerabilities that are either known or unknown in the network systems.

6. Social engineering

Social engineering is a type of attack which uses human beings as attack vectors. In most information security configurations, human beings are regarded as the weak link through which an attacker can gain access to a system. An attacker can penetrate a target network and execute a malicious code that will do some damage and, in some cases, create a backdoor for future use. All this will have been made possible through deceiving the people in charge of or those using a given network. Social engineering can be of different forms. For instance, an attacker using a phone can pretend to be a network administrator prompting a user to disclose their account information. Another form of social engineering is an e-mail phishing scam, which is used by malicious users to steal the account details of your bank. Physically, a person can imitate a legitimate user to gain access to a physical location. This is also social engineering. From these examples, we can see that the possibilities for achieving a required goal are immense. To make any penetration testing exercise successful, it is important that the tester or attacker takes time to understand human psychology as it is a skill that will help them improvise accordingly in their targeting. Note that most countries have laws regulating this, and as such, it is good to know the laws before attempting anything lest you end up in jail.

7. Target exploitation

After we have studied the vulnerabilities we have uncovered, we can go ahead and penetrate our target based on the available types of exploits. Most of the time, modifications or additional research on existing exploits are needed to ensure the exploits work as intended. The task is, of course, daunting. However, Kali Linux comes prepackaged with advanced exploitation tools that can help in the simplification of the exercise. Further, a tester is at liberty to employ client-side exploitation tactics in addition to some little social engineering to enable them assume control of a target system. A keen reader should, by now, see that this phase concentrates more on the process of target acquisition. Target exploitation encompasses three key areas. These are pre-exploitation, exploitation, and post-exploitation activities.

8. Privilege escalation

After target acquisition, the penetration exercise will be deemed successful. The penetration tester or auditor will now be able to roam in the system freely based on their access privileges. Using local exploits matching the environment of the system, a tester can escalate these privileges. Once these exploits are executed, a hacker or a penetration tester will now be able to get system-level or super-user privileges. From here onwards, a tester can carry out additional attacks on the local network systems. Based on a target's scope, this process can either be non-restricted or restricted. It is also possible to get more information regarding a compromised target through cracking passwords to various services, network traffic sniffing, and employing spoofing tactics on local networks. This implies that the main objective of privilege escalation is to enable one to acquire the highest-level access to the targeted system.

9. Maintaining access

A penetration tester, in some instances, can be requested by a client to maintain their access in the system for a specified period. This can be used as a demonstration to the network managers to show how illegal access to the system can be done without the need for a penetration process again. Also, it serves to save resources, time and cost that is spent in gaining access to the system for purposes of assessing its security. One can choose to use secret tunneling methods that utilize proxy, protocols, or end-to-end connection strategies. This way, a tester can create backdoor access, which will assist them in maintaining their presence in a target system for as long as they are required to. This technique of accessing the system gives us an indication of how an attacker can keep their presence in a targeted system without raising suspicion.

10. Reporting and Documentation

A penetration testing exercise will not be complete if a presentation of disclosed vulnerabilities is not done. Verified and exploited vulnerabilities should be well documented, reported and presented. Ethically speaking, this is crucial as it will help the network and system administrators and managers to direct their resources towards sealing any security loopholes present in their infrastructure. The reports will have different outlooks based on the needs of the different contracting organizations. The customizations of the report will help technical staff and businesses get to know and analyze points of weaknesses existing in their IT infrastructure. In addition to that, the reports can be used in the comparison of the integrity of a target system after and before the penetration process.

Let us look at the Ethics

To ensure that everything remains legal, we have rules of engagement. These must be adhered to by the auditors and other information security professionals.

These rules describe the way the penetration testing should be given, the way testing is to be performed, the determination of legal negotiations and contracts, definition of the testing scope, test plan preparation, the process the test should follow, and the management of a reporting structure that is consistent. A keen examination is required to address each of these areas. The making of formal procedures and practices need to be adhered to throughout the engagement period. These rules include but are not limited to, the following:

1. The test schedule should be chosen in a way that does not affect or interrupt the normal operation of a business. It is prudent to create a schedule that does not cover the typical working hours.

2. The rules governing the test process clearly outline a set of steps to be followed during the testing exercise. The organization’s managers and technicians participate in the formulation of these rules for purposes of restricting the testing process with its environment and people.

3. It is forbidden to provide testing services to a client after hacking their systems prior to coming up with any formal agreement. This is akin to unethical marketing, and in some cases, it may lead to failure of the normal business operations and can cause one to face excruciating legal repercussions based on the country's rules and laws.

4. It is strictly prohibited to conduct a penetration test past the scope of testing or breaching the set limits without a clients' express permissions.

5. A legally binding contract should be agreed upon by parties involved so that it limits the liability of a job unless there is evidence of illegal activity. It must clearly state the conditions and terms of the test procedure, the emergency contact information, the description of work, and any conflicts of interest if present.

6. The scope of the penetration test should be clearly defined, indicating the contractual entities and any restrictions that have been imposed on them during the procedure.

7. On completion of the testing, reports and results must be presented in a consistent and clear fashion. It should include all the vulnerabilities that are known and unknown. Furthermore, it needs to be confidentially delivered to authorized personnel only.

Terminologies

In this book, we are going to encounter commonly used terms in the field of penetration testing. The terms are normally understood differently by members, technicians and professionals in the same field, and that is the reason we need a working definition to avoid any misunderstanding. Below are the terms and associated definitions we shall be using.

Penetration Testing

We define it as the process, methodology and procedures that are used in the attempt to bypass the safeguard mechanisms of the information systems, including overcoming the integrated security set up of that system. Normally, the entire process follows approved and specific guidelines. Penetration Testing is concerned with examining the administrative, technical, and operational controls and settings of a system. The testing assesses the security of a particular information system exactly as it is configured. The system administrators and staff of the targeted network may or may not know that such an exercise is happening.

Ethical Hacking
This is a professional penetration tester whose main job is to carry out an attack on the computer or network systems for an organization or a particular owner of the information system. In this book, you will note that Ethical Hacking and Penetration Testing are used interchangeably.

White Hat
This terminology is synonymous with computer security professional or an Ethical Hacker who is specialized in the security testing of information systems so as to provide security where it is lacking or improve it where it is possible.

Black Hat
This is a terminology used to describe a person who uses his IT skills for bypassing the security of information systems without permission. The intention of black hats is normally to commit computer crimes. Red Team members, together with Penetration Testers, normally employ techniques used by Black Hats in their work. This is to simulate the malicious fellows in security testing while they are carrying out legitimate tests or exercises.

Grey Hat
In life, we have the good guys, the bad guys and those who lie in between. In hacking, grey hats are those in the middle. Normally, they will try to circumvent the security features of an information system in most cases without prior permission. They do this normally to bring to light the

discovered weaknesses to the system administrators. In most cases, they are not after profit. What makes them illegitimate is the fact that they do not seek prior permission from the owners before carrying out their activities.

Vulnerability Assessment/Analysis

This is an exercise done to evaluate the security configurations of a system. The forms of the assessments that can be carried out comprise the evaluation of security patches that have been applied to a system and those that are missing. The team that carries out Vulnerability Assessment can either be external or it can be part of an organization's IT team.

Malicious User Testing

In this scenario, the assessor will act as if they were an insider acting maliciously. Of course, being an insider makes them a trusted entity. What happens is that the assessor will be given legitimate login credentials belonging to an authorized user; this will be a test account. They will then go ahead and use the credentials to try and circumvent laid down security measures. They can do this by modifying settings that are not supposed to be changed, viewing settings and documents that the account is not authorized to and escalating their permissions and privileges beyond the level the test account should have. In summary, a malicious user test attempts to simulates actions that a rogue insider can carry out using their trusted credentials.

Phishing

In this type of attack, attempts will be made to get the targeted entities to reveal personal information such as passwords, account numbers, and user names. Normally, this is done by the use of authentic-looking emails that are fake. The emails can be from customer support staff, banks and corporations. A different type of phishing attack is where users are prodded to click on phony hyperlinks. This will make it possible for malicious codes to be installed on the target system without the owner's knowledge. Once this has been done, the malware can be used to attack other computers or for obtaining data stored on the computer. Phishing attacks are by nature, not directed to a specific target. Targets can be all the people in a mailing list or those whose email addresses have a specific extension, such as those with a "@kali.com" extension.

Spear Phishing
This is a type of phishing attack whereby the targets are specific. For instance,

An attacker can perform reconnaissance to discover email addresses of top-level management of an organization. They can go ahead then to carry out the phishing attack on only these individuals.

Dumpster Diving
In this technique, the penetration tester will make attempts to filter through a systems' discarded trash. This trash might be from any of the users and the system administrators. Any information obtained here will be of great help in understanding a particular target. A penetration tester might recover information detailing network diagrams, system settings and configurations, the hardware components and the software versions that are being used. On a good day, one might even get user credentials such as passwords and user names. Dumpster Diving is a term used to explain the process of entering a large trash container. Also, garbage cans from small offices normally have some lucrative information.

LiveOS, Live Disk, Live CD
The terms above are used to refer to an optical disk containing a complete operating system. Live disks are a crucial asset to penetration testers and assessors since it is possible to modify them to suit the needs at hand. One can customize them to have specific settings, tools and software components. Many of the live disks in distributions are normally Linux based, although, over the years, we have had numerous Microsoft Windows versions being released. In most assessments, it is sufficient for an assessor to only bring with them a live disk. The systems under assessment can be directly booted to the live disk, effectively turning the information systems assets against the system itself.

Chapter 2: The Basics of Kali Linux

Downloading Kali

In the introduction, we pointed out that Kali Linux is a Linux distribution and can be downloaded as an ISO file. You will be required to download it from a different computer, after which you will burn it onto a disk before installation. You can download this interesting distribution of Linux from this link http://www.kali.org/downloads/ . To know how to install it, you can get the documentation for configurations, advanced operations, and special cases on http://www.kali.org/official-documentation/ . If you need any additional help, we have an active community where you can make any inquiries or you can help other members solve their problems. Offensive Security manages these community boards, and new users are required to register to enable them to obtain access.

The security company is the makers of Kali Linux. Occasionally, Offensive Security will provide messages pertaining to their products, community information and updates. When downloading Kali Linux, ensure that you select the proper architecture for your computer (either amd64564-bit or i386532-bit). I do not wish to talk about the images of Kali Linux in this book since that information is well captured in the links I have provided. Tap on the correct link to select and download the image. For those of you that are using Microsoft Windows, you will need to burn the image using the Burn ISO or any other application (I can think of Rufus). Proceed with the burning process until it is complete. Similarly, Linux users can use a disk burning application (say K3b) to convert the ISO image.

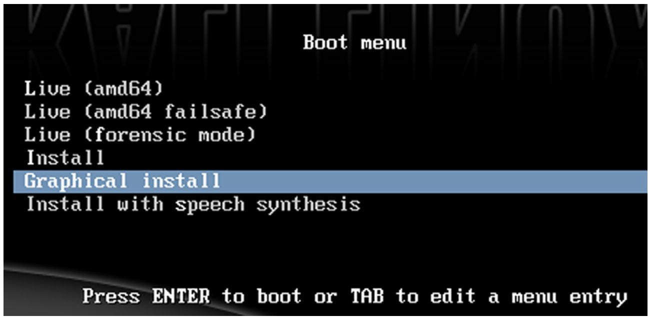
Installation of Kali Linux on the Hard Drive

You are going to learn how to do a graphical and textual installation of this operating system. The graphical interface has been designed to be as simple as possible. You will be required to configure your Basic Input Output System

(BIOS) to boot from the optical disk you have created. First, load your optical disk or flash drive containing Kali onto the computer and start. For advanced users, there is an option of using virtualization technology like Oracle's VirtualBox or VMware's Player.

First Time Booting of Kali Linux

The screenshot below shows a computer that has successfully booted to the Kali Linux disk. 64-Bit Kali Linux version 1.0.5 has been used in this book. With time, you will observe that versions of Kali Linux that are downloaded at different times will appear different, albeit slightly. That aside, graphical installations are similar.



```
                    Boot menu

Live (amd64)
Live (amd64 failsafe)
Live (forensic mode)
Install
Graphical install
Install with speech synthesis

      Press ENTER to boot or TAB to edit a menu entry
```

At http://www.kali.org/ , you will find up to date guides for all the latest releases of Kali Linux. As such, it is important to check out this site before you carry out an installation. Kali Linux, besides being installed on a computer's hard drive, it can be run straight from the disk having the converted image. This is what we call a Live CD. This enables the operating system to boot. The tools that come with Kali will also execute. The only thing to note here is that the operating system from the live CD is nonpersistent. This terminology is used to mean that upon shutting down the computer, any memory, documents, saved settings and any other essential research or work is likely to be lost. A great way to learn Kali Linux is by running it in a nonpersistent state. Additionally, your current operating system will not be affected in any way. You can see that we have

an option for installation with Speech Synthesis. We will not be going into the intricate details for that, but you should know that it is a recent upgrade feature to the Debian operating system and Kali. Users can control the installation procedure vocally if their hardware can support speech synthesis. How exciting! Like I have said before, let us concentrate on the graphical installation for
now. Using the directional keys, scroll and highlight Graphical Install and bang the Enter key.

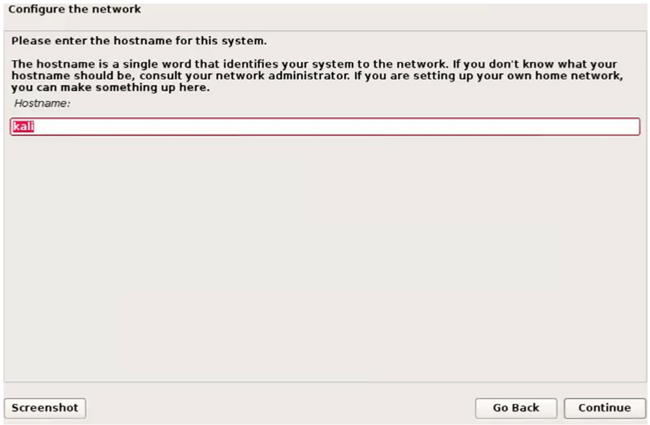
Setting the Defaults

You will be required to select default settings for your location, keyboard layout, and language in the next few screens. After you have made the appropriate selections, click on continue to proceed to the next step. You will notice various bars denoting progress on your computer's screen throughout the installation as the computer begins the actual installation of Kali. Picking the default settings is a good choice for most of the selection screens.

Initial Network Setup

See the image below. In this stage, you will be required to do a basic configuration and an initial setup of your primary network interface card. Select a Hostname. Do this simply by typing in the provided box and hit the continue button to proceed. Make sure you pick a unique hostname to avoid having different computers with similar hostnames on the same network.

That will help to minimize networking complications. Once you are done choosing a hostname, hit the Continue button to proceed. On the next screen, you are going to provide a fully qualified domain name, FQDN. For most lab environments, this is not necessary unless you wish to join a domain environment. Let us leave it blank for now. We will click on the Continue button to move ahead.



Configure the network

Please enter the hostname for this system.

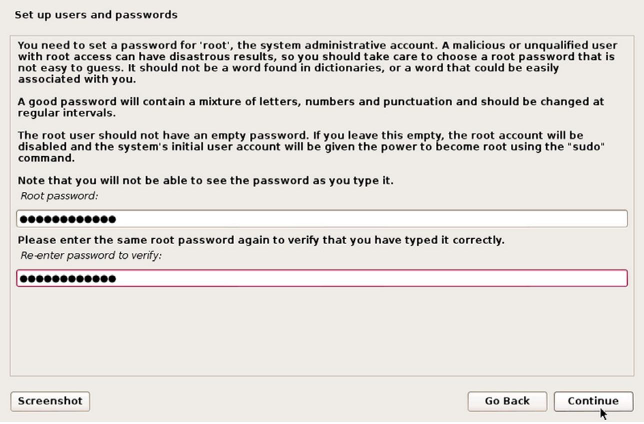
The hostname is a single word that identifies your system to the network. If you don't know what your hostname should be, consult your network administrator. If you are setting up your own home network, you can make something up here.

Hostname:

kali

Setting Up Passwords

The next screen that comes up will prompt you for a root-level password. In Kali Linux, the default password is toor. I recommend that you create a new password that is strong, have no traceability to the user and that it should not be easy to guess. On keying in the password twice, tap the Continue button to move on to the next step. Are you still with me? Let us now configure the system clock.



Set up users and passwords

You need to set a password for 'root', the system administrative account. A malicious or unqualified user with root access can have disastrous results, so you should take care to choose a root password that is not easy to guess. It should not be a word found in dictionaries, or a word that could be easily associated with you.

A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.

The root user should not have an empty password. If you leave this empty, the root account will be disabled and the system's initial user account will be given the power to become root using the "sudo" command.

Note that you will not be able to see the password as you type it.

Root password:

●●●●●●●●●●●●●

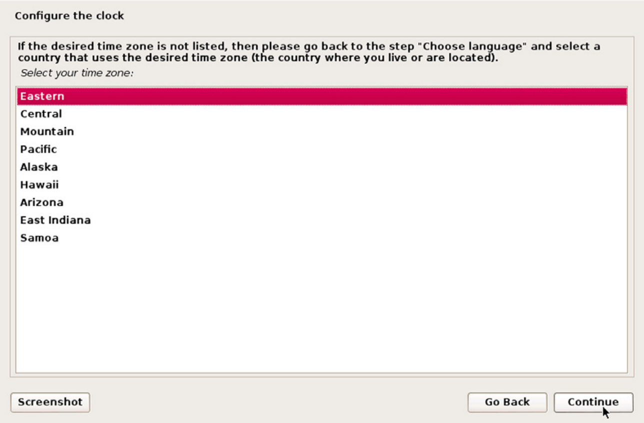
Please enter the same root password again to verify that you have typed it correctly.

