HACKING WITH KALI LINUX

A STEP BY STEP GUIDE TO LEARN THE BASICS OF LINUX PENETRATION. WHAT A BEGINNER NEEDS TO KNOW ABOUT WIRELESS NETWORKS HACKING AND SYSTEMS SECURITY. TOOLS EXPLANATION INCLUDED

AXEL ROSS

HACKING

WITH

KALI LINUX

A STEP BY STEP GUIDE TO LEARN THE BASICS OF LINUX PENETRATION. WHAT A BEGINNER NEEDS TO KNOW ABOUT WIRELESS NETWORKS HACKING AND SYSTEMS SECURITY. TOOLS EXPLANATION INCLUDED

AXEL ROSS

HACKING WITH KALI LINUX

A STEP BY STEP GUIDE TO LEARN THE BASICS OF LINUX PENETRATION.
WHAT A BEGINNER NEEDS TO KNOW ABOUT WIRELESS NETWORKS HACKING AND SYSTEMS SECURITY.
TOOLS EXPLANATION INCLUDED

AXEL ROSS

Disclaimer

While all attempts have been made to verify the information provided in this publication, neither the author nor the publisher assumes any responsibility for errors, omissions, or contrary interpretations of the subject matter herein.

This book is for entertainment purposes only. The views expressed are those of the author alone and should not be taken as expert instructions of commands. The reader is responsible for his or her own actions.

Adherence to all applicable laws and regulations, including international, federal, state and local governing professional licensing, business practices, advertising, and all other aspects of doing business in the US, Canada, or any other jurisdiction is the sole responsibility of the purchaser or reader.

Neither the author nor the publisher assumes any responsibility or liability whatsoever on the behalf of the purchaser or reader of these materials.

Any perceived slight of any individual or organization is purely unintentional.

Description

Modern-day hacking has become more sophisticated than ever. Hacktivists groups, ransomware, and highly classified document releases are a daily problem. In modern times, the ethical hackers are needed more than ever to protect and prevent hack attacks. The information available to everyone makes it all the easier for hack attacks, but it makes protection available as well.

Hacking is not always black and white, and there are different types of hackers and types of hacking. The major types of hackers are divided between ethical, unethical, and somewhere in between.

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.

This book covers topical issues like wireless network attacks, cyber-attacks, and penetration testing, among others. It, therefore, means that you are now in an excellent position to discern network attack mechanisms being perpetrated in the real world and recommend appropriate remedial measures.

This guide will focus on the following:

- How To Install The Kali Linux
- Setting Up Your Hacking Lab
- Essential Linux Terminal Commands
- Web-Based Exploitation
- Types of Penetration Testing
- Hacking Wifi Passwords
- Networking To Achieve Targets
- The Effects Everyone Suffers From
- Advanced kali Linux concepts
- Preventing Cyber Attacks… AND MORE!!!

Introduction

What makes Kali Linux different from other Linux distros?

Kali was developed specifically to meet the requirements of professional penetration testing, hacking, computer security research, reverse engineering, computer forensics, or security auditing. In order to make this happen, Offensive Security made various core changes to the original Linux source code to build a system that meets the following requirements:

a) Custom Linux kernel : The Linux kernel that powers Kali is upstream, specially patched for wireless injection on-the-go.

b) Single user OS with root access by design : Because of the nature of security testing and penetration, Kali Linux is designed to be a single-user system that grants root access by default. After all, most tools that come with Kali Linux require escalated privileges.

c) Network services are disabled : By default, network services are by default disabled by system hooks. This enables the user to install all kinds of services without compromising the security of the computer they use. Some connectivity services such as Bluetooth are also blacklisted by default.

d) Trusted set of repositories : Considering the purpose of Kali, it is very important that the integrity of the system as a whole is maintained. Kali developers kept the set of upstream software the system comes with to a minimum to achieve this. You can add more repositories as needed to *sources.list* if need be.