Re-enter password to verify:

●●●●●●●●●●●●●

Configuring the System Clock

You will be prompted to select a time zone of your choice, as shown in the figure below. Choose appropriately and then press the Continue button to proceed onto the next installation step.



Configure the clock

If the desired time zone is not listed, then please go back to the step "Choose language" and select a country that uses the desired time zone (the country where you live or are located).

Select your time zone:

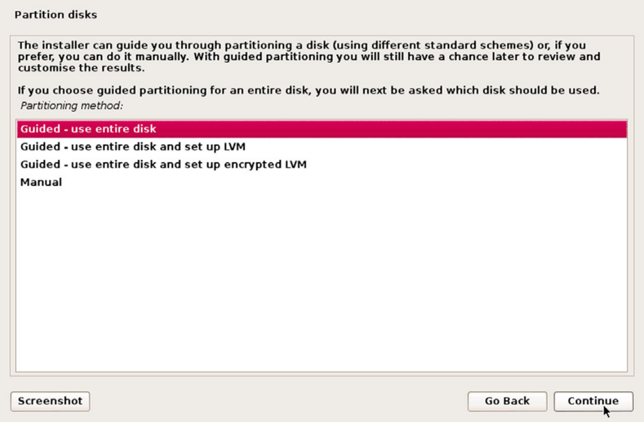
- Eastern
- Central
- Mountain
- Pacific
- Alaska
- Hawaii
- Arizona
- East Indiana
- Samoa

Configuration of the clock.

Partitioning Disks

We have several ways of configuring partitions for setting up a Linux OS. We are going to focus on Guided Partitioning, which is the most basic installation. The figures below display the settings that are normally highlighted by default. You do not have to select anything till you reach the figure under partition disks - 5. All you need to do is click on the continue button until partitioning is complete. Let us take some time and understand what is happening at each step of the installation wizard.

Below, you will see the various options that you can choose for partitioning your computer's hard drives during the installation.



Partition disks

The installer can guide you through partitioning a disk (using different standard schemes) or, if you prefer, you can do it manually. With guided partitioning you will still have a chance later to review and customise the results.

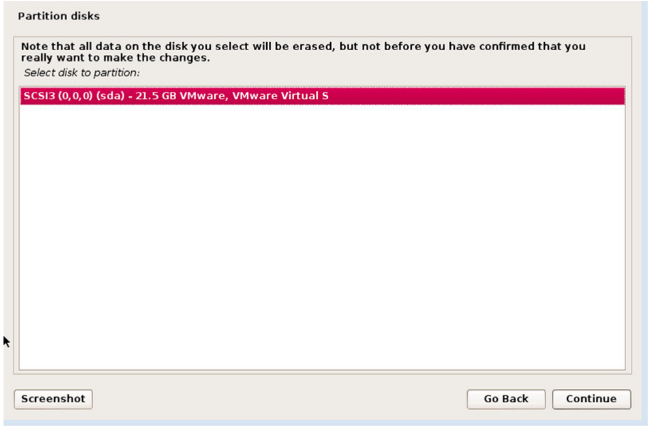
If you choose guided partitioning for an entire disk, you will next be asked which disk should be used.

Partitioning method:

- Guided - use entire disk
- Guided - use entire disk and set up LVM
- Guided - use entire disk and set up encrypted LVM
- Manual

Partition disks - 1.

For laptop SD card or thumb drive installation, it is not recommended to use Logical Volume Management (LVM). Advanced users normally use LVM for managing many hard drives. The option that you should select is "Guided - user entire disk." Hit the Continue button to move onto the next step of the installation process. The figure below will indicate which drive has been picked for installation. Click on Continue to proceed.



Partition disks

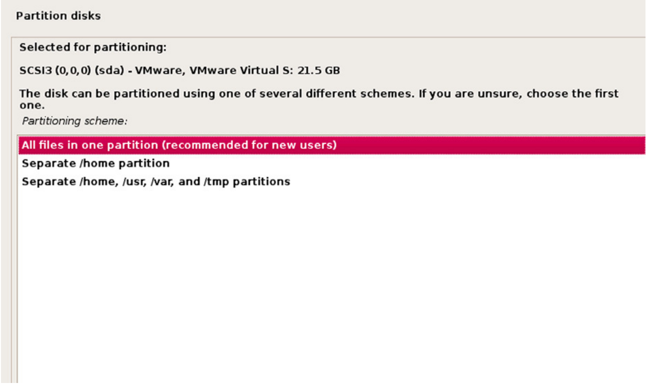
Note that all data on the disk you select will be erased, but not before you have confirmed that you really want to make the changes.

Select disk to partition:

SCSI3 (0,0,0) (sda) - 21.5 GB VMware, VMware Virtual S

Partition disks - 2.

If you are a new Kali Linux user, select the option "All files in one partition (recommended for new users)." This is the best option for you. Hit the Continue button to proceed with the installation.



Partition disks

Selected for partitioning:

SCSI3 (0,0,0) (sda) - VMware, VMware Virtual S: 21.5 GB

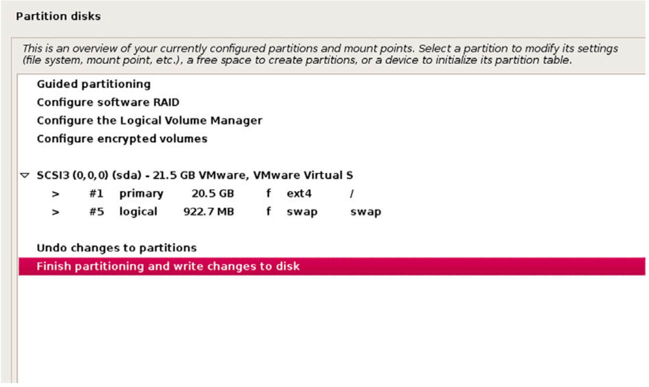
The disk can be partitioned using one of several different schemes. If you are unsure, choose the first one.

Partitioning scheme:

All files in one partition (recommended for new users)
Separate /home partition
Separate /home, /usr, /var, and /tmp partitions

Partition disks - 3.

Keep clicking on the continue button to advance the installation.



Partition disks

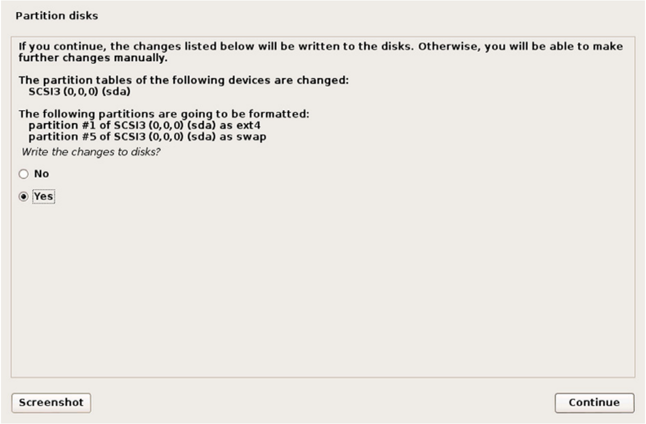
This is an overview of your currently configured partitions and mount points. Select a partition to modify its settings (file system, mount point, etc.), a free space to create partitions, or a device to initialize its partition table.

```
    Guided partitioning
    Configure software RAID
    Configure the Logical Volume Manager
    Configure encrypted volumes

▽  SCSI3 (0,0,0) (sda) - 21.5 GB VMware, VMware Virtual S
      >      #1   primary     20.5 GB     f   ext4       /
      >      #5   logical    922.7 MB     f   swap       swap

    Undo changes to partitions
    Finish partitioning and write changes to disk
```

Partition disks - 4.

The wizard will take you through the above steps and present you with a screen for your review. Now, a partition having all the system, scripting, and user files, known as the primary partition, will be created as a single partition. A second partition will be made for swap space. This is a virtual memory in the system that is used for paging files to and from the computer's random-access memory and the central processing unit. It is recommended that all systems running Linux have a swap area. The common practice is to configure the swap area be one and a half times or even equal to the amount of the computer's installed physical random-access memory (RAM).

You will come to a screen looking like this.



Partition disks

If you continue, the changes listed below will be written to the disks. Otherwise, you will be able to make further changes manually.

The partition tables of the following devices are changed:
  SCSI3 (0,0,0) (sda)

The following partitions are going to be formatted:
  partition #1 of SCSI3 (0,0,0) (sda) as ext4
  partition #5 of SCSI3 (0,0,0) (sda) as swap

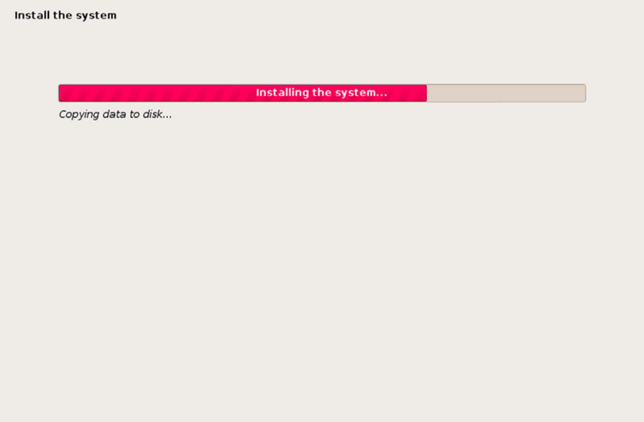
Write the changes to disks?

○ No

● Yes

Partition disks - 5.

From the figure above, you will be asked to "Finish partitioning and write changes to disk." Pick the Yes option and click on the Continue button to proceed with the installation process. Take note that that will be the last chance you will have to review your partitioning options prior to the installation of the operating system on the hard drive. Should a need to amend the sizes of the partition arise in the future, it is still possible to do that. However, changing the partition sizes can destroy your operating system if it is not carried out properly.



Install the system

Installing the system...

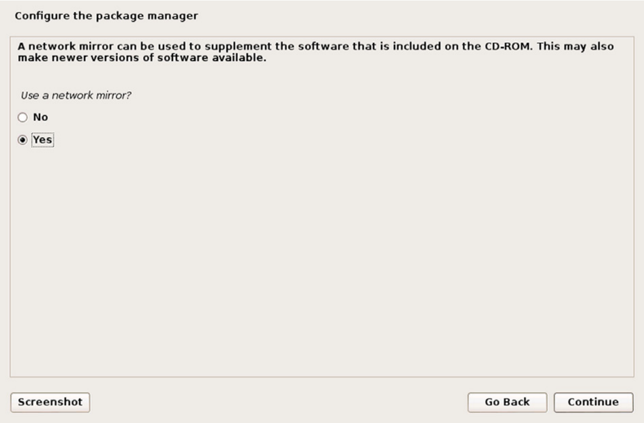
Copying data to disk...

Installation in progress.

The partitioning of the hard drive and installation will begin after you click continue (at the figure at partition disks – 5). The installation can take an hour or even a few minutes depending on your computer's hardware.

Setting Up the Package Manager

This is the update repository where your operating system will derive its security patches and updates from. As such, the package manager is very important in the functioning of the operating system. You can use the network mirror, which comes together with the Kali Linux image. It is recommended to use it since it contains the latest for package management sources. A "YES" option will be picked for you by default, as shown in the figure below. Proceed with the installation process by clicking on the Continue button.



Configure the package manager

A network mirror can be used to supplement the software that is included on the CD-ROM. This may also make newer versions of software available.

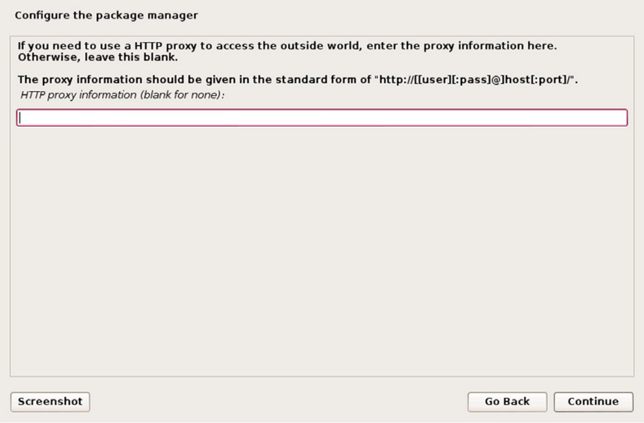
Use a network mirror?

○ No

● Yes

Configuration of the package manager.

Suppose you are utilizing a proxy; you will need to input the configuration information on the next prompt the installation wizard will bring up. You can leave it blank as below. Hit the Continue button to proceed to the installation of the GRUB loader.



Configure the package manager

If you need to use a HTTP proxy to access the outside world, enter the proxy information here. Otherwise, leave this blank.

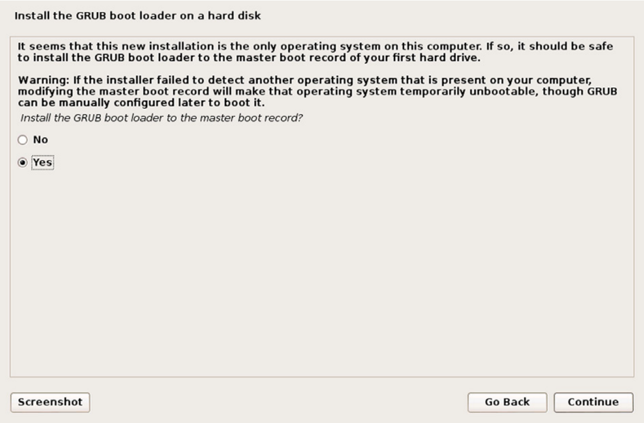
The proxy information should be given in the standard form of "http://[[user][:pass]@]host[:port]/".

HTTP proxy information (blank for none):

Configuring a proxy.

Install the GRUB Loader

GRUB is an abbreviation for Grand Unified Bootloader, and it is the main screen you will see each time you start the computer. GRUB provides a platform where a user can verify specific settings during the booting up, make changes where it is necessary and adjust settings prior to the loading of the operating system. GRUB is highly recommended for most Linux installations even though there are advanced users who do not necessarily need it. The figure below indicates that "YES" has been picked for you to install the GRUB. To advance to the next installation stage, click on the Continue button.



Install the GRUB boot loader on a hard disk

It seems that this new installation is the only operating system on this computer. If so, it should be safe to install the GRUB boot loader to the master boot record of your first hard drive.

Warning: If the installer failed to detect another operating system that is present on your computer, modifying the master boot record will make that operating system temporarily unbootable, though GRUB can be manually configured later to boot it.

Install the GRUB boot loader to the master boot record?

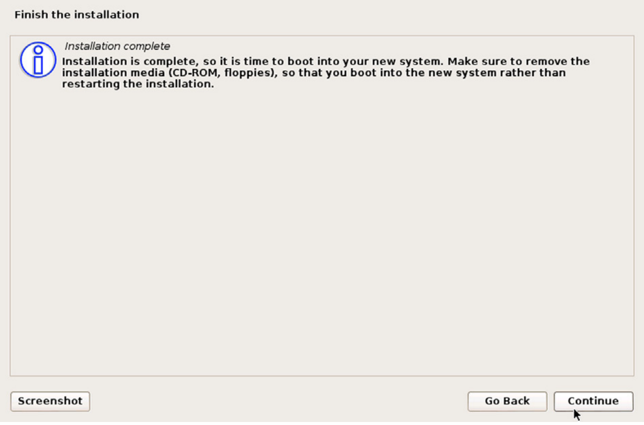
○ No

● Yes

Installing the GRUB loader.

Completing Installation for Kali Linux

Your installation will now be complete. Take out the optical disk or flash drive from the computer and reboot. The computer will prompt you to reboot. Select the Continue button to complete your installation. See the figure below. Upon rebooting, you will be met with a welcome screen requiring you to log in. Use the credentials you set up earlier. That will be it. Welcome to Kali Linux!



Finish the installation

Installation complete

Installation is complete, so it is time to boot into your new system. Make sure to remove the installation media (CD-ROM, floppies), so that you boot into the new system rather than restarting the installation.

Completing the installation.

Why You Should Use Kali Linux

As we have said before, Kali Linux comes with just about every tool pre-installed that can be used for any of the above purposes. It is for this reason that Security Auditors, Forensics Investigators, Penetration Testers and Researchers prefer it.

Kali can be used in the breaking of WiFi networks, to hack websites and networks, to run Open Source Intelligence on an entity, among others. Kali Linux possesses tools that can be used for forensic investigation besides ethical hacking. This is becoming an equally essential branch of security that primarily collects evidence, analyze it and uses the results to backtrack Cyber Criminals. Forensic Investigation makes it possible to locate and eradicate malicious effects emanating from malicious activities. It also comes in handy in the calculation and management of loss that occurs after a Cyber Attack. A key feature in Kali is the stealth Live mode mostly used in forensics and that it does not leave traces (fingerprints and footprints) on a host's system.

The Terminal

The very initial step in using Kali is to open the terminal, which is the command-line interface we'll use in this book. In Kali Linux, you'll find the icon for the terminal at the bottom of the desktop. Doubleclick this icon to open the terminal or press CTRLALTT. The terminal opens the command line environment, known as the shell, which enables you to run commands on the underlying operating systems and write scripts. Although Linux has many different shell environments, the most popular is the bash shell, which is also the default shell in Kali and many other Linux distributions. To change your password, you can use the command passwd.