A few things to remember about Kali Linux:

Despite its popularity, Kali Linux still poses some great challenges even to experienced Linux users. Do not expect to master it within a few days, weeks, or months, especially if you are new to Linux. This operating system is designed to be highly customizable but it does not support ‘out of band’ and unrelated packages and repositories. For instance, you cannot install *Steam* and begin gaming on it and even mainstream packages such as *NodeJS* takes quite some effort to set up.

If you have the passion and the capacity to train to become a hacker or a professional pentester, Kali Linux is the ideal toolkit that will help you

achieve this goal. Kali Linux has been the world's favorite pentesting and hacking toolkit used by security engineers, geeks, hackers, system admins, and fanatics alike. This is a full Linux operating system you can install as the primary OS on a computer dedicated to hacking and penetration testing.

Alternatively, you can install and run it in a virtual box on a Linux or Windows computer or set it up on a dual-boot system.

Why Python?

Python is the most preferred language for hackers to develop tools for use in the field of cyber security. Most of the tools you will find being shared online today such as port scanners, vulnerability analysis tools, password crackers, and scripts to execute brute force are written in Python. If you have been introduced to Python, you have probably come across or heard of Python APIs and other third-party modules that make it very easy to develop and integrate your modules and tools.

The top reason that you should learn to code in Python as you study to become a hacker is because it is known to be a language for lazy programmers. You can write fewer lines of code that do huge tasks compared to the number of lines you would write in another language to carry out the same task.

Unless you learn how to write scripts that do what you want, you risk getting stuck as a script kiddie who relies on the tools developed by other proficient hackers and programmers to gain access to vulnerable systems. Relying on ready-made scripts rather than writing your own decreases the success rate of your exploits since such tools are more easily detected by intrusion detection systems (IDS) and antivirus software or even the law enforcement.

Many of the features that Python has makes it a very useful language for budding hackers. The thousands of pre-built libraries make it a very powerful and functional language to script. There are also thousands of modules and hundreds of thousands you can download from such sites as Github.

Now that we have all the basics out of the way, let us learn some hacking.

Whether the few resources covered in this section of the book is useful now or not, the best resource a hacker can have is skills. You must drive your learning and keep the passion alive even when experiments are not working or concepts difficult to understand.

You should be willing to take a step back and revisit an area you already covered even or research further and extensively on a subject not well covered in this course.

Chapter 1 Let’s Start! How To Install The Kali Linux

There are numerous explanations behind the changing job of firewalls, including falling costs, less complex structures and more prominent needs. The early firewalls were fundamentally equipment based gadgets, and they were over the top expensive also. At the point when programming put together firewalls originally accompanied respect to the market, they were confounded to utilize and very exorbitant too. Nowadays, notwithstanding, there are various reasonable, and even free, programming put together firewalls with respect to the market. Truly, firewalls have turned out to be so well known and significant that Microsoft incorporated a free one as a component of its Windows XP Service Pack 2 update.

There are numerous reasons why a home PC client needs to utilize a firewall. For a certain something, the individuals who interface with their office system should have a firewall set up to anticipate unapproved access to the home PC and the corporate system. What's more, anybody with a fast Internet association will get themselves the subject of undesirable consideration by programmers, infection/spyware authors, etc. A firewall can help hinder that undesirable traffic.

Why you need the security of a firewall

The truth of the matter is that a PC which is unprotected by a firewall can be hacked in merely minutes, by any of various robotized programmer programs that meander the Internet. The main way you can make certain that your PC and the data it contains are sheltered is to ensure it with a firewall.

From multiple points of view, running a PC loaded with individual data without the insurance of a firewall resembles leaving your vehicle entryways opened with the keys in the start. It's similarly as simple for an Internet criminal to take the data from your PC for what it's worth for a cheat to take your vehicle. Truth be told, taking the data on your PC would presumably be significantly simpler.