Basic Commands in Linux

To begin, let's look at some basic commands that will help you get up and running in Linux.

- Finding Yourself with pwd

The command line in Linux does not always make it apparent which directory you’re presently in, unlike that in Windows or macOS. To navigate to a new directory, you usually need to know where you are currently. The present working directory command, pwd, returns your location within the directory structure. Enter pwd in your terminal to see where you are:

```
kali >pwd
/root
```

In this case, Linux returned /root, telling me I’m in the root user’s directory. And
because you logged in as root when you started Linux, you should be in the root user’s directory too, which is one level below the top of the filesystem structure (/). If you’re in another directory, pwd will return that directory name instead.

- Checking Your Login with whoami

In Linux, the one “all-powerful” superuser or system administrator is called root, and it has all the system privileges needed to add users, change passwords, change privileges and so on. Of course, you do not want just anyone to have the ability to make such changes; you want someone who can be trusted and has proper knowledge of the operating system. As a hacker, you usually need to have all those privileges to run the programs and commands you need, so you may want to log in as root. A Linux user can see which user they are logged in as using the “whoami” command as below:

```
kali >whoami
root
```

Here, the user is logged in as root.

- Navigating the Linux Filesystem

Navigating the filesystem from the terminal is an essential Linux skill. To get anything done, you need to be able to move around to find applications, files and directories located in other directories. In a GUI-based system, you can visually see the directories, but when you're using the command-line interface, the structure is entirely text-based and navigating the filesystem means using some commands.

- Changing Directories with cd

To change directories from the terminal, use the change directory command, cd. For example, here's how to change to the /etc. directory used to store configuration files:

```
kali >cd /etc
root@kali:/etc#
```

The prompt changes to root@kali:/etc, indicating that we're in the /etc. directory. We can confirm this by entering pwd

```
root@kali:/etc# pwd
/etc
```

To move up one level in the file structure (toward the root of the file structure, or /), we use cd followed by double dots (..), as shown here:

```
root@kali:/etc# cd ..
root@kali:/# pwd
/
root@kali:/#
```

This moves us up one level from /etc. to the /root directory, but you can move up as many levels as you need. Just use the same number of double dot pairs as the number of levels you want to move:

- You would use .. to move up one level.
- You would use .. .. to move up two levels.
- You would use .. .. .. to move up three levels, and so on.

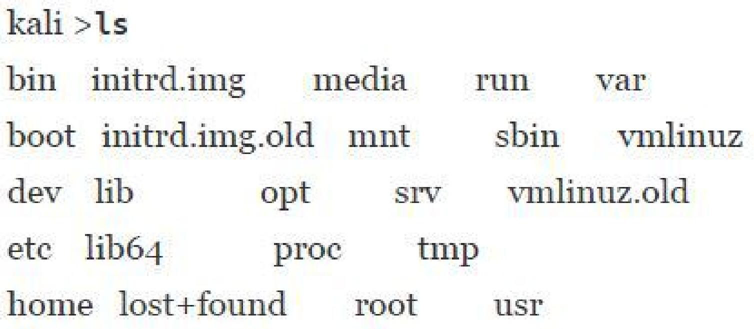
So, for example, to move up two levels, enter cd followed by two sets of double dots with a space in between:

kali >cd .. ..

You can also move up to the root level in the file structure from anywhere by entering cd /, where / represents the root of the filesystem.

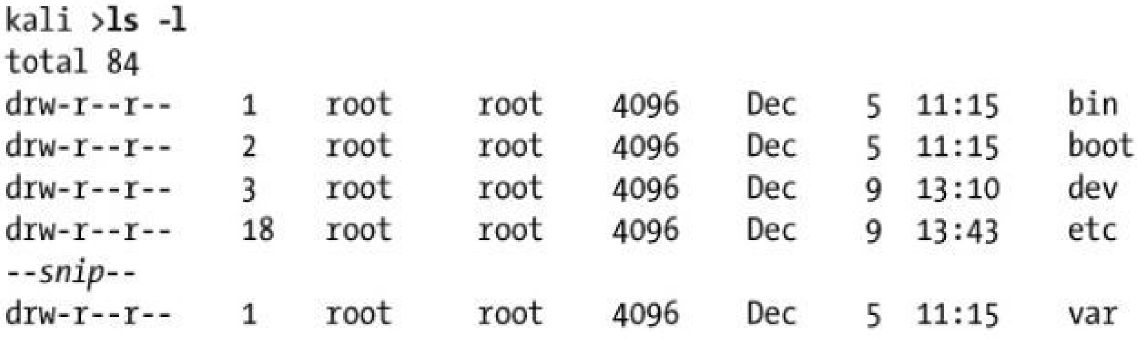
- Listing the Contents of a Directory with ls

To see the contents of a directory (the files and subdirectories), we can use the ls (list) command. This is very similar to the dir command in Windows.



```
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 lists both the files and directories contained in the directory. You can also use this command on any particular directory, not just the one you are currently in, by listing the directory name after the command; for example, ls /etc. shows what’s in the /etc. directory. To get more information about the files and directories, such as their permissions, owner, size and when they were last modified, you can add the -l switch after ls (the l stands for long). This is often referred to as the long listing. See the example 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

Nearly every command, application or utility has a dedicated help file in Linux that guides its use. For instance, if I needed help using the best wireless cracking tool, aircrack-ng, I could type the aircrack-ng command followed by the --help command:

```
kali >aircrack-ng --help
```

Note the double dash here. The convention in Linux is to use a double dash (--) before word options, such as help, and a single dash (-) before single letter
options, such as –h. When you enter this command, you should see a short description of the tool and guidance on how to use it. In some cases, you can use either -h or -? to get to the help file. For instance, if I needed help using the hacker's best port scanning tool, Nmap, I would enter the following:

```
kali >nmap -h
```

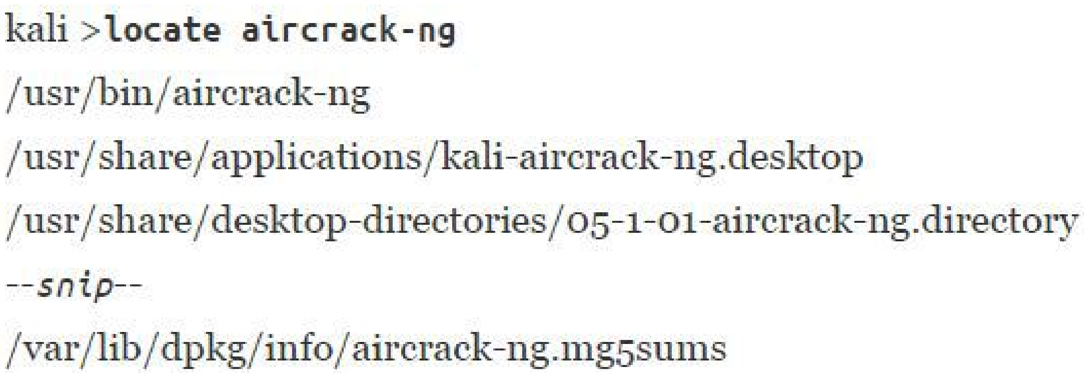
Unfortunately, although many applications support all three options, there is no guarantee of the application you are using will. So if one option refuses to work, please try another.

Finding Files

Until you become familiar with Linux, it can be frustrating to find your way around, but knowledge of a few basic commands and techniques will go a long way toward making the command line much friendlier. The following commands help you locate things from the terminal.

- Searching with locate

Probably the easiest command to use is locate. Followed by a keyword denoting what it is you want to find, this command will go through your entire filesystem and locate every occurrence of that word. To look for aircrack-ng, for example, enter the following:

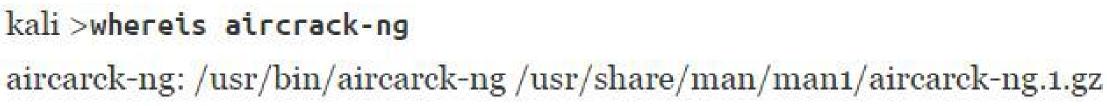


```
kali >locate aircrack-ng
/usr/bin/aircrack-ng
/usr/share/applications/kali-aircrack-ng.desktop
/usr/share/desktop-directories/05-1-01-aircrack-ng.directory
--snip--
/var/lib/dpkg/info/aircrack-ng.mg5sums
```

The locate command is not perfect, however. Sometimes, the results of locate can be overwhelming, giving you too much information. Also, locate uses a database that is usually only updated once a day, so if you just created a file a few minutes or a few hours ago, it might not appear in this list until the next day. It’s worth knowing the disadvantages of these basic commands so you can better decide when best to use each one.

- Finding Binaries with whereis

If you’re looking for a binary file, you can use the whereis command to locate it. This command returns not only the location of the binary but also its source and main page if they are available. Here’s an example:



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

- Finding Binaries in the PATH Variable with which

The which command is even more specific: it only returns the location of the binaries in the PATH variable in Linux. For example, when I enter aircrack-ng on the command line, the operating system looks to the PATH variable to see in which directories it should look for aircrackng:

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

Here, which was able to find a single binary file in the directories listed in the PATH variable. At a minimum, these directories usually include /usr/bin, but may consist of/usr/sbin and maybe a few others.

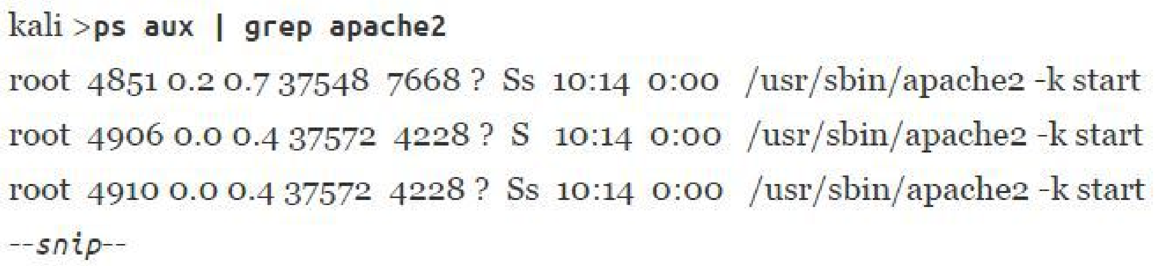
- Performing More Powerful Searches with find

The find command is the most powerful and flexible of the searching utilities. It is capable of beginning your search in any designated directory and looking for several different parameters, including, of course, the filename but also the date of creation or modification, the owner, the group, permissions and the size.
Here is the basic syntax for find:

find directory options expression

- Filtering with grep

Very often, when using the command line, you may want to search for a particular keyword. For this, you can use the grep command as a filter to search for keywords. The grep command is often used when output is piped from one command to another.



```
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--
```

In the above example, the command will display all the services that are running and then pipe that output to grep. What grep does is it will search the received output for the keyword we asked it to look for. In our case, the keyword is apache2. Grep will go ahead and output only the relevant results. This command saves time.

Modify Files and Directories

After finding the directories and files you were looking for, you may need to carry out several operations on them. We are going to learn the creation of directories and files, copy files, rename files, plus delete the files and directories.

- Creating Files

There are many ways to create files in Linux, but for now, we will look at two simple methods. The first is the cat, which is short for concatenate, meaning to combine pieces (not a reference to your favorite domesticated feline). The cat command is generally used for displaying the contents of a file, but it can also be used to create small files. For creating bigger files, it's better to enter the code in a text editor such as vim, emacs, leafpad, gedit or kate and then save it as a file.

- Concatenation with cat

The cat command followed by a filename will display the contents of that file, but to create a file, we follow the cat command with a redirect, denoted with the > symbol, and a name for the file we want to create. Here is an example:

```
kali >cat > kalilinux
Hacking with Kali Linux!
```

- File Creation with touch

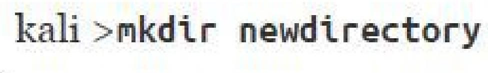
The second command for file creation is touch. This command was initially developed so a user could touch a file to change some of its details, such as the date it was created or modified. However, if the file does not already exist, this command creates that file by default. Let's create newfile using the touch command:

```
kali >touch newfile
```

Now when I then use ls –l to see the long list of the directory, I see that a new file has been created named newfile. Note that its size is 0 because there is no content in the newfile.

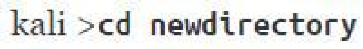
- Creating a Directory

The command for creating a directory in Linux is mkdir, a contraction of make directory. To create a directory named newdirectory, enter the following command:



```
kali >mkdir newdirectory
```

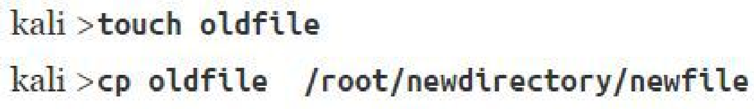
To navigate to this newly created directory, do enter this:



```
kali >cd newdirectory
```

- Copying a File

To copy files, we use the cp command. This creates a duplicate of the file in the new location and leaves the old one in place. Here, we are going to create the file oldfile in the root directory with touch and copy it to /root/newdirectory, renaming it in the process and leaving the original oldfile in place:



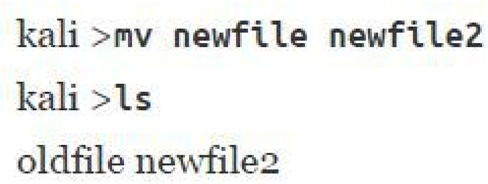
```
kali >touch oldfile
kali >cp oldfile  /root/newdirectory/newfile
```

Renaming the file is optional and is done simply by adding the name you want to give it to the end of the directory path. If you don’t rename the file when you copy it, the file will retain the original name by default. When we then navigate to newdirectory, we see that there is an exact copy of oldfile called newfile:

```
kali >cd newdirectory
kali >ls
newfile oldfile
```

- Renaming a File

Unfortunately, Linux doesn’t have a command intended solely for renaming a file, as Windows and some other operating systems do, but it does have the mv (move) command. The mv command can be used to move a file or directory to a new location or to give an existing file a new name. To rename newfile to newfile2, you would enter the following:



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

Now when you list (ls) that directory, you see newfile2 but not newfile, because it has been renamed. You can do the same with directories.

- Removing a File

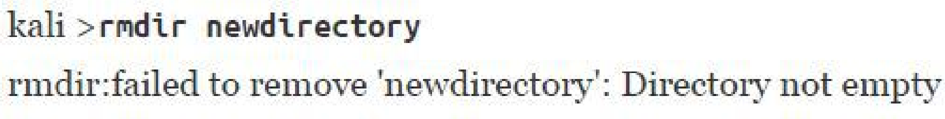
To remove a file, you can use the rm command, like so:

kali >rm newfile2

If you now do a long listing on the directory, you can confirm that the file has been removed.

Removing a Directory

The command for removing a directory is similar to the rm command for removing files but with dir (for directory) appended, like so:



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

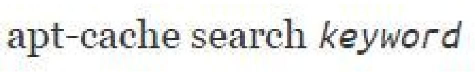
It is important to note that rmdir will not remove a directory that is not empty but will give you a warning message that the “directory is not empty,” as you can see in this example. You must first remove all the contents of the directory before removing it. This is to stop you from accidentally deleting objects you did not intend to delete. 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. Using rm -r in your home directory, for instance, would delete every file and directory there, that is certainly not what you were intending.

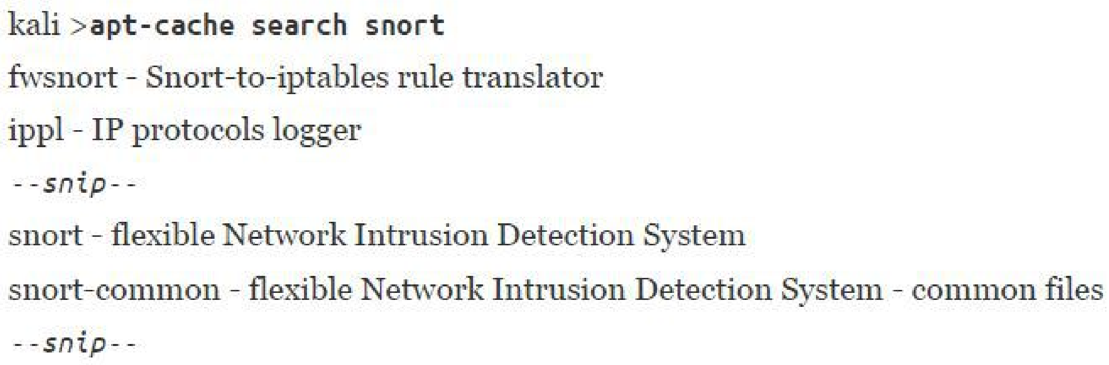
Searching for tools/packages

Before you download a software package, you can check whether the package you need is available from your repository, which is a place where your operating system stores information. The apt tool has a search function that can check whether the package is available. The syntax is straightforward:



```
apt-cache search keyword
```

Note that we use the apt-cache command to search the apt cache or the place it stores the package names. So if you were searching for the intrusion detection system Snort, for example, you would enter the command shown below.