Along these lines, similarly as you ought to secure your vehicle by locking the entryways, you should secure your PC with a dependable firewall. A firewall program, related to against infection programming, hostile to spyware programs and other Internet assurance, gives a safe and safe figuring condition for you and your family.

Be that as it may, it's imperative to download and introduce all the fundamental updates to your working framework before introducing any sort of firewall program. This is on the grounds that a product based firewall would itself be able to be in danger if the working framework has a security defect.

What's more, it's constantly a smart thought to stay up with the latest, as there are in every case new security dangers, and security defects, being found. So having your working framework cutting-edge will give you a decent base to pass by.

Finding a dependable firewall

There are various superb firewall programs available, and it's commonly a smart thought to attempt a few of them before choosing which one to utilize. Look at the online surveys and after that since most firewalls give a free time for testing, exploit this choice before you purchase.

A few firewalls will come bundled with other security situated programming, for example, hostile to infection programming or spyware end programs. Other firewall projects are essentially independent items. Whichever type you pick is more a matter of individual inclination than all else. In any case, regardless of what sort of firewall you pick, it's critical to arrange it appropriately, as indicated by the directions gave. An appropriately arranged firewall, related to great enemy of infection programming and a spyware disposal program, is the most ideal approach to ensure your PC and the important information that it contains.

Normal idea

This section portrays basic idea of Windows individual firewalls. It isn't important to execute the firewall along these lines to have it secure. Normal individual firewall is actualized as three or four separate parts.

Bit driver

The initial segment is piece driver. Its has two principle capacities and that is the reason it is now and again actualized in two parts as opposed to in one. The primary capacity is a parcel channel. As a rule on the NDIS, TDI or the two levels this driver checks each bundle that roll in from the system or goes out to the system. This is otherwise called inbound and outbound association security.

Chapter 2 Setting Up Your Hacking Lab

In this chapter, we will set up a decent hacking lab wherein you can carry out all the practical hacking exercises we will carry out in this book. The chapter explains why having a hacking lab is important and what the minimum hardware and software requirements you should set up for efficient learning are.

It also goes in depth to describe how to install and configure Kali Linux as a standalone OS or in a virtual environment, and how to configure Python 3 on your computer.

Is a hacking lab really necessary?

It is acceptable for a hacker new into the world of hacking to have only one working computer with decent specs during the learning phase. However, for best results and to significantly cut your learning period, it is recommended that you set up a personal "hacking laboratory" to learn and sharpen your hacking skills in a safe and suitable environment.

Just as with everything else we learn, practice, practice, and more practice is what will make you ready for the real world hacks. There is no better place to learn and practice than your personal lab.

Hardware requirements

The biggest problem in becoming a hacker is not learning the theoretical skills but putting them into practice. This is why it is VERY important that you have a safe space with the right equipment to practice whatever you learn from this book or any other tutorial or guide.

You may never really grasp the strengths or application of the techniques you will learn here unless you have a practical exposure to hacking. As you prepare to dive into the world of hacking, here are the minimum hardware requirements you need to start learning and practicing.

Computer requirements

An ideal computer hacking lab is one that has at least two computers – one being the user's and the other or others being test targets. You obviously already have you own computer. Even if you do not have an extra computer at your disposal, you can still make it work with the one, but it must be a decently powered computer. This is because you will have to set up a virtual system and even set up virtual networks in it.

The host computer, which you will use to hack local or remote targets, should be powerful enough and with sufficient hard disk space to install and run a virtualization environment such as Microsoft's Hyper-V, VMware Workstation or Oracle's VirtualBox.

VMware Workstation, the virtualization software used in the demonstration of this book requires an AMD Athlon 64 FX Dual Core Processor or 64-bit x86 Intel Core 2 Duo Processor with 1.3GHz speed or better. It also requires a minimum of 2GB RAM although 4GB is recommended and a 64-bit operating system. You should check the specific hardware requirements of the virtualization platform you prefer to use to ensure that your host machine can support it.

Network and Internet connectivity requirements
While hacking may refer to gaining access to a local computer you have physical access to a secured target computer, most of your exploits during and after this course will involve penetrating a computer system remotely over a network. Therefore, having a good local network, preferably wireless with a modern router in your lab, is the best setup to make the most of this course.

You must also have a good internet connection to download the software you need to set up the software environment. Some of the files such as Kali Linux's ISO file may be as large as GB. There are also many resources on the internet that you will be introduced to in this course that you can use to practice your hacking skills.

Software requirements

The kind of software you will need in your hacking lab will largely depend on the types of exploits you wish to concentrate on during and after training. If you have a single computer, you will need to download and install a virtualization software such as VirtualBox or VMware Workstation then install the Kali Linux and Windows 7 target operating systems on it. While both may be installed on the same virtual space, only one can be run at a time.

We recommend that you have separate Windows 7 and Linux target machines, or a single machine dual-boot system with both Windows 7 and your favorite distro of Linux such as Debian Mint or Ubuntu.

Here are the steps to follow to set up the right software environment for your hacking lab (or computer if you prefer simplicity.)

Setting up a virtual environment

Choose one out of the two most popular Virtualization programs VMware Workstation or VirtualBox then download and install. Each of these products has its own pros and cons, it is prudent that you do a little research before choosing which system to go with. The process of downloading and installing the software is straightforward and should pose no challenge to an individual striving to be a hacker.

One great thing about using these software, besides eliminating the need for an extra computer, is that you can run them in different modes, some which allow you to bridge virtual and real networks to test your network penetration skills just as you would on a real network. VirtualBox, for instance, features NAT, Bridge, and Internal Network modes that causes the hosted OS to behave just like a computer on a specified type of network.

While setting up the virtual environment, pay close attention to configuration details such as the amount of memory (RAM) that is allocated to the virtual machine. Allocating too little memory will hamper the speed and performance of the virtualized operating system while allocating too much will negatively impact the performance of the host operating system.

Setting up Kali Linux

After a virtualization environment is properly set up and configured, you can then go ahead and download Kali Linux from kali.org/downloads/ . Offensive Security releases fresh image files of Kali Linux every few months but you should always download the latest stable version.

Note that there are multiple options of the operating system to choose from: 32-bit or 64-bit and light or standard. The light version has limited tools and features compared to the standard version, which explains why it is less than 1GB in size while the standard is over 2.5GB.

Alternatively, rather than download an ISO to re-install on your new virtual environment, you can download a version already optimized for VMware or VirtualBox – but with the same infrastructure as the standard version. You can download these images and read through the set up instructions from the Offensive Security website.

Once the image files are downloaded, follow the instructions on the page to install Kali Linux on your virtual computer environment. This may sound complicated if you are new to virtualization but if you have ever installed an operating system before then you will be able to do it without difficulty.

Setting up target Windows machine

If you have more than one computers to use in your hacking lab, you may set up the target Windows systems (Windows XP or Windows 7) as well as another distribution of Linux on the target computer.

Since we will be learning to hack both Windows and Linux systems, you can install the two operating systems side-by-side if the computer supports dual-boot or you can set them up in the virtual environment.

Note that this will only work if you also have a local network such as a routed wired or wireless connection.

Chapter 3 Network Basics

The most straightforward way, of course, to gain access to a particular system would be directly from the interface terminal of the target device. This presents many obstacles to the hacker because it requires him to gain physical access to the system, exposing him to being discovered or leaving traces of his presence. However, the networked nature of most computers and information technology provides safer, less conspicuous avenues to exploitation – the network.

In general, a network is any collection of interconnected parts. There are networks of people, organizations, political states, machines, and just about any group of entities in which information passes between members. Computer and IT networks have grown and combined to connect billions of nodes, from small household networks with one or two personal computing devices to enormous server farms that require their own powerplants.