```
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, many files have the keyword snort in them, but near the middle of the output, we see snort – flexible Network Intrusion Detection

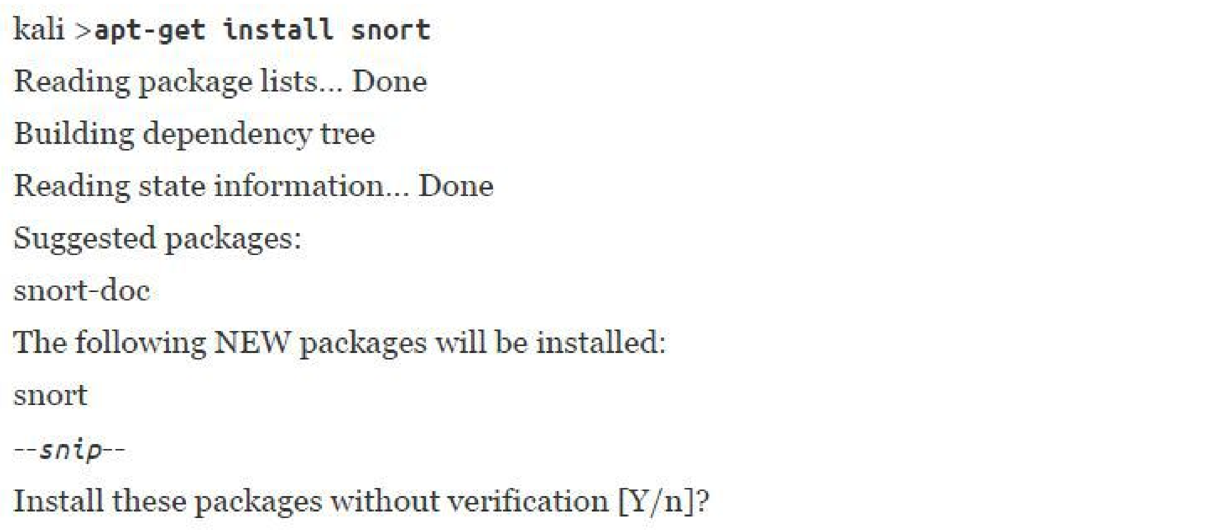
System. That is what we are looking for.

Adding Softwares

Now that you know the snort package exists in your repository, you can use apt-get to download the software. To install a piece of software from your operating system’s default repository in the terminal, use the apt-get command, followed by the keyword install, and then the name of the package you want to install. The syntax looks like this:

apt-get install packagename

Let us try this out by installing Snort on your system. Enter apt-get install snort as a command statement, as shown below.

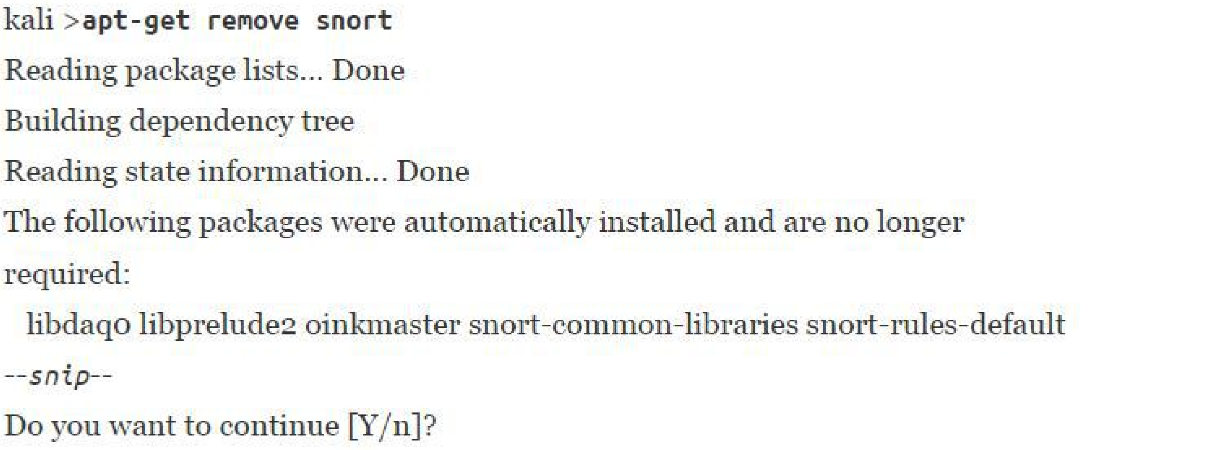


```
kali >apt-get install snort
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
snort-doc
The following NEW packages will be installed:
snort
--snip--
Install these packages without verification [Y/n]?
```

The output you see tells you what is being installed. If everything looks correct, go
ahead and enter Y when prompted, and your software installation will proceed.

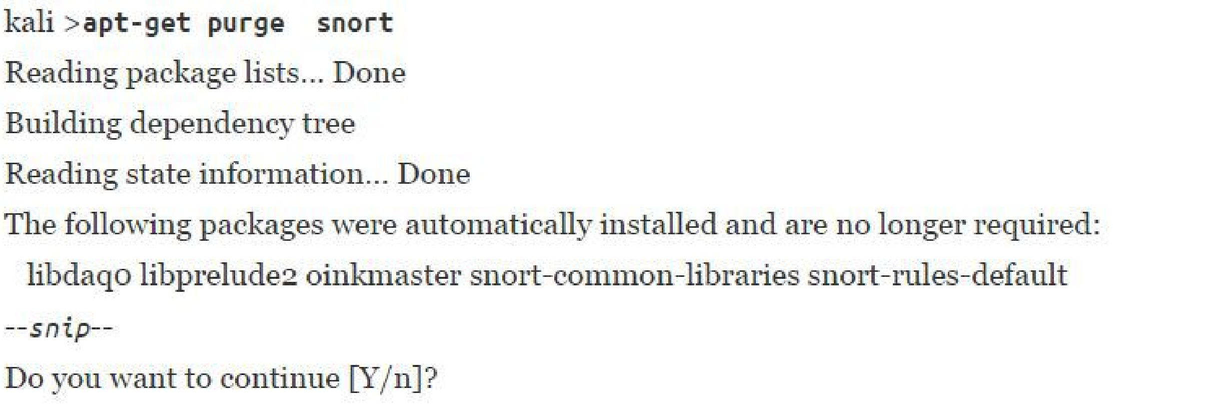
Removing Softwares

When removing software, use apt-get with the remove option, followed by the name of the software to remove. An example is listed below.



```
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]?
```

Again, you will see the tasks being done in real-time, and you will be asked whether you want to continue. You can enter Y to uninstall, but you might want to keep Snort since we will be using it again. The remove command does not remove the configuration files, which means you can reinstall the same package in the future without reconfiguring. If you do want to remove the configuration files at the same time as the package, you can use the purge option, as shown below.



```
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]?
```

Enter Y at the prompt to continue the purge of the software package and the configuration files. To keep things small and modular, many Linux packages are broken into software units that many different programs might use. When you installed Snort, you installed several dependencies or libraries with it that Snort requires so that it can run. Now that you are removing Snort, those other libraries or dependencies are no longer needed, so they are removed, too.

Updating Packages

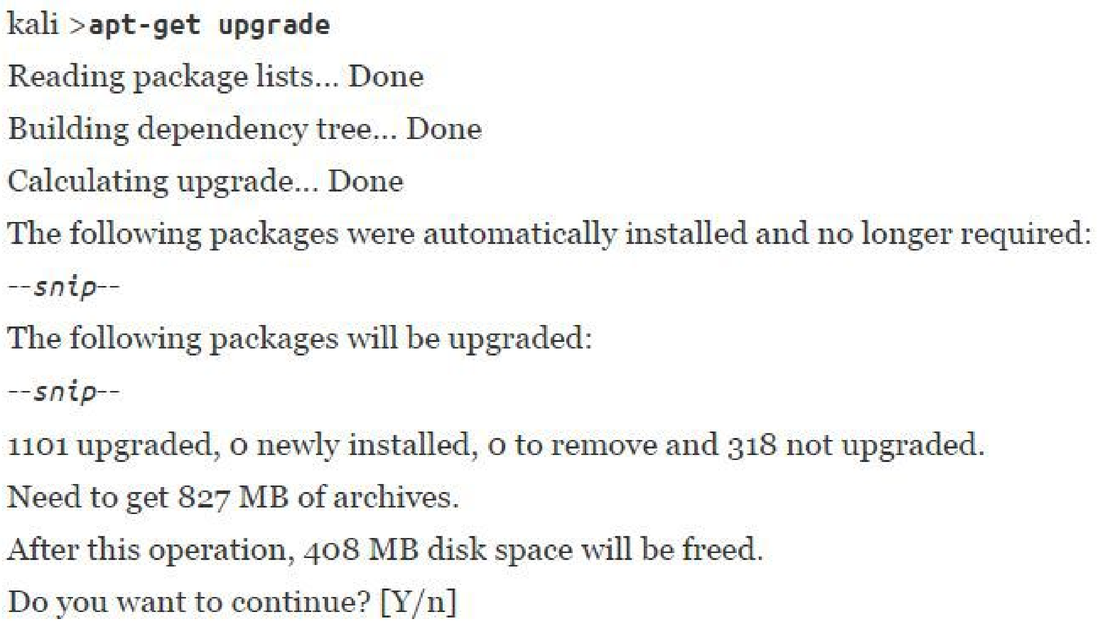
Software repositories will be periodically updated with new software or new versions of existing software. These updates do not reach you automatically, so you need to request them to apply these updates to your system. Updating is different from upgrading: updating updates the list of packages available for download from the repository, whereas upgrading will upgrade the package to the latest version in the repository. You can update your system by entering the apt-get command, followed by the keyword update. This will search through all the packages on your system and check whether updates are available. If so, the updates will be downloaded. See the example 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
```

The list of available software in the repository on your system will be updated. If the update is successful, your terminal will state Reading package lists... Done, as you can see above. Note that the name of the repository and the values, time, size and so on might be different on your system.

Upgrading Packages

To upgrade the existing packages on your system, use apt-get upgrade. Because upgrading your packages may make changes to your software, you must be logged in as root or use the sudo command before entering an apt-get upgrade. This command will upgrade every package on your system that apt knows about, meaning only those stored in the repository, as shown below. Upgrading can be time-consuming, so you might not be able to use your system for a while.