Whether sending contact information from one smartphone to another with a bluetooth connection, or streaming a movie through the internet from Moscow to Buenos Aires, the basics of networking and communication are the same. Understanding computer networking and communication protocols is essential to becoming an effective hacker.

Network Components and Architecture

Any device capable of some sort of connectivity can comprise a node on a network. Traditional user platforms like servers, desktop PCs, laptops, tablets, and personal handheld devices such as smartphones are common on networks. There are also an increasing number of networked peripherals and standalone smart appliances like printers, televisions, gaming platforms, network cameras, entertainment consoles, audio devices and watches. Each device can typically connect to multiple other devices through various communication media. Physical connections like copper wiring and fiber optic cable serve as a backbone to the global internet, and connect most networks up to the main access point of a local area network. Within a LAN, any number of connection types may exist, including physical wiring and Wi-Fi. At short ranges, devices may connect

through Bluetooth or Near-Field Communication (NFC) technology. Alongside of this architecture is a growing broadband cellular network that consists of any array of radio-frequency towers that are connected to the Internet backbone and to various satellites. As broadband cellular technology improves, usage is expanding beyond telephones and are becoming the primary internet access methodology for many individual devices and small networks.

Network Models and Protocols

Regardless of the type of node or communication medium, two devices must communicate using some sort of common protocol. A standard protocol used by all devices across a network is necessary to prevent miscommunication. Internet Protocol (IP) had been around since the earliest days of networking. Although it has changed a bit in form and function, it remains the de facto standard for network communication. IP, combined with another standard known as Transmission Control Protocol (TCP) forms a layered networking paradigm called TCP/IP. This scheme divides a network into various layers from the basic network hardware up to the user application. The collection of protocols is a conceptual network communication model known as the TCP/IP model, or TCP/IP "stack". There is another model known as the Open Systems Interconnection (OSI) model, which is more granular with regard to the number of layers. The OSI model can be more generally applied, but it describes the same essential principles as the TCP/IP model.

The TCP/IP Model

The TCP/IP model consists of four, stacked, conceptual layers that each have a role to play in the preparation and transport of data from one point in a network to another. These are the application, transport, network, and data link (or link) layers.

Network Data Flow in Layers (infosecinstitute.com)

The application layer of the TCP/IP stack (considered the "top" layer) is the layer most visible and accessible to the user. This is the layer where the content or payload of a communication is created before it is packetized for transport. Email clients, web browsers, file sharing

software, video streaming applications and other connected apps all operate in the application layer. It's worth noting that the application layer executes other protocols that reside within (or above) TCP/IP. This includes the hypertext transfer protocol (HTTP) of web applications, smtp for email, and File Transfer Protocol (FTP) among others.

Functioning in the transport layer is an advanced concept, but suffice it to say that this layer helps to ensure the quality of communication through error checking and other means. Additionally, the transport layer is where information passed from an application is initially divided into packets, which are then appended with appropriate headers. TCP operates at this level, but it is not the only protocol available. User datagram protocol, or UDP is used when it is necessary to sacrifice the successful arrival of a small number of packets in exchange for real-time delivery of information. UDP is the transport protocol of choice for audio and video streaming.

The network layer, often called the Internet layer, is where the work of routing packets is done. In this layer, the best network route for a packet is determined, then the packet header is appended with a source and destination IP address before it is relayed to the network interface hardware. There are other protocols that can operate at this layer, but IP is by far the most prevalent, and is the underlying structure for most global data communication. The manipulation of IP headers at various stages of transit is the basis for many hacking attacks.

The bottom layer of the TCP/IP model is the hardware or data link layer. The hardware layer is the last stop of a data packet before it leaves its source machine and arrives at its next destination through the physical medium. The MAC addresses of the network hardware involved in relaying the packet are appended to the packet header at this level.