```
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]
```

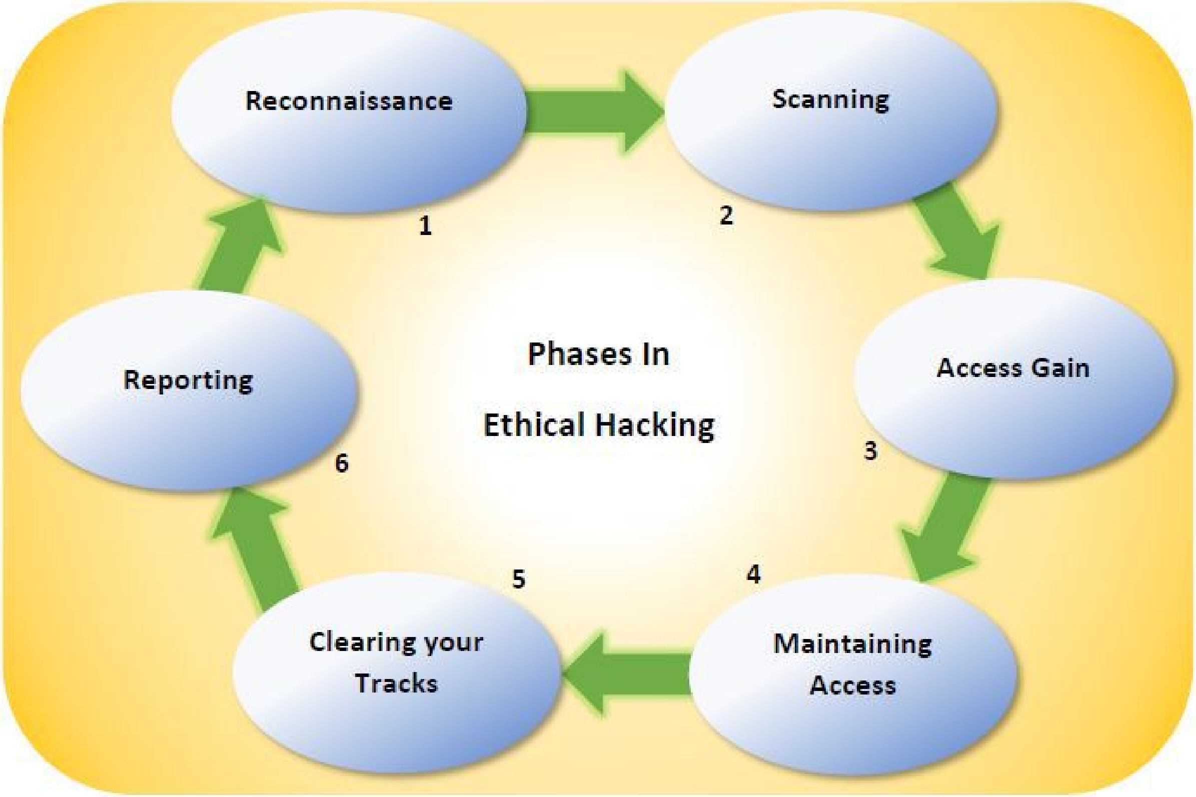
You should see in the output that your system estimates the amount of hard drive space necessary for the software package. Go ahead and enter Y if you want to continue and have enough hard drive space for the upgrade.

Chapter 3: The Hacking Process

In short, Ethical hacking, performed by white hat hackers, is a term used to describe defense hacking for companies and organizations, which involves the identification of potential threats on a computer or network.

Like all good projects, ethical hacking also has a set of distinct phases. It helps hackers to make a structured ethical hacking attack.Different security training manuals explain the process of ethical hacking in different ways, but in my experience, the entire process can be categorized into the following six phases:

1. Reconnaissance.
2. Scanning.
3. Access Gain.
4. Maintain Access.
5. Clearing your Tracks.
6. Reports.



Reconnaissance

What is Reconnaissance? From the dictionary meaning, it is a preliminary survey that is carried out to obtain information. An example is the exploratory surveys that militaries conduct on the territory belonging to the enemy. When it comes to cyber-security, Reconnaissance is a way of gathering information on a target using different techniques. When performing this exercise, there are three main information that is of interest to an ethical hacker;

1. The Network.
2. The Host.
3. Users/People involved.

Steps in Performing a Reconnaissance Exercise.

In ethical hacking, the first step is normally meant to help a penetration tester better understand their targets. This is done under a category that is collectively known as Information Gathering. Hereunder, we have something known as Reconnaissance, which we define as being a set of techniques and processes that are utilized in the discovery and collection of crucial information about a target. They include Scanning, Enumeration and Foot-printing. In an exercise meant for Reconnaissance, an ethical hacker tries to gather as much information about a target system as possible, following the seven steps listed below;

1. Collecting first information.
2. Determine a network's range.
3. Identification of active machines.
4. Discovering of Access Points and open ports that are available.
5. Operating System Fingerprinting.
6. Scanning for services running on various ports.
7. Network Mapping.

Reconnaissance is categorized into two major parts.

1. Active Reconnaissance: Active reconnaissance involves direct contact with your target's computer system to gain information, and information gotten directly is actually accurate. There is the risk of being caught in the

process of active reconnaissance without permission. But most hacking activities require active recon.
2. Passive Reconnaissance: In this process, you will not be directly connected to a computer system. This process is used to gather essential information without ever interacting with the target systems.

Enumeration

Enumeration, in the actual sense, is the complete listing of things in an orderly manner with regards to items in a collection. Enumeration is the act of making a list of policies, user accounts, shares and other resources. This step happens just before vulnerability assessment and after scanning. This helps the attacker put together the best strategy for gaining access. Enumeration can be used to gain information on:

1. Users and Groups
2. Networks and shared paths
3. Hostnames
4. Route Tables
5. Service Settings
6. SNMP port scanning
7. DNS Details Applications and Banners.

Enumeration can be done with the following tools. In the Windows Operating System, the use of many tools is done to enumerate NetBIOS names with commands like:
- Net accounts,
- Net config server,
- Net config workstation,
- Net view.

Scanning

This is a procedure that is used in the identification of services, active hosts and the ports that are used by the target application. Let us say you wish to unearth the vulnerabilities in a system, what you will need is a point you can attack in the System. In ethical Hacking, Network Scanning is employed to find out these points. These are points that Black Hats use to penetrate a system. After discovering these points, the relevant teams will then direct their efforts to improve the system. We know that all organizations have networks. They can either be internal or even connected to the internet. To hack these networks, you must first find a vulnerable point within them so that you can use it to carry out exploits. Network Scanning is the method we employ to help us discover such points within a network.

Network Scanning Objectives

1. It helps in the discovery of open ports, live computers or hosts and the IP address of the victim.
2. Network scanning makes it possible to identify the services which are running on the host computer.
3. It also aids in the discovery of the system architecture and the operating system of the target.
4. Scanning Live hosts enables us to unearth and mitigate vulnerabilities.

How is Network Scanning different from Reconnaissance ?

To help you understand the difference between the two, I am going to use this analogy. Assume that you are commander in the army and you have been tasked together with your team to go and carry out an attack on a terrorist camp. We are going to assume that you already have an idea of the camps' location and the details about the vicinity of the camp. Now, this is information normally obtained through Reconnaissance. You will still be required to identify an entry point to the terrorist camp so that you can launch your attack. This is now what we are calling Network Scanning. We can confidently conclude that Reconnaissance is a technique you will use for gathering information to help you know more about your target. On the other hand, Network Scanning is a technique you will employ to help you locate possible vulnerable points within the network. It is through these points that one can penetrate a targeted network. Based on the information revealed by the scan, Network Scanning can be divided into two main categories:

- Port Scanning
- Vulnerability Scanning

Port Scanning

From the name, we can deduce that Port Scanning is a way of identifying active ports on the network. A Port Scanner works by transmitting requests from a client to the range of ports located on a network that they are targeting. The details about the ports will be saved and then a response will be transmitted back. This, good readers, is how active ports are found. Upon acquiring a target's IP address (through scanning a victim organization's UDP and TCP ports), the hacker will proceed to map the organization's network under his/her grab.

Types of Port Scanning

SYNScan: In this mode of scanning, the TCP three-way handshake technique is not completed. Here, a hacker or penetration tester will send a victim the SYN packet. In case the response of an SYN/ACK frame is received, a connection will be completed by the target and the port will be able to listen. Receiving an RST from the target can mean that the port is not activated or it is closed. This type of scan has an advantage in the sense that only a few IDS systems will log this as a connection attempt or an attack.

XMASScan: The scan transmits a packet containing PSH (push), URG (urgent), and FIN (finish) flags. Suppose we have an open port; we do not expect a response; the target will respond with an RST/ACK packet if the port is closed. (RST=reset)

FINScan: This scan is almost similar to an XMAS scan with one exception. FINScan transmits packets with just the FIN (finish) flag. The scan does not have the other two flags (URG and PSH flags). The response is similar to that of XMAS scans. Also, the two scans have similar limitations.

IDLEScan: This kind of scan utilizes a spoofed IP for the transmission of a SYN packet to the target through the determination of the responses from the port scan together with the IP header sequence number. The port is considered opened or closed based on the response of the scan.

Inverse TCP Flag Scan: In this case, a hacker will transmit TCP probe packets with a TCP flag (FIN, URG PSH) or with no flags. If there is no response, then it indicates that the port is open and RST means the port is closed.

ACK Flag Probe Scan: In this type of port scanning, an intruder will transmit TCP probe packets to a point where an ACK flag is set to a remote device that is used for the analysis of the header information. This information comprises of WINDOW and the TTL field. To know if the port is open or closed, one uses the RST packet. You can also use this scan for checking a target's filtering system.

Vulnerability Scanning

Essentially speaking, this is a type of Network Scanning that we use in our search for a network’s weak points. Vulnerability Scanning unearths the vulnerabilities which can arise because of a misconfiguration of the network or due to poor programming. Before we go far, let us have a look at a few tools used for Network Scanning.

Tools for scanning networks and ports
Nmap: is utilized in the extraction of information, for instance, operating systems, type of packet filters/firewalls, live hosts on the network, services and the operating system versions.

Angry IP Scanner: this tool can be used to scan for IP addresses on systems available in each input range.

Superscan: this is a powerful tool developed by Mcafee. Besides being a TCP port scanner, it can also be used for pinging.

ZenMap: this scanner has a very powerful Graphical user interface tool that can help one detect the type of OS version, port scanning, OS, ping sweep, etc.

Net Scan Tool Suite Pack: this refers to a collection of different utilities and tools that are used for performing web rippers, port scans, mass emailers and flooding. Note that the tool is a trial version, but paid versions are also available.

Omnipeak and Wireshark are famous and powerful tools that are used for listening to network traffic. Both tools can be used as a network analyzer.

Countermeasures against scanning

1. System administrators can set up IDS and firewalls not only detect, but also block any probing attempts.
2. Employing custom rules which will lock down the network and bar any ports not wanted.
3. A user can run tools for port scanning so as to ascertain if the firewall detects any port scanning activities accurately.
4. Security Experts are required to make sure that there is a correct setting up of anti-spoofing and anti-scanners rules.
5. System and network managers need to ensure that the firewall firmware IDS and routers are up to date.

Gaining Access

Gaining access is by far the most critical phase of an attack. I am talking in terms of potential damage. Malicious actors do not always require to have access to a system to cause damage. For example, a denial-of-service attack can be carried out remotely with the potential to cause an abrupt termination of the services that are actively being executed on the target or in some cases, exhaust available resources. To stop a service, one can kill processes. This can be accomplished by the use of a logic/time bomb. Also, a reconfiguring and crashing of the system can achieve similar results. Network resources can be exhausted locally via the filling up outbound communication links. Such exploits can be done over a LAN or the Internet, locally, or offline as a deception or theft. Let us list some examples of these below:

- Session hijacking
- Buffer overflows that are Stack-based
- Denial-of-service and distributed denial-of-service

Sophisticated attackers normally carry out spoofing so that they can exploit a target’s system by way of pretending to be different systems or strangers.

Using this approach, they can transmit a malformed packet having a bug. This bug will attempt to exploit vulnerabilities that are found in the target system.

A technique known as packet flooding can be employed to remotely stop the availability of essential services. We have a different type of attack known as smurf attacks. These attacks attempt to elicit a response from the available network users. Their legitimate addresses will then be used to flood the victim. The success of gaining access to a target system by an attacker is heavily dependent on the following:

- The initial level of access gained.
- The level of skill of the attacker and
- The configuration and architecture of the target system.

The most damaging type of denial-of-service attack is the distributed denial-of-service attack. This happens when an attacker employs the use of zombie software that is spread over many machines on the Internet to initiate a coordinated large-scale denial of services.

Maintaining Access

After a hacker gains access to his target system, he/she will need to dedicate their efforts to ensure their boat remains afloat, metaphorically speaking. The attacker can decide to exploit the hijacked system while being in stealth mode, use it as a launching pad for attacks such as DDoS or spam campaigns or use it for scanning and exploiting other systems. All these actions can be damaging. Let me show you a practical example. A hacker can create a sniffer to help them intercept all network traffic (both inbound and outbound). Part of the traffic can include the telnet sessions with other systems and file transfer protocols to enable them to send the captured data to any destination. Those who do not wish to be detected will be required to take steps that will help to conceal their presence. We have many techniques to do this. The preferred method is where the hacker installs hidden infrastructure based on covert channels, rootkits, Trojan horses and backdoors to enable them to have unfettered access to those systems.

Tools and Methods

A Trojan or backdoor is one such way to establish quick access to a system that has already been breached. A Trojan horse allows a hacker application-level access. The downside to this is that the Trojans need to be installed locally on a target system. In systems running Windows, it is possible for Trojans to install themselves as a service. After that, they will have administrative access. This means that they can run as a local system. A malicious individual can use these Trojans to steal credentials, passwords and any other sensitive information on the system. As the case with remote access Trojans, the backdoors attackers normally install come with inbuilt download and upload functionality. This technique relies on port 80 in the case of HTTP, 443 for HTTPS and port 53 for DNS for covering up their traffic.

A Covert Channel

This is a scenario where secret communication tunnels are used for transmitting data. Examples of such paths include HTTP tunnels, DNS tunnels, ICMP tunnels and VoIP. Take note that the covert channels we have mentioned can be used for transporting encrypted data as well. Detection of covert channels is possible. Only that it requires substantial efforts on the victim's part. There are indicators of anomalies in the traffic going out, such as protocol analysis, network signatures and flow data analysis. These require special tools to come across. Take note that the detection of a covert channel is one thing, but blocking it is a different ball game. You can employ one or more of the following measures.

- Barring outbound ICMP at the corporate information border;
- Blocking requests that are DNS related to servers outside corporate networks. The requests can be allowed for internal DNS servers;
- HTTP tunnels disposing through the leveraging of Web proxies;
- 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 in the same way an antispam software works.

Rootkits

This is a malware that is highly adept at concealing itself from a computer system. It is this feature that distinguishes rootkits from other malware types. Their heightened capability to hide gives them the ability to circumvent security measures that have been put in place on the computer. The main idea behind their creation is the very fact that they are not easily detected by normal malware detection software. Normally, Trojan horses are used to load rootkits beginning with "user" level access on the platform that is being targeted. Once in the target system, the rootkits will spy on login details such as passwords so that they can get "administrator" level access. Keen readers will say this is privilege escalation. That is correct. Despite this, the real specialty of the rootkits is to maintain access.

Rootkits will tend to hang around a targeted system slowly and progressively undermining it. This is unlike the norm with ordinary viruses that are designed to cause maximum damage in as little time as possible. The keyword here is 'secrecy.' For instance, keyloggers possessing rootkits are purposely built to capture all the words an unknowing victim keys in using their keypad. It will collect sensitive information for as long as it remains undetected. This makes identity theft highly probable. A good analogy is a parasite which, through various means, enters the body. It will stay dormant for a very long time. After it has mustered up enough energy to surmount over the body's immune system, it will now go ballistic.

A computer system can be broken down into three basic layers. These are the operating system, the kernel and the hardware level. The kernel is the backbone of the operating system, essentially speaking. Many a time, low-priority processes are used by user-level rootkits to compromise the software tasked with safeguarding a computer. A dangerous and stealthier rootkit is the kernel-level rootkit. This is majorly due to the following reasons:

- Time and again, the removal of boot-level and kernel-level rootkits have been proven to be difficult.
- The rootkits that have made a residence in the kernel memory do not leave any traces on the hard disk normally. Additionally, these rootkits normally change parts of the disk, files and sometimes modify the kernel to enable them to become "reboot resistant."
- Rootkits can camouflage their presence in cases where they make the addition of their code to sectors of the kernel;
- Kernel-level rootkits can run even before the operating system starts;
- This category of rootkits can bypass encryption through the creation of secret channels to allow them unfettered access to the compromised system.

Rootkits that are installed at the kernel level will acquire complete administrator access to the targeted systems. Rootkits normally create an access path right to the operating system level, unlike Trojan horses.

Removing rootkits

The typical security measures, for instance, antivirus software, cannot sufficiently deal with rootkits on their own. Alternatively, we have purpose-built programs such as Malwarebytes Anti-rootkit, TDSSKiller, Sophos Anti-Rootkit, and GMER that you can use to eradicate rootkits from your system. Note that, in some cases, the rootkit cannot be removed from your system for good. The programs above can only reduce the adverse effects that the rootkit leaves all over your system. In addition to using software to deal with rootkits, a user can also opt to initiate the clean slate procedure. Here, the important files are backed up, and a clean re-installation of the operating system is done. Normally, this will ensure that the rootkit is removed from your system. Again, this is not a guarantee that the removal will be 100%. We have BIOS-level rootkits, which are rare but can survive the re-install. We will always have signs indicating a presence of rootkits in any system, no matter how hard they try to hide. This is major because they are designed to keep an ingress path for an attacker from outside.

Data Exfiltration

This can be described as an unauthorized transfer of data to an external device or system. The data can originate from IT servers or a computer system. The process can either be manual (copy-pasting) or automatic (through malware). Back in 2015, the security organization, McAfee, reported that the majority of the data exfiltration cases (Around 60%) were carried out through direct electronic means. The remaining 40% happened via physical media, for example, stealing a laptop or using a USB drive to download data. Interestingly, a significant portion of that 40% involved mobile phones. The data categories which were most exfiltrated were personal health information, personally identifiable information, financial data and intellectual property. Different kinds of tunneling protocols, file transfers, web protocols or email transfers are used in the electronic exfiltration of data. We know that the file transfer protocol is a standard network protocol meant to help us transfer files. It can also come in handy in data exfiltration campaigns.

Peripheral devices on the targets and other components such as microphones and webcams can be rigged to enable the monitoring of the target's activities. To stay anonymous, the hacker can use the Tor network or make use of HTTP file transfers. To prevent hackers from exfiltrating your data and staying safe from Advanced Persistent Threats, early detection is what will make the difference. It is important that organizations possess a working threat intelligence mechanism that will aid in the identification of suspicious activities relating to data exfiltration. Linking the local threat intelligence system to the global threat intelligence network will help in keeping abreast of the latest trends in the security realm. Let me list some notable indicators of data exfiltration. These can be used as a platform to launch a comprehensive investigation. They are:

- Port activities that are not approved/sanctioned.
- Multiple email transmissions to non-corporate domains
- Excessive email sending by hosts
- Above normal DNS queries
- Web upload activity by the users. The uploads will normally be directed to non-corporate sites.