Network Protocols

When one node in a network communicates with another, it divides its message into small, independent packets. Each packet is then appended with a header as it passes through each layer so it can be properly reassembled into a message at its destination. The beauty of TCP/IP is that each individual packet may take a different route, and can be re-sent if lost, assuring a high degree of efficiency and message fidelity.

At the heart of TCP/IP is the IP address. Each device on a network has a unique address to identify its location within the network and any subnetworks to which it belongs. Understanding IP addressing because it allows them to zero in on particular targets. In addition, hackers may need to hide or manipulate their own IP address in order to remain conspicuous.

The standard version of IP has been IP v.4 for many years and is used on most networks and devices. IP v.6 is a new standard that can accommodate many more addresses. Within an individual LAN, the first octet in an IP address typically indicates the designation of the overarching network, with subsequent octets designating subnetworks and individual machines.

IP Address Notation

One of the most important things to understand about IP addressing is that the IP address of a given node within a local network is different than the one assigned to it when it communicates through the Internet. This is because it's impossible to control or prevent two individual machines on separated networks from accidentally or intentionally being given the same address.

From the hacker’s perspective, IP addresses provide a roadmap on any individual network to identify and distinguish individual machines. Additionally, so much tax involved intercepting individual data package in transit on the network. The header information in the packet contains the IP address of birth the source and the destination. It is the manipulation of these headers that allows doctors to conduct man in the middle and denial of service attacks. It is the manipulation of these headers that allows knockers to conduct man in the middle and denial of service attacks.

IP addresses are considered logical addresses, meaning they are assigned via software, either directly by the user or automatically through some kind of process. IP addresses reside on the network layer. In many cases, IP addresses can be spoofed or forged in a packet header. This can be done to obfuscate the source of an email or some other attack payload, or to maliciously reroute packets.

It’s important to understand that IP forging cannot be used to hide any two-way communication. In order for two machines to exchange information, their addresses must be valid or the packets being exchanged cannot reach their destinations. This is why it is futile to try to hide or

change ones IP address when operating on a peer to peer service, or to hide the designation of a downloading node. The best one can hope for in this scenario is to route information through a large number of geographically and logically distinct proxies. The TOR network, which serves as a basis for the Dark Web, operates by creating multiple layers through which information can pass.

Another important type of device identifier is the (Media Access Control) MAC address. MAC addresses are considered permanent physical addresses and are assigned to individual network interface devices. The MAC addressing scheme is designed so that no two devices should, in theory, ever have the same designation. The address is burned into the device ROM so that it cannot be easily changed. MAC addresses are part of the data link layer.

Although MAC addresses are intended to be permanent, there are ways to "spoof" an address by writing a false address onto a packet header. This does not change the permanent address of a device, but allows a hacker to avoid being identified through their network interface. If an attacker with a spoofed MAC gains local access to a network, especially through wireless means, they can avoid being traced through their hardware.

Chapter 4 Virtual-box & Kali Linux Installation

Virtualization

What is virtualization? This is the ability to run an operating system with all its installed software in a specialized environment.

Let us use an example for a better understanding. Assume that I have a computer running on Windows 10; this will be our "host". Using virtualization software, I can run a "guest" operating system on our host computer. Let's assume our guest system is Windows XP. This means that we can run two or more operating systems at the same time.

The guest (Windows XP) will think it is running independently on a real machine while in reality, it is on software on our host machine (Windows 10).

VirtualBox

Oracle VM VirtualBox is free software that is used for virtualization. It is easy to use and is available for Windows, Linux, Macintosh, and Solaris operating systems. Just download it from here then click the downloaded executable to install. Just click on the "Next" button on installation and give it the necessary permissions.

I will be installing and using it on a Windows 7 operating system. VirtualBox works the same way regardless of which operating system you are using. If you encounter any troubles while installing the software please feel free to consult the user manual by clicking here .

After installation, once you click it, you will get a window that looks something like this.