As I conclude this sub-topic, you have learned that for an attacker to obtain meaningful information, they will have to linger around their targets for some time. That implies that “Maintaining Access” is a key cycle of the hacking process which you will be required to master. This is easier said than done. Kali Linux comes with plenty of tools that can help you maintain access to a targeted system. Maintaining access is like getting into somebody else’s house without their permission. You will quickly realize that getting inside the house is just one part. Maintaining your presence without being detected is another. It may be even more difficult than the former task.

Clearing Tracks

In this step, we will be learning about how hackers cover their tracks with the objective of erasing any digital signs they may have left behind. It is obvious that this as an unethical activity. Simply put, it is concerned with the deletion of logs of the activities which took place during the hacking process. I am going to be very detailed in the covering of this sub-topic since it is of immense importance to the readers who seek to be professional hackers. There is one more process after clearing tracks, that is report writing, which is mostly paperwork. To know if a system has been targeted, we can carefully examine digital signs left behind by an intruder. It is in a hacker's interest to clear any traces of such activity that can lead to them. You may have noticed that in the previous phases, a penetration tester or hacker successfully avoided detection by intrusion detection systems and firewalls. In this phase, however, the objective is to conceal any hints that are likely to disclose the nature of the hacker's deeds.

The key components of covering/clearing tracks are:

1) Anti-Incident Response – these are measures that are meant to prevent real-time detection and,

2) Anti-Forensics – these are measures aimed at thwarting the collection of digital evidence during a possible post factum inquiry.

Anti-Incident Response

The main objective of Anti-Incident Response is to disrupt, confuse and out-maneuver the incident response team at work in the company, which was targeted. Additionally, activities falling under this category make it possible for a hacker/penetration tester to obtain a long-term foothold within their target even after they have been detected. Crucial tasks that can be carried out under anti-incident response include:

- Deployment of backdoors secretly
- Configuration of infrastructure to allow for agility in lateral movement
- Constantly updating the number of infected hosts. Also, their numbers should not be too large.
- Using a wide variety of malware on the network.
- Preventing investigators or responders from keeping up with what is going on by way of picking up the pace yourself.
- A perfect cover for internal hop-points can be provided by busy servers
- You can also use busy file servers as avenues for data staging.
- Using a VPN for communication in some cases may circumvent some measures put in place for network monitoring.

- Camouflaging the origin of malware transmission

The actions are undertaken in the prevention of immediate detection of an ongoing, or a continuous cyberattack is what matters when it comes to the working of an anti-incident response. The deliberate measures undertaken by hackers or penetration testers to destroy any evidence present and lead to a digital investigation to die out during the initial stages, anti-forensics, on the other hand, is designed to handicap the investigators' ability in obtaining adequate digital evidence that will be submitted before a court of law during later stages. This, therefore, implies that activities under anti-incident response are urgent since a large portion of the action occurs on a live, running system in real-time. The countermeasures that the incident responders are likely to take are presumably much more time-constrained as compared to those by investigators in a potential digital investigation in the future.

Anti-Forensics

Before we start devouring this topic, let us first understand what forensics is. We define computer forensics as a discipline whose main objective is to enable the acquisition, preservation, analysis and presentation of digital evidence in a court of law by forensic experts. We define anti-forensics as a discipline that encompasses all the existing means and tools for purposes of deleting, modifying, or hiding digital evidence. The main objective of anti-forensics is the destruction, erasure, or manipulation of digital evidence. Anti-forensics has also been described by some as the "Attempts made to negatively compromise the quality, amount, and the 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." One can tell from the name that this is involved with the techniques or actions that are supposed to create obstructions to an eventual digital investigation and to reduce both the quantity and quality of digital evidence. Cyber terrorists, hackers, counterfeiters, online pedophiles and other cybercriminals are among the typical users of anti-forensic techniques and tools. It is obvious that their intentions are to erase any existing traces capable of incriminating them.

Deleting Evidence

There are those of us who are so paranoid to the extent that they have invested resources on privacy protection tools and commercial disk cleaners solely to wipe data they do not wish others to lay their eyes on. It is believed that these tools can permanently delete everything from the hard disk. The specific information that can be deleted include:

- Web browsers history and cache
- Instant messengers chat logs including Skype and others
- Giving users a "secure delete" option with which they can wipe files
- Carry out the cleaning of these: registry items, thumbnails, jumplists, Skype chatsync and so on.

A forensic expert can use specific forensic tools to outsmart many of these clean-up programs. For example, pictures of interest to a forensic expert can be recovered. This is because even with the erasure of the original image, Windows Thumbnails will still have a smaller version of this picture. Even with the removal of the thumbnail, forensic can restore it by doing what we call file carving. Jumplists can also give information pertaining to pictures, applications, documents and numerous other types of files that the user has interacted with. The jumplists are normally created even for externally accessed files.

They will stay intact, regardless of whether there has been an erasure of the original file or that the external device has been removed. These lists will typically have a MAC address, the name, the path to the file being accessed, the application used to view the file, the computer name, alongside the time and date that the item was accessed. This implies that jumplists can be used as an excellent proof of access. Deleting Skype history manually will not clean internal data stored in the "chatsync" folder. The folder's content can be used to unearth bits of user conversations. Despite the methods imperfectness (Deleting), when it is done properly, it can dispose of evidence irreversibly, leading the forensics experts to come out empty-handed.

Hiding, Moving, Renaming or Altering Files

This may sound naïve even though some of the wrongdoers can use this method to evade detection. The method used to cover tracks here can include renaming files, moving files containing conversation histories or changing file extensions. This, my friends, is not an easy task. There exist programs which can be used to break large files into small partitions. These partitions can be concealed at the end of other files. Using specialized programs, a hacker can use the unused file space, which is known as slack space, for hiding crucial information from plain sight. Additionally, a hacker can conceal a file inside another (You may have heard of stenography). This method works fine with executable files.

Timestamping

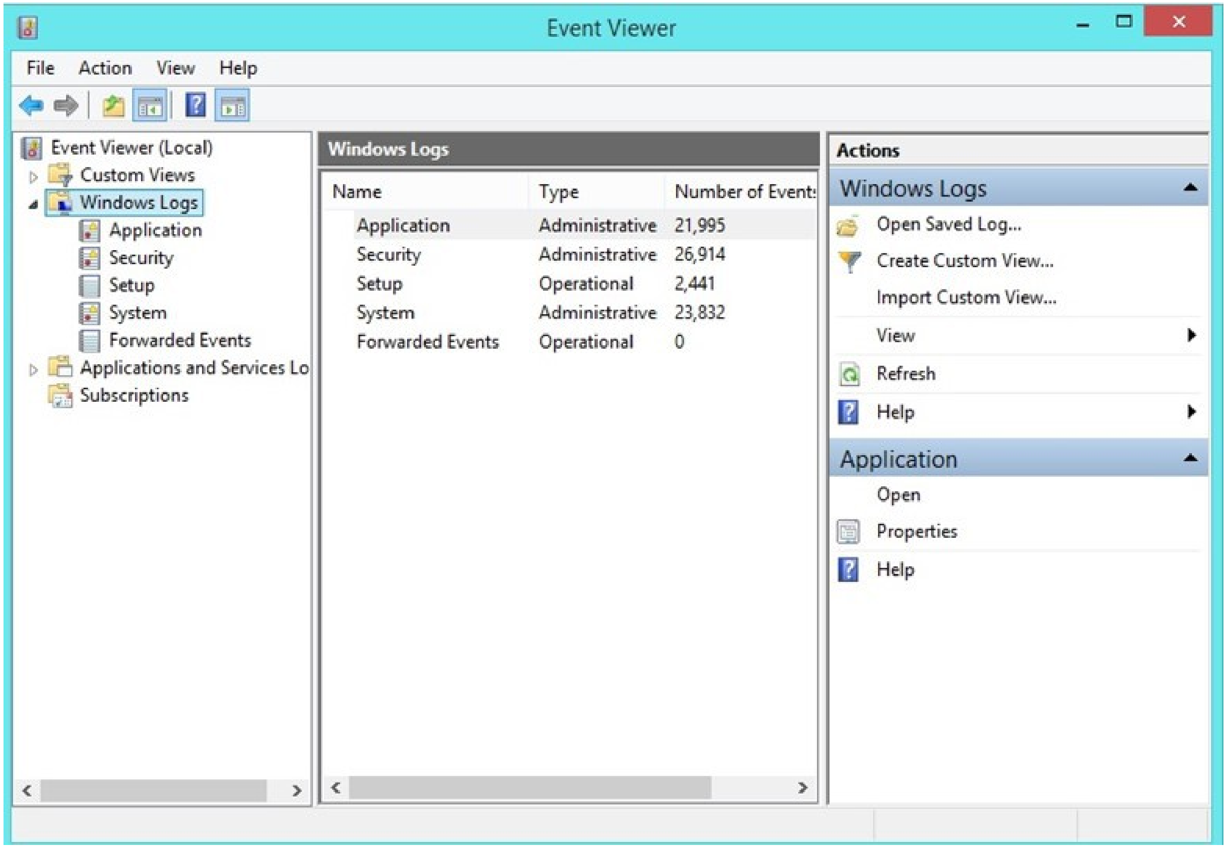
Many a time, the investigators do not normally examine all the files in a computer system. In most cases, they sort the information chronologically so that they can prioritize their search for potentially relevant information. They will want to view the information just at the time an attack occurred in cases where it is known. Criminals will typically attempt to counter this approach through the modification of the metadata belonging to the files they require. Usually, they alter the times and the dates when each file was last accessed, last modified and when it was created. This anti-forensic technique is known as time stamping. Once the modification or transformation of a file has been done, the computer or device will think that the file is a different one. For instance, renaming an mp4 file to make it look like a .gif file.

Despite this, forensic investigators will normally depend on their experience and skills to find moved or renamed files. Also, we have methods for information forensics that can assess hard drives for suspicious discrepancies automatically. An example of such a method is data carving. This is a method that is used for carrying out a comprehensive and sequential scan of media. Data carving is effective in the sense that it can directly read low-level data from the media. It does not depend on the manner in which the file locations and names appear on the file system. For instance, an mp3 file is identified based on the contained actual data stream that is inherent to mp3 files and not based on the file’s name.

Finally, encryption is a wonderful security measure a hacker can use. As far as digital forensics is concerned, encryption is a nightmare. Utilizing a strong encryption algorithm can result in the data being unreadable and will, therefore, be useless to the investigators.

Log Tampering

In computers running Windows, log files are typically kept in the event viewer. You can easily find it using the “Search” bar. The logs are stored in the/var/log directory in most Linux/UNIX operating systems.



Name	Type	Number of Events
Application	Administrative	21,995
Security	Administrative	26,914
Setup	Operational	2,441
System	Administrative	23,832
Forwarded Events	Operational	0

System administrators can view any malicious activities that have occurred in their systems simply by examining the log files. We have two types of log files, the application generated and the system-generated log files. In log manipulation, a hacker normally has two options. One way is to completely delete the logs and the other way is to modify the contents of the log files. Here, a hacker can also replace the system binaries with malware such as Trojans to make sure that any evidence of cyber intrusion will not be detected. Deleting log files is not normally a good idea as it will create a gap in the logs files and this will raise suspicion. The log files can be used in the detection of malicious activities. They can be used as a warning system on the health and the actual state of a system. Any discrepancies in the logs will likely draw unwanted attention. A wise attacker will likely carry out his attacks when the probability of viewing the log data is minimal say on weekends or during nighttime. An attacker will need to have root privileges to tamper with the information on log files. After escalating their privilege, a hacker can modify the log data associated with their activities within the log file itself. Any scrutiny by a system administrator will, therefore, not display any unusual activity. Prudent system administrators normally set up their system in a way that they will send all the log files to a remote server.

In summary

One precondition for success is being stealthy. Therefore, preventing detection during the hacking process is not enough. The process should continue even after the actual attack has been carried out. Any missteps will likely set off the radar detection and the forensics team will be quickly brought in to identify the attacker. This implies that the final step of covering tracks is of immense significance and should not be underestimated. If you wish to break into sophisticated systems, maintaining a low profile is a key skill that you will be required to have. We can say that covering tracks is a fail-safe technique that hackers employ to keep them out of trouble. The trouble can be immediate or after some time, say during an investigation.

Chapter 4: Wireless Network Hacking

Wireless Hacking

There are many advantages to using wireless networking. However, this kind of technology comes with a host of threats and vulnerabilities that hackers can take advantage of. Since information is sent over the air via radio frequencies, it is easier for hackers to intercept it compared to wired connections. This is more so when the information being sent is not encrypted or the encryption algorithm is weak.

Wireless networks consist of for basic elements:

- A wireless access point that connects to the network
- Data being transmitted via radio frequencies
- The Client device used, such as a laptop, tablet, etc.
- The users

Every one of these elements can be targeted by a hacker to compromise at least one of the three major objectives of a secure network: availability, integrity and confidentiality.

Wireless Network attacks

1. Accidental association

It is possible for a wireless network to be hacked accidentally. In some cases, one wireless network overlaps with another, thus enabling any user to jump into another unintended network accidentally. This may seem benign, but a malicious hacker can take advantage of this and gain access to information that should not have been exposed in such a manner. If the overlapping networks belong to organizations, then the link can be used to steal proprietary data.

2. Malicious Association

This occurs when malicious hackers gain access to a private network using their own device rather than through the legitimate access point (AP). A hacker can create a "soft AP," which can be a laptop with software that makes its wireless network card appear to be a genuine access point. This allows the hacker to steal passwords, attack computers or send users Trojan horse programs. A hacker can effectively have full control of every computer that joins the fake network.

3. Ad-hoc Networks

These are networks between two wireless computers with no access point separating them. Such networks can be attacked quite easily since they rarely have adequate protection.

4. Non-traditional networks

These include Bluetooth devices, wireless printers, handheld PDAs and barcode readers. These kinds of networks are rarely secured by IT personnel since all the focus is usually on laptops or access points. This makes them fair game for malicious hackers.

5. MAC Spoofing

This is a form of identity theft where a hacker monitors network traffic to identify which computer has network privileges. The aim is to steal the MAC (Media Access Control) address of that computer within the network. Many wireless systems have a MAC filter that allows only specific computers with specific MAC addresses to access and use the network. A hacker may get software that is able to "sniff" the network to find these authorized computers and their IDs and then employ other software that allows the hacker's computer to use these stolen MAC addresses.

6. Man-in-the-middle Attacks

This occurs when a malicious hacker sets up their laptop as a soft access point and then lures other users to use it. The hacker then connects the soft access point to a genuine access point using a different wireless card, thus forcing users to go through the fake AP to reach the real one. This enables the hacker to sniff out whatever information they want from the traffic. This type of attack has been made easier by software such as AirJack and LANjack. Wireless Hotspots are a great place to launch this kind of attack since there is hardly any meaningful security on such networks.

7. Denial of Service Attacks

This is where a hacker continuously sends numerous requests, commands and messages to a specific access point until the network crashes or just to prevent genuine users from getting onto the network.

8. Network Injection Attack

A malicious hacker injects counterfeit networking re-configuration commands into an access point that does not filter traffic. These fake commands bring down the entire network or switches, routers and hubs, forcing a reboot or reprogramming of every networking device.

Wireless Network Authentication
Wireless networks are designed to be accessible to anyone who has a wireless-enabled device. For this reason, most networks are protected using passwords. There are two common authentication techniques used: WEP and WPA.

WEP

This stands for Wired Equivalent Privacy and was developed to provide users with the same level of privacy as wired networks. It adheres to IEEE 802.11 WLAN standards. WEP encrypts data that is being sent over a network to prevent eavesdropping.

WEP vulnerabilities
There are significant flaws in the design of this type of authentication technique:

1. It uses Cyclic Redundancy Check 32 to verify the integrity of packets. The problem with CRC32 is that a hacker only needs to capture two packets to crack into the network. They can also modify the checksum and encrypted stream to force the system to accept the packet.

2. It uses an RC4 encryption algorithm to make stream ciphers composed of a secret key and an Initial Value (IV). The IV length is fixed at 24 bits, but the secret key can be 40 to 104 bits in length. If a secret key of a lower length is used, the network becomes easier to hack.

3. Since it is a password-based authentication technique, a hacker can successfully deploy a dictionary attack.

4. It does not have a central key management system, thus making it very difficult to change keys in big networks.

Due to the numerous security flaws, WEP has fallen out of favor and replaced by WPA.

How to crack WEP networks

Exploiting the numerous security vulnerabilities on a WEP network is possible either through passive attacks or active cracking. If a passive attack is launched, the network traffic is not affected until WEP authentication has been successfully cracked. This makes it harder to detect. Active cracking tends to increase the load on the network, thus making it easier to detect, though it is also more effective.

The tools that can be used for cracking WEP include:

Aircrack — This is also a network sniffer and can be downloaded from www.aircrack-ng.org/

Kismet — This multi-purpose tool can sniff network packets, detect invisible and visible networks and even identify intrusions. It can be downloaded from www.kismetwireless.net/

WEPCrack — This open-source tool can crack secret keys and can be downloaded at www.wepcrack.sourceforge.net/

WebDecrypt — It cracks WEP keys using a dictionary attack and generates its own keys. Get it at www.wepdecrypt.sourceforge.net/

WPA

WPA is an abbreviation for Wi-Fi Protected Access. It was primarily developed to mitigate the weaknesses of WEP. WPA uses greater IV than WEP, 48 bits to be precise. Packets are encrypted using temporal keys.

WPA vulnerabilities

1. Hackers can easily overcome it using denial of service attacks.
2. Its keys rely on passphrases and if weak passphrases are used, a dictionary attack can be successfully launched.

How to crack WPA networks

Since WPA uses passphrases to authenticate user logins, a well-coordinated dictionary attack makes it vulnerable, especially if short passphrases are used. The tools for cracking WPA include:
Cain and Abel — It is used to decode files that have been sniffed by other programs like Wireshark.
CowPatty — This is a brute force attack tool that cracks pre-shared keys. Download from wirlessdefenc.org/Contents/coWPAttyMain.htm

How to crack network WPA and WEP keys

You are going to need the right software, hardware and patience in order to crack the keys to a wireless network. However, successfully doing so is dependent on the activity levels of users within the network you have targeted.
Backtrack is a great security operating system that is based on Linux. It contains many well-known tools that are very effective for collecting data, evaluating weaknesses and exploiting networks. Some of these tools include Metasploit, Ophcrack, Wireshark, Nmap and Aircrack-ng.

Cracking network authentication keys requires the following:

- Wireless network adapter able to inject packets.
- Backtrack OS, downloadable from backtrack-linux.org/downloads/
- Proximity to the network radius.

- Adequate knowledge of Linux OS and how to use the scripts in Aircrack.
- Patience, as there are factors that you may not be able to control.

Remember, the greater the number of people actively accessing the network, the faster this will work.

How to perform MAC spoofing

To carry out MAC spoofing, you will have to bypass the MAC filtering that the target network is using. MAC filtering is commonly used to lockout MAC addresses that have not been authorized to connect to a wireless network. This is usually an effective way to prevent people who may somehow acquire the password from connecting to the network. However, MAC filtering is not an effective security measure when it comes to locking out hackers.

The steps below will show you exactly how to go about spoofing the MAC address of a client who is authorized to connect to the network. The Wi-Fi adapter should be in monitoring mode. Airodump-ng on Kali Linux will be used to recover the MAC address. After this, the Macchanger program will be used to do the spoofing, bypass the filter and connect to the network.

Instructions:

1. Make sure your Wi-Fi adapter is in monitoring mode. To find the wireless network that is being targeted as well as any clients connected to it, enter this command:

```
Airodump-ng—c [channel]-bssid [target router MAC Addres]-l wlan0mon
```

A window will open up, displaying a list of clients who are connected to the network. Their whitelisted MAC addresses will also be shown. These are the addresses you need to spoof to enter the network.

2. Pick one of the whitelisted MAC addresses from the list to use to spoof your own address. Before you can perform the spoofing, you must take down the monitoring interface. Enter the command:

```
Airmon-ng stop wlan0mon
```

3. The next step is to take down the wireless interface of the MAC address you intend to spoof. Enter the command:

```
Ifconfig wlan0 down
```

4. Then you use the Mcchanger software to change the address. Enter the command:

```
Macchanger —m [New MAC Address] wlan0
```

5. Remember, you had taken down the wireless interface in step 3. Now it is time to bring it back up. Use the command:

```
Ifconfig wlan0 up
```

Now that the MAC address of your wireless adapter has been changed to that of an authorized user, test and see if the network will authenticate your login. You should be able to connect to the wireless network.

Transmissions

Hacking of wireless networks poses three main threats: Disruption, Alteration and Interception. To prevent malicious hackers from eavesdropping on wireless transmission, you can use:

Signal-hiding methods — Before a malicious hacker can intercept wireless transmissions, they first have to locate the wireless access point. An organization can make this more difficult by switching off the SSID (service set identifier) being broadcast by the access point, assigning a cryptic name to the SSID, lowering signal strength to provide just enough requisite coverage or stationing access points away from exterior walls and windows. There are also more effective but expensive techniques, such as employing directional antennas to restrict the signal within a specific area or using TEMPEST (a technique to block the emission of wireless signals).

Stronger encryption of all wireless traffic — This is very important, especially for organizations that must protect the confidentiality of their information being broadcast wirelessly. This measure reduces the risks of a man-in-the-middle attack.

Stronger authentication procedures — This should apply to users as well as their devices. This minimizes man-in-the-middle attacks.

Countermeasures against Denial of Service Attacks

Malicious hackers may, at times, attempt to bring down the servers of an organization, but in some cases, a DOS attack may be unintentional. There are certain steps that can be taken to minimize the risks of this form of attack:

- Performing site surveys carefully to determine the location of signals emanating from other devices. This should be used as a guide in deciding where the access points should be located.
- Conducting regular audits of network performance and activity to determine areas with problems. If there are any offending devices, they should be removed. Measures should also be taken to enhance signal coverage and strength in problem areas.

Access Points

Wireless access points that are poorly configured are a major vulnerability and may allow malicious hackers unauthorized access to confidential information. To secure wireless access points, the following countermeasures must be taken:

- Eliminate all rogue access points — The best way to do this is to use 802. Ix to prevent any rogue devices from plugging into and connecting to the wireless network.
- Ensure all authentic access points are properly configured — Make sure that all default settings are changed since they are publicly available and hackers can easily exploit them.

- Authenticate every device using 802. Ix protocol — a strong authentication system will prevent unauthorized devices from setting up backdoors. This protocol ensures stringent authentication before assigning any device to an IP address.

Devices

There are two perspectives when it comes to assessing security threats against wireless devices: Theft/Loss and Compromise. Laptops and PDAs usually contain a lot of confidential and sensitive information and therefore must be protected from theft or loss. Wireless client devices can also be compromised when a malicious hacker gains access to stored data in the device. Hackers can also use the device to launch attacks on other systems and networks.

Networks

- Encryption — This is the best way to secure a wireless network. Most base stations, access points and wireless routers come with inbuilt encryption mechanisms that enable scrambling of network communications. Always make sure that the router you buy comes with an encryption feature. Most manufacturers turn this feature off, so ensure that you manually turn it on before you start using your router.

- Anti-spyware, anti-virus and firewalls — Make sure that your wireless network is protected in the same way as a wired connection. Keep all your software updated and always check whether your firewall is switched on.

- Switch off your router's identifier broadcasting - This is the mechanism that a wireless router uses for broadcasting its presence in an area. However, there is no need to announce the presence of a network if the users know that it is already there. Malicious hackers tend to search for the identifier broadcast to zero in on potential targets.

- Change default identifier — Every router has a default ID given to it by its manufacturer. You may have switched off the identifier broadcaster, but hackers can still attack the network if they find out the default ID, which is publicly accessible. Change the identifier and do not forget to configure the new ID into your computer.

- Change the default password — Every router is assigned a default password by the manufacturer. This is for purposes of configuring the device initially. These default passwords are easy to find, so make sure that you change your router password to something that will be very difficult to crack. Also, try to make your password as long as possible.

- Specify the devices authorized to connect to the network — Configure your router to only allow specific Mac addresses to connect to the network. However, do not rely on this technique alone, as Mac spoofing is still possible.

- Shut the network down when unused — Whenever a wireless network is not being used, make sure that it is switched off. This will limit the window of opportunity that hackers can use to penetrate the network.

- Be vigilant in W-Fi hotspots — Most people love to use the free Wi-Fi at airports, cafes, hotels and other public places. These wireless networks are rarely secured, so do not assume that they are.

The Users

There is no greater way to secure a wireless network than educating and training all users. Users are not just people who connect to the network but IT personnel and administrators as well. It is very important to teach people how to behave in a way that will maintain the security of the wireless network. This user training and education must be a periodic endeavor.

Let us face it. It is not possible to completely eliminate every risk that a wireless network comes with. Eventually, a hacker will get through. However, there are actions that can be taken to maintain a reasonable level of general security. This is possible using systematic risk evaluation and management techniques. Every component of a wireless network must be considered when establishing countermeasures against malicious hackers.

Chapter 5: Uses and Applications of Kali Linux

The uses of Kali Linux are wide-ranging. Below, I have outlined and discussed some of them. Feel free to download the documentation from the links provided in chapter 2. Now let us get down to the serious stuff.

Penetration testing

This is a mechanism that is utilized by organizations to ascertain the robustness of their security infrastructure. Here, security professionals will play the role of the attackers, whereby they will attempt to discover flaws and vulnerabilities in a system before the malicious fellows do. One key objective is the identification and reporting of vulnerabilities to companies and organizations. As organizations become increasingly security conscious and the cost of security breaches rises exponentially, many large organizations are beginning to contract out security services. One of these critical security services is penetration testing. A penetration test is essentially a legal, commissioned hack to demonstrate the vulnerability of a firm's network and systems. Generally, organizations conduct a vulnerability assessment first to find potential weaknesses in their network, operating systems and services. I emphasize potential, as this vulnerability scan includes a significant number of false positives (things identified as vulnerabilities that are, in reality, not vulnerabilities). It is the role of the penetration tester to attempt to hack, or penetrate, these vulnerabilities. Only then can the organization know whether the weakness is real and decide to invest time and money to close the vulnerability.

Espionage and military

Cyber espionage can be said to be the practice of accessing information and secrets without the knowledge and permission of the entities being targeted. They can be ordinary individuals, rivals, competitors, groups, governments or even enemies. The objectives here are broad. They can be political, economic, personal or even military-related. The techniques used, too, are diverse. Hackers can use malicious software, cracking techniques, proxy servers, among others, to attain their stated objectives. Espionage can be carried out online by professionals from their computer desks or it can be done by infiltration using trained moles and conventional spies. In some circumstances, it can be carried by amateurish hackers with malicious intent and software programmers. It is common knowledge that every nation on earth carries out some form of cyber espionage or even cyber warfare, albeit covertly. Gathering intelligence on military activities of other countries has been made more cost-effective by hacking. Thus, a hacker has their place cut out in the defense systems of any nation.

Forensics:
For years, the popularity of Forensic Linux Live Boot environments has become well known. There are so many forensic tools that are Linux based on this distribution. Using Kali, forensic experts can do all that pertains to their tradecraft starting from the initial triage, data imaging all the way to case management and full analysis.

Reverse Engineering:
Recently, reverse engineering has become an indispensable skill in various sectors, including law enforcement. Reverse Engineering is a primary method that is used in the identification of vulnerabilities and the development of exploits. That is on the offensive side of it. Defensively speaking, reverse engineering can be utilized in the analysis of malware that has been used to target a given system. Here, the objective will be to establish the capabilities of a given piece of tradecraft.

Wireless Attacks:
Kali supports a wide range of wireless hacking tools. What makes wireless networks a commonly attacked vector is their pervasive nature. Kali Linux also supports multiple wireless cards and is a hacker's favorite choice for conducting attacks against different types of wireless networks.

Password Attacks:
Kali Linux can be used for conducting password attacks where a user encounters an authentication system. The OS comes with numerous useful tools and utilities for this purpose. We have both offline and online password attack tools that a Kali Linux user can use to deal with hashing and encryption systems.

Database Assessment:

Kali Linux is capable of database attacks such as SQL injection and attacking credentials. All this is made possible by the tools present in Kali's vast repositories that can be used for testing attack vectors ranging from data extraction and analysis to SQL injection.

Sniffing and Spoofing:

Again, Kali Linux has plenty of tools an aspiring hacker or a professional one can use to get access to data as it is being transmitted over the network. You can use spoofing tools to impersonate a networks' legitimate user and then use the sniffing tools if you wish to capture and analyze data you have just captured. These tools are a lethal combination when used together.

Stress Testing

To check whether your system is stable, you carry out a stress test on it. In this scenario, you will use the numerous tools provided by Kali Linux to generate more than normal traffic. This way you will be able to know the limits of your system. The tools for stress testing can either be proprietary or open-source. As an expert, it is essential that you know all the tools that are used for testing a system's availability.

Hardware Hacking

Another application of Kali Linux is in hardware hacking. Kali Linux comes with the following tools that can be used to accomplish this task.

- **android-sdk** - The Android SDK provides you the API libraries and developer tools necessary to build, test and debug apps for Android.

- **apktool** - It is a tool for reverse engineering 3rd party, closed, binary Android apps. It can decode resources to the nearly original form and rebuild them after making some modifications; it makes possible to debug smali code step by step. Also, it makes working with the app easier because of project-like files structure and automation of some repetitive tasks like building apk, etc.

- **Arduino** - This is an electronics prototyping platform that is open-source. It is based on easy-to-use, flexible software and hardware.

- **Sakis3G** - Sakis3G is a tweaked shell script that is supposed to work out-of-the-box for establishing a 3G connection with any combination of modem or operator. It automatically setups your USB or Bluetooth™ modem and may even detect operator settings. You should try it when anything else fails.

- **Smali** - smali/baksmali is an assembler/disassembler for the dex format used by dalvik, Android’s Java VM implementation. The syntax is loosely based on Jasmin’s/dedexer’s syntax and supports the full functionality of the dex format (annotations, debug info, line info, etc.)

Chapter 6: Introduction to Cybersecurity

Introduction

We define cybersecurity as being the protection of computer systems, computer networks, and their associated programs from attacks that are of a digital form. Typically, cyberattacks are carried out with the intent of gaining access, modification or even destruction of information that is sensitive. They also attempt to extorting money from victims and are meant to interrupt the normal processes of a business.

Confidentiality, Integrity and Availability

The three are famously referred to as the CIA triad. We can describe it as a model whose purpose is to guide information security policies within any given organization. To prevent confusing the triad with the American Central Intelligence Agency, we sometimes refer to it as the AIC triad. The three elements are the most critical components of security. In our case, we can say that availability is defined as a guarantee of access that is reliable to information by people with authorization, confidentiality is said to be a set of protocols that are used to limiting access to information and integrity is the undertaking given to show that the information at hand is both accurate and trustworthy.

Confidentiality:
This is a rough equivalent of privacy. While ensuring that the right people can have access to crucial information, it is also prudent that vigorous measures are undertaken to make sure that there is confidentiality. There should be restricted access to the data in question by those who are authorized to view it. Out there, it is not uncommon to categorized data based on the type and amount of damage that can result from it falling into unauthorized persons. Stringent measures can more or less be implemented depending on these categories. Guarding the confidentiality of data sometimes requires specialized training for authorized to view/use

persons. It would generally involve security risks that could harm that information. It can, without a doubt, help people with the proper authorization to get to know the various risk factors and equip them with countermeasures. Additional aspects of the training may comprise best practices in password-related issues alongside social engineering mechanisms.

This will help them avoid breaching rules governing data-handling with potentially disastrous results in as much as they may have intentions we can describe as being noble. For example, using a routing number or an account number is an effective measure that can be used to ensure confidentiality. We can also employ the use of data encryption to make sure that there is confidentiality. Passwords and user IDs are part of a standard procedure that is becoming a common phenomenon, two-factor authentication. There are different options. They include security tokens (soft tokens or key fobs) and biometric verification.

Furthermore, it is incumbent upon the users to take precautions in ensuring that locations where their information appears and the number of times required to send it to complete a transaction is at a minimal. In cases where we have critical data, extra measures may be necessary. Such actions can involve storing the information on disconnected storage devices on air-gapped computers or it can even be stored in the form of hard copies only.

Integrity:

This component of the triad comprises ensuring the trustworthiness, consistency, and accuracy of data throughout its complete life cycle. It is of immense importance that data that is in transit is not altered. Solid steps need to be taken to make sure that no modification on the data by unauthorized people happens. For instance, in cases where we have a confidentiality breach. Here, the countermeasures can involve user access controls and file permissions. To prevent accidental deletion or erroneous changes by authorized users, we can employ the use of version control. In place, there also need to exist mechanisms to help in the detection of data changes, which may result from non-human events, including a server crash or an electromagnetic pulse. We can include checksums and cryptographic checksums to help with the integrity verification of data.

Lastly, it may be necessary to have some form of redundancies and backups that will help in the restoration back to its former state.

Availability:

The rigorous maintenance of all the hardware ensures that there will always be availability fo the services rendered by this hardware. Failing equipment should be promptly and adequately repaired to keep in order a properly functioning operating system environment that is devoid of any software conflicts. One aspect of maintenance that should also be carried out is updating all the necessary system components. It will also be to provide ample bandwidth for communications and to ensure a minimal occurrence of bottlenecks. Mitigation of hardware failures and their repercussions can be done using high-availability clusters, redundancy, RAID and even failovers.

For the worst-case scenarios that occur, disaster recovery that is both adaptive and fast is essential. For this to be possible, the disaster recovery plan laid down has to be comprehensive. Prevention of data loss or connection interruptions needs to also account for unpredictable events. Examples include fire and natural disasters. Copies of back up data can be securely stored at a location that is geographically-isolated to prevent loss of data resulting from such occurrences. Such sites also need to be water and fire-resistant. To guard against issues such as downtime and inaccessibility of data due to denial-of-service attacks and network intrusions, we can employ the use of extra security equipment, for instance, proxy servers, firewalls and software.

Issues arising from the CIA:

The CIA paradigm faces immense challenges where big data is involved. This is primarily because of the sheer volume needing to be kept safe, the variety of formats of the data, and, finally, the multiplicity of the originating sources. Disaster recovery plans and duplicate sets of data all make the already high cost even higher. Additionally, oversight is often lacking since the main objective of big data is for analytics purposes, i.e., gathering data and using it to make some kind of useful interpretation. We all know this fellow, Edward Snowden, who brought this issue to light. Security agencies carry out the collection of enormous volumes of peoples’ private data throughout the world. To safeguard individual information from exposure in the IoT environment, we have special considerations known as the Internet of Things privacy. This means that almost any logical or physical entity can be assigned a unique identifier to enable autonomous communications over a network, including the Internet.

The transmitted data from a particular endpoint may not, on its own, necessarily result in any privacy issues. The catch is, however, when the fragmented data from multiple endpoints is accessed, gathered and analyzed, sensitive information can be obtained. Securing the Internet of Things is itself a formidable challenge since it comprises numerous Internet-enabled devices besides computers. Such devices are, in most cases, often set up with default passwords that are weak or in some cases, the devices are unpatched. Unless IoT is protected adequately, there is a likelihood that it may be used as a separate vector of attack or be made a part of a thingbot. Recently, it has been demonstrated by researchers that it is possible to compromise a network just by using a Wi-Fi-enabled light bulb. It is essential for us that we consider the security of the numerous network-capable products that are under development.

Encryption

We define encryption as a mechanism through which plaintext or other data type are changed from their currently readable form to an encoded way. It is only an entity having access to a decryption key that can decode the data. This is an important measure that usually is used to provide end-to-end data security across networks. Encryption, as a proactive security measure, is commonly used all over the internet for purposes of protecting crucial information belonging to users, which is being exchanged between servers and browsers. That can include private information such as payment information, passwords and other personal information. Individuals, together with organizations, may also opt to use encryption to ensure the safety of sensitive data that is stored on mobile devices, servers and computers.

How encryption works

Plaintext data, also known as unencrypted data, is encrypted through the use of an encryption algorithm plus an encryption key. The result of this is a ciphertext that can be seen only in its original form if decrypted with the correct key. On the other hand, decryption is the reverse of encryption. The steps used in encryption are followed in a reverse fashion. In the modern age, we have two commonly used encryption algorithms. They are symmetric and asymmetric encryptions.

When it comes to the symmetric encryption mechanism, a single key is utilized for encryption. The Advanced Encryption Standard (AES) is one of the most used symmetric-key ciphers. It was designed primarily to protect classified information for governments. This mechanism is faster in comparison to asymmetric encryption. The sender must, however, share the encryption key with the recipient. The keys need to be managed in a secure fashion. This uses an asymmetric algorithm in most cases.

On the other hand, we have asymmetric cryptography. We can also refer to it as public-key cryptography. Here, two different keys are used. They are, however, mathematically linked. The keys are as follows; one key is public and the other one private. The public key many times can be shared with anyone. The private key has to be kept secret. In asymmetric cryptography, the commonly used encryption algorithm is the RSA. The reason is to some extent that the two keys can encrypt a message, which is to imply the key that is opposite to the one used for the encryption is used to decrypt it. This feature offers a way of ensuring that we not only have confidentiality but also authenticity, non-reputability and integrity of electronic communications and data.

Benefits of Encryption

Confidentiality of digital data, which is stored on computer systems or that which is sent through the internet or any other computer network, is protected by using encryption. Organizations such as Payment Card Industry Data Security Standard (PCI DSS) require that sensitive data be encrypted to keep unauthorized entities from accessing the data. We also have some standards requiring or recommending data encryption. Nowadays, modern encryption algorithms serve an integral role in making sure that the security of communications and IT systems possess not only confidentiality but also the under listed key elements of security:

- Authentication: the origin of a given message should be able to be verified.
- Integrity: This has got to do with keeping the message intact. That is, the contents of messages have not been altered or deleted from the time it was sent.
- Nonrepudiation: Here, non-repudiation means that a particular sender cannot dispute that they send the message.

Backup and Redundancy

Usually, we use backup where copies of data are created in anticipation of a catastrophic loss. On the other hand, redundancy is a lot more than just data storage. Redundancy aims to provide a continuity of service regardless of what will happen. Data redundancy ensures that the storage of data is done at multiple and heterogeneous locations. We also have what we call network redundancy whereby a given network is configured in such a way that it has numerous alternative systems. The alternative systems serve to ensure continuity of service regardless of what happens.

Data Redundancy

For any organization, it is essential first that regular services are restored as soon as possible after there has been a security breach. Data should be able to be reconstructed as quickly as possible. To this end, businesses have come up with various ways to make sure there is data redundancy. It is common knowledge that these methods come with their own merits in terms of cost-effectiveness, speed and management. The most common way is using off-site tape backups. In this method, magnetic tapes are used to store a complete bit-for-bit copy of a storage volume. The tapes can be transferred to an off-site storage facility where they can be easily retrieved whenever there is a catastrophic failure. Besides, we can use Cloud Backup to safeguard data against losses.

Network Redundancy

Most of the infrastructure we use for our networks are unbelievably fragile. For instance, when a router burns out due to one reason or another, the result is that there will be a prolonged period of network downtime. To mitigate against this, businesses make sure that networks they use have an adequate redundancy so that they can survive and provide services in cases of an emergency. Fundamentally, network redundancy means that no matter what type of failure occurs, a network will still be up and running. To be able to do this, we can have multiple network devices such as hubs, routers and switches configured to stand in for one of them that fails. We also have ISP redundancy, where a gateway in the network is joined to more than one separate ISP. Just like with the devices, one ISP will take over whenever there is a failure. In cases where a network is functioning correctly, we can use the ISPs to share the traffic resulting in reduced congestion of the network. This here is called load sharing.

Preventing a SPOFF

SPOFF is full for a single point of failure. We do not desire that one critical part of a system failure can render the entire system unusable. Any planning needs to mitigate this phenomenon. A single point of failure can be reduced or eliminated by way of redundancy. This will make sure that there is not a single component that can prevent the proper working of a system.

Chapter 7: Network Scanning and Management

Introduction

The ability to scan for and connect to other network devices from your system is crucial to becoming a successful hacker, and with wireless technologies like WiFi
and Bluetooth becoming the standard, finding and controlling WiFi and Bluetooth connections is vital. If someone can hack a wireless connection, they can gain entry to a device and access to confidential information. The first step, of course, is to learn how to find these devices. In this chapter, we are going to examine two of the most common wireless technologies in Linux: WiFi and Bluetooth.

Network Scanning

We say that it is the utilization of a computer network for purposes of collecting information about IT systems. We carry out scanning of networks primarily to help us do system maintenance or a security assessment. Hackers can also conduct a network scanning exercise before launching their attacks. The following are some of the reasons we scan networks:

- Identification of the present TCP and UDP network services, which may be actively being executed on the targets.
- To get to understand the systems for filtering that are in between the targeted hosts and the user.
- Discover the operating systems that are being used through the assessment of their IP responses.
- Analyze a particular host that is being targeted for its number predictability of the TCP sequence. This is to enable the TCP spoofing and attack sequence prediction.

Network scanning comprises of two key aspects: vulnerability scanning and network port scanning. The latter denotes a way of sending data packets through a network over to a systems' specific port numbers. The goal is to discover network services that are present in that particular system. It is an excellent way for troubleshooting issues that a given system has. That way, the problems can be dealt with so that the system is secure. For us to discover known vulnerabilities present in network systems, a method known as vulnerability scanning is used. Through it, we can identify weak spots both in the operating system and the application software. It is these weak points that are usually used to compromise computing systems.

Both vulnerability scanning and network port scanning can be said to be techniques that are used in information gathering. On the flip side, they can be a prelude to an attack when they are put to use by anonymous entities. Such entities usually have malicious intentions. The inverse mapping is another technique for network scanning. It is useful when it comes to collecting IP addresses that are not mapped to live hosts. By doing so, it will be aiding in the focussing attention on addresses that are worth focussing on, that is, those that are feasible. There are three stages in which information gathering can be accomplished.

i. The footprinting stage
ii. The scanning stage
iii. The enumeration stage

This, therefore, implies that network scanning is among the crucial steps an attacker needs to be able to gather information.

Network scanning with ifconfig
The ifconfig command is one of the essential tools that can be used for examining and interacting with active network interfaces. You can use it to query your active network connections by simply entering ifconfig in the terminal.

Scanning Wireless Networks with iwconfig
If you have a wireless adapter, you can use the iwconfig command to gather crucial information for wireless hacking, such as the adapter's IP address, its MAC address, what mode it's in and more. The information you can glean from this command is particularly important when you're using wireless hacking tools like aircrackng.

Changing your network information

Being able to change your IP address and other network information is a useful skill because it will help you access other networks while appearing as a trusted device on those networks. For example, in a denial of service (DoS) attack, you can spoof your IP so that that the attack appears to come from another source, thus helping you evade IP capture during forensic analysis. This is a relatively simple task in Linux and it's done with the ifconfig command.

Changing Your IP Address

To change your IP address, enter ifconfig, followed by the interface you want to reassign and the new IP address you want to be assigned to that interface. For example, to assign the IP address 192.168.181.115 to interface eth0, you would enter the following:

```
Kali >ifconfig eth0 192.168.181.115
kali >
```

When you do this correctly, Linux will go back to the command prompt and say nothing. This is a good thing! Then, when you again check your network connections with ifconfig, you should see that your IP address has changed to the new IP address you just assigned.

Changing Your Network Mask and Broadcast Address

You can also change your network mask (netmask) and broadcast address with the ifconfig command. For instance, if you want to assign that same eth0 interface with a netmask of 255.255.0.0 and a broadcast address of 192.168.1.255, you would enter the following:

```
Kali >ifconfig eth0 192.168.181.115 netmask 255.255.0.0 broadcast
192.168.1.255
kali >
```

Once again, if you've done everything correctly, Linux responds with a new command prompt. Now enter ifconfig again to verify that each of the parameters has been changed accordingly.

Spoofing Your MAC Address

You can also use ifconfig to change your MAC address. The MAC address is globally unique and is often used as a security measure to keep hackers out of networks —or to trace them. Changing your MAC address to spoof a different MAC address is almost trivial and neutralizes those security measures. Thus, it’s an instrumental technique for bypassing network access controls. To spoof your MAC address, use the ifconfig command’s down option to take down the interface (eth0 in this case). Then enter the ifconfig command followed by the interface name (hw for hardware, ether for Ethernet) and the new spoofed MAC address. Finally, bring the interface back up with the up option for the change to take place.

IP Addresses assignment

Linux has a Dynamic Host Configuration Protocol (DHCP) server that runs a daemon, a process that runs in the background, called dhcpd or the dhcp daemon. The DHCP server will carry out the assignment of IP addresses to all of the systems that are located on the subnet. It also keeps a log of which IP address is allocated to which machine at any one time. This makes it an excellent resource for forensic analysts to trace hackers after an attack. For that reason, it’s useful to understand how the DHCP server works. Usually, to connect to the internet from a LAN, you must have a DHCP-assigned IP.

Therefore, after setting a static IP address, you must return and get a new DHCP-assigned IP address. To do this, you can always reboot your system, but I will show you how to retrieve a new DHCP without having to shut your system down and restart it. To request an IP address from DHCP, all that is required is to call the DHCP server using dhclient, followed by an interface that you wish to assign the address. The different Linux distros use different DHCP clients. Kali, for instance, is based on Debian that uses dhclient.

Manipulating the Domain Name System (DNS)

Hackers can find a treasure trove of information on a target in its Domain Name
System. This is a key element of the internet and although it's designed to translate domain names to IP addresses, a hacker can use it to garner information on the target.

- **Examining DNS with dig**

DNS is the service that translates a domain name like google.com to the appropriate IP address. This way, your system knows how to get to it. Without DNS, it would mean that we would be required to remember the thousands of IP addresses that belong to the websites we visit frequently. Dig is one of the commands any aspiring hacker needs to know. It offers a way to gather DNS information about a target domain. The stored DNS information can be a crucial piece of early reconnaissance to obtain before attacking. This information could include the IP address of the target's nameserver (the server that translates the target's name to an IP address), the target's email server and potentially any subdomains and IP addresses. You can also use the dig command to get information on email servers connected to a domain by adding the mx option (mx is short for mail exchange server). This information is critical for attacks on email systems.

- **Changing Your DNS Server**

In some cases, you may want to use another DNS server. To do so, you will edit a plaintext file named /etc/resolv.conf on the system. Open that file in a text editor. Then, on your command line, enter the precise name of your editor, followed by the location of the file and the filename.

Wi-Fi Networks
Firstly, let us look at WiFi. Before doing so, here is a small introduction to the various WiFi security protocols that usually are frequently used. The original, Wired Equivalent Privacy (WEP), was severely flawed and easily cracked. Its replacement, WiFi Protected Access (WPA), was a bit more secure. Finally, WPA2PSK, which is much more secure and uses a

preshared key (PSK) that all users share, is now used by nearly all WiFi AP’s (except enterprise WiFi).

Basic Wireless Commands

ifconfig

To perform a network interface configuration in Unix-based operating systems, one needs ifconfig. It is an administration utility that is found in the system. Ifconfig has utilities that are utilized in the configuration, querying and controlling of the parameters of the TCP/IP interface. As an interactive tool, ifconfig can be used to show settings of the network interface and analyze them.

In summary, ifconfig does the following:

- The command enables the viewing of settings of a network;
- Carrying out enabling of a network Interface and also disabling it;
- Network Interface IP address assigning ;
- Assigning network interfaces a netmask ;
- Allocating a Broadcast to Network Interface;
- Assigning an IP, Netmask and Broadcast to Network Interface;
- Changing MTU for a Network Interface;
- Enabling and disabling Promiscuous Mode;
- Addition and removal of New Alias to Network Interface;
- Changing the MAC address of Network Interface.

iwevent

This command displays Wireless Events received through the RTNetlink socket. Each line shows the specific Wireless Event, which describes what has happened on the specified wireless interface. This command doesn't take any arguments.

iwlist

This command can be used for scanning wireless networks available and also for displaying any other information about the wireless networks which are not displayed when the iwconfig command is used. Iwlist is utilized in the generation of wireless access points that are nearby together with their SSIDs and their MAC addresses.

iwspy
This command is used for monitoring nodes in a network. It can also be used for recording the link quality of the nodes.

ifrename
This command is used for renaming wireless network interfaces depending on multiple criteria that are static to allocate names consistently to each interface. The interface names usually are dynamic by default. This command helps users decide the name of the network interface.

iwgetid
This is used in the reporting of the NWID, ESSID or address of the access point of the wireless network presently being used. By default, iwgetid will display the devices' ESSID. Suppose that it is unavailable, it will output its NWID instead. The information reported is the same as the one shown by iwconfig. In comparison, it is easier to do integration in various scripts.

Detecting and Connecting to Bluetooth

In recent times, nearly all gadgets, systems and devices have inbuilt Bluetooth. The devices can be computers, iPods, smartphones, speakers, game controllers, keyboards, tablets, among others. The ability to break into Bluetooth networks can result in the compromising of the information on the device, assuming a devices' control and acquisition of a platform to transmit privileges information from and to the device, among other things. We, therefore, need to understand how Bluetooth works if we are to exploit this technology. From this book, you will be able to acquire some basic knowledge that will come in handy during the scanning and connecting to Bluetooth devices in preparation for hacking them.

How Bluetooth Works

First, we can define Bluetooth as a wireless communication technology that enables devices to transmit voice or data wirelessly. This happens over a relatively short distance. This technology was meant to replace the ubiquitous cables that were being used to connect devices while still securing the communications across them. The process of joining two Bluetooth devices is known as pairing. Pretty much any two devices can pair if they are set to a discoverable mode. In the discoverable mode, a Bluetooth device will broadcast the following information about themselves:

- Technical information
- Name
- List of services
- Class

Upon pairing, two Bluetooth devices will exchange a link key. The devices will store the key to be used in the identification of the other device in future pairings. Every device has a unique identifier and usually a manufacturer-assigned name. These will be useful pieces of data when we want to identify and access a device.

Bluetooth Scanning and Reconnaissance

Linux has an implementation of the Bluetooth protocol stack called BlueZ that we are going to use to scan for Bluetooth signals. Most Linux distributions, including Kali Linux, have it as an inbuilt feature by default. BlueZ possesses utilities that can help us scan and manage Bluetooth capable devices. Examples of the utilities are outlined below:

- hciconfig: this is an equivalent of ifconfig in Linux, but made for Bluetooth capable devices.
- hcitool: this is a tool that we use to perform inquiries. The inquiries can be the device ID, name, class or even its clock information. This helps the devices to work in sync.
- hcidump: sniffing of Bluetooth communications is carried out by this tool, it, therefore, gives us a chance to capture data that is being sent over the Bluetooth signal.

The first scanning and reconnaissance step with Bluetooth is to check whether the Bluetooth adapter on the system that we are using is recognized and enabled so we can use it to scan for other devices.

Scanning for Bluetooth Devices with hcitool

Now that we know our adapter is up, we can use another tool in the BlueZ suite called hcitool, which is used to scan for other Bluetooth devices within range.

With the simple scan command, we can find out Bluetooth devices that are transmitting using their discover beacons. That is, the devices set to their discovery mode. Most of the tools for Bluetooth hacking you are likely to encounter will be using these commands in a script. You should be able to create your tools from these commands using Python script or even bash script.

Using the sdptool to scanning for services

The service discovery protocol, SDP, as it is commonly known, is a protocol of Bluetooth that is used in the searching of Bluetooth services (Bluetooth is a suite of services), and, helpfully, BlueZ provides the sdptool tool for browsing a device for the services it offers. It is also important to note that the device does not have to be in discovery mode to be scanned. The syntax is as follows:

```
sdptool browse MACaddress
```

Seeing Whether the Devices Are Reachable with l2ping

Once we have gathered the MAC addresses of all nearby devices, we can send out pings to these devices, whether they are in discovery mode or not, to see whether they are in reach. This lets us know whether they are active and within range. To send out a ping, we use the l2ping command with the following syntax:

```
l2ping MACaddress
```

Summary

Wireless devices represent the future of connectivity and hacking. Linux has developed specialized commands for scanning and connecting to Wi-

Fi APs in the first step toward hacking those systems. The aircrack-ng suite of wireless hacking tools includes both airmon-ng and airodump-ng, which enable us to scan and gather vital information from in-range wireless devices. The BlueZ suite includes hciconfig, hcitool and other tools capable of scanning and information gathering, which are necessary for hacking the Bluetooth devices within range. It also includes many other tools worth exploring.

Chapter 8: Web Security

Web Security

Just like physical stores, homes, government locations, web applications alongside websites are also susceptible to their security arrangements and protocols being circumvented. What is needed to counter cyber-crimes and the compromising of web applications is robust and reliable security measures.

Web security does this exactly. A functional definition of web security for us can be that it is a set of protocols and protection measures employed in the safeguarding of your website together with your web applications against hacking and against unsanctioned access by personnel who are unauthorized. The integral division of Information Security can protect web services, websites and web applications. This provides crucial security for anything that is carried out on the Internet.

Normally, there exist multiple considerations that are involved when we are dealing with web protection and/or web security. For an application on the web or a website to be said to be secure, it must be backed up by a variety of techniques and checkpoints to guarantee its security. We always have standards of security that need to be adhered to. OWASP is responsible for the highlighting and implementation of these standards. Web developers who have plenty of experienced normally adhere to OWASP standards and keenly study the Web Hacking Incident Database to be able to know vulnerabilities that lead to websites being hacked and how they are hacked.

Common website security threats

Websites can be attacked in more than one way. Before proceeding, we need to understand some common threats to website security. These are what we shall be looking to avoid and be prepared for during the planning of security measures. Some of these include Spam, Viruses and malware, WHOIS domain registration, and DDoS attacks, among many others.

How to safeguard your website

After getting to know common security threats, let us now focus on how we can prevent them. The assumption that your website is secure is not correct. As long as you have not instituted any safeguard mechanisms, there is a high chance that it can be attacked. Here are a few steps you are required to effect to better the security of your website:

- **Restrict file uploads**

It is risky to let visitors on your website upload files. The uploads may contain a script meant to exploit vulnerabilities present on your website. All uploads need to be treated as a threat to the security of the website.

- **Use HTTPS protocol**

This tells the visitors of a given website that essentially, they are dealing with a proper server. This translates to "no one can intercept the interactions they are having or the content they are viewing."

- **Secure your personal computer**

Security starts with you! It is important that you take care of the security of your devices. Hackers can use your PC as a gateway to your website. Ensure that you have antivirus software that is updated with the latest definitions. This will protect you from many malicious attacks including from file downloads. It is also possible to inject malware to the websites through stolen FTP login credentials. It is important that you frequently scan your devices for malware and viruses regularly.

- **Change your default CMS settings**

We have seen that numerous attacks are normally automated these days. Malicious users do program bots to help them locate sites still using their default settings. Make it hard for them. Upon installation of a CMS you own, modify the settings which are still on default mode:

- ✓ Settings required for comments
- ✓ Controls that users require
- ✓ Information visibility
- ✓ Permissions for files

Above are settings you can change right away.

- **Software updates**

All the software must stay up to date. This includes the CMS, plugins, Word Press software, among many others. The updates bring improved functionality, security patches to cover vulnerabilities, fixes for bugs and software glitches, and so on.

- **Select a web hosting plan that is safe**

Web hosting plans that are shared have higher chances of getting compromised. In as much as they are appealing to users due to the potential cost savings, the levels of protection are reduced. As such, they are not a secure option. Remember, cheap is expensive!

- **Limit access to users**

Errors caused by human beings account for a majority of cybersecurity attacks. Reducing or limiting humans can contribute greatly to error reduction. It is not necessary for every employee to access your website. Guests, web designers and consultants likewise, do not deserve automatic access. The least privilege principle needs to be implemented to secure your website.

- **Do a password change**

Password changing is a significant shot in the arm for web security. So, change your password. Changing the password alone is even not enough;

make it a habit to change it often.

- **Monitor your security**

You can get utilities that can help you monitor your websites' security online. Such utilities can help you with conducting security audits, which can help to expose potential vulnerabilities. In so doing, you can launch countermeasures before an attack happens.

- **Make a backup for your website**

It is said that when you have been forewarned, you should forearm yourself. It is good to always be prepared for the worse. In this case, the worst that can happen is your website getting compromised. A backup ensures you are at peace since there will be no data that is lost in the event of a compromise.

Conclusion

May I take this opportunity to thank you for being able to make it to the end of this informative book, Kali Linux. I want to believe that it has been edifying, and through it, you are now able to hit the ground running in matters revolving around hacking. Also, I hope that you have gained the relevant expertise to enable you to begin your hacking career or better your skills if you are already one. I sincerely hope that you have enjoyed turning pages right from the first topic which was Introduction to Kali Linux, all 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 trust that by studying this book, you have gotten to learn plenty of practical concepts that you need to become a hacking expert.

By now, you must have been able to get access to a vast body of theoretical knowledge regarding the various types of attacks that can be launched on your systems, the reason for launching them and how you are able to safeguard your infrastructure against such attacks. These are your first steps towards becoming a professional hacker. The book covers topical issues like wireless network attacks, cyber-attacks and penetration testing, among others. It, therefore, means that you are now in a good position to discern network attack mechanisms that occur in the real world and prescribe appropriate remedies.

I have also given you a few security measures you can implement to keep your networks safe. The formatting is such that the language is a user-friendly language that you can understand the importance of securing your networks. Going forward, the next step is to put the concepts you have acquired from this book into practice. They say practice makes perfect and it is by practicing that one can become an expert in the field of hacking, more so using Kali Linux. Let the knowledge you have acquired from the book work for you.

Finally, if you found this book useful in any way, a review on Amazon is always welcome!