We can now download the VirtualBox extension pack for additional features. You can download it from the VirtualBox website. To install the extension pack just go to where the downloaded file is and click it, a VirtualBox window will appear asking if you want to install the extension pack.

Kali Linux

This is because it comes with a wide range of hacking software but we will focus only on the network hacking parts only.

Kali Linux is free and can be downloaded from the Kali website here . However, there is a version of Kali Linux that is suitable for use in VirtualBox that you can download here (please make sure you select the VirtualBox image and not the VMware one), this is the one that we will use since it is simple to install compared to the other images.

You will be given a torrent file that you will use to download the Kali Linux file, so make sure you have software for downloading torrents.

After using the given torrent to download the Kali Linux VirtualBox file, we can now get to install the OS on VirtualBox. In order to do so, just simply click the downloaded Kali Linux VirtualBox file. A VirtualBox window will appear that looks something like this.

Now let us change a few things before we click the import button. If you scroll down you will find that CPU is set to 4, you can leave it that way depending on the type of processor you have on your computer but Kali Linux can still run on 1 so feel free to change it. If you have the latest processors on your computer, you can leave it at 4.

Under the CPU option, you will find the amount of RAM allocated to it is 2048 MB. This will do just fine but you can increase it if you have a high amount of RAM on your device or reduce it to 1024 MB which will still work.

The base folder is where the disk image for your virtual machine will be set. You can just leave it to the default or change it to another location you find comfortable with. The disk image will take about 10 to 15 GB of space.

In the MAC Address Policy change it to “Generate new MAC addresses for all network adapters” as shown below.

Once everything is set, you can click the import button at the bottom of the window. It will take some time for the image to be imported. After that, we can fire up Kali Linux.

Your virtual machine will now appear at the top-right of the VirtualBox window as shown below in the red area.

If you click on it once, you'll to see a new window with a bar on top that has buttons for settings, start and discard. Click on the settings button, you should see a window similar to the image below.

Head over to the Network window and change the Attached to setting from NAT to NAT Network as shown below, this will allow our virtual machine to access the internet.

Click on the OK button to save the settings. We can now go ahead and run our Kali Linux machine. Click on the virtual machine and then click on the start button. Give it a minute or two to start.

Kali Linux Basics

If the machine starts correctly, you should be asked for a username. The default username for Kali is *root* and the default password is *toor* . Once you have entered the username and password, the Kali Linux home window will appear. You switch to full screen by pressing *right ctrl + F* .

In order to properly use Kali Linux, you will have to learn how to use terminal commands. Head over to the taskbar on the left side of the screen and click on the terminal icon as shown below to open the terminal.

A terminal will open, which just looks like a black window with a blinking white cursor. Let us now take a look at some common commands that will be used from time to time.

Command	***Use***
apt update	*Update old programs.*
apt get install <package>	*Install a specific package <package> = package name*
clear	*Clear the terminal window*
git clone <link>	*Install a package from github*
mkdir <name>	*Create a new directory*
rm <file name>	*Remove a file*
cp <file name>	*Copy a file*
ls	*List the files and folders in a directory*
cd <directory path>	*Navigate to a certain directory or*

	folder
ifconfig	*See your network details*

Let us type the *apt update* command to update our system packages.

You can learn more about a command by adding *--help* or *–h* after the command, for example, to learn more about how you can use the apt command you can type *apt --help* .

You can also use the terminal to open programs. If you type and enter *firefox* , you will be able to open the Firefox browser.

There are many different commands that can be used in Linux that you will see in use as you progress through this book. I highly recommend that you mess around with the terminal and get a good understanding of commands and of the Kali Linux operating system itself, maybe you will learn a trick or two.

Chapter 5 Essential Linux Terminal Commands

Before the emergence of graphical user interfaces and ergonomic input devices such as mice, computer users had only their keyboard and a monochromatic screen with a prompt. Commands were entered line-by-line and either interpreted on the spot or compiled EN MASSE into a program. In order to interact with the file system or peripherals (via the kernel), users had to employ a lexicon of special commands to perform desired actions. The original Unix systems, in fact, booted directly to a command terminal (typically a login prompt) to await input. Although most modern Linux distributions now boot to a GUI, the operating system is still underlied by the Unix terminal command system. Any Linux system can be made to boot directly into the command line, but most users open the *Terminal* application from the main GUI desktop if they want to enter commands directly.

Although "point and click" graphical interfaces are convenient and generally more intuitive, advanced Linux users - especially hackers - often prefer to use the terminal to execute commands. Typing a Linux command manually is not only, in many cases, more efficient, but it also gives the user more direct control over operations. A single, one line command, entered properly, can replace multiple clicks and nested windows. Furthermore, by entering a command directly, the user can more easily trace the source of errors. Hackers tend to be independent, self-reliant individuals, and are loathe to relinquish control of their machine to automated processes written by others.

This chapter will discuss how to navigate in Linux through the Terminal, and introduce some of the more critical shell commands.

Linux System Anatomy

Before getting into the command list, it is important to understand the basic structure and file system of a typical Linux distribution. The command library is very powerful and can control virtually any aspect of the operation or configuration of a Linux system.

Architecture

All Linux systems are built upward from the kernel. The kernel is the machine-level instruction set that loads into memory when the OS is

booted. Kernel instructions interact directly with the machine's hardware, including the processor(s), memory, network interface, and any peripherals.

The Linux shell (Figure 14) is the means by which a user interacts with the kernel. The shell can be either a direct command prompt or a graphical user interface.

Linux Kernel Architecture

THE DIRECTORY SYSTEM

Linux has an organized directory structure that is designed to compartmentalize files for security and stability. Directory paths use the fore-slash (/) to separate subsequent directory names in the path, as opposed to Windows which uses the backslash (\ ). The term "root" can at times be confusing to Linux beginners because there are a few locations which may be referred to as a root directory. The true "root" in a Linux file system – inasmuch as there are no parent directories above it – is designated simply by a lone fore-slash, "/". All other directories lie under this location. The directories under "/" vary slightly between Linux distributions, but the general structure was inherited from the original Unix system and is largely universal.

Linux Directory Structure

Linux Commands

Linux has a rich set of terminal commands, many of which are the same, or similar, to those of the original Unix OS. These commands allow users to manage and manipulate files and folders, install software, interface with peripherals, and among many other tasks, perform various networking operations. Although Linux commands will be introduced in context in various sections throughout this book, the following basic commands serve as an introduction to the basic Linux lexicon and the general format and usage of terminal commands.

Directories and Files

The first commands a Linux user should learn are the ones associated with navigating and manipulating directories. Once at the terminal command prompt, the following command will list the files and directory present in the root directory:

 # ls

In most cases, the default terminal directory will be '/home/username', so typing "ls" will list the contents of the current user's files and folders.

Most Linux commands feature options that can be appended to the default command form. These options vary for each command, and range from changing the format of the output to directing the command to perform specific functions that it doesn't perform by default. The "-l" option for the ls command is an example of a command option that results in more detailed output.

Note that the directory listing now contains details for each file and folder in the current directory, including access permissions, size, and creation date. Options are preceded by various symbols (-, --, |, etc.) depending on the nature of the command ans option. Many options can be chained together in a single command, making them a powerful way to accomplish many things in an efficient single line of code.

To display the options for a particular command, along with other useful information, one can append the command with "-- help". However, the help output for mot commands is several pages long and cannot be viewed in a terminal window without scrolling. Attaching the "| more" option will pause after a single page of output, allowing the user to advance page-by-page by pressing the spacebar until the output is complete.

The cd command allows the user to change the active directory to a specified location. A given path is assumed to be relative to the current directory unless otherwise constructed. To change to a directory within the current active path, simply append cd with that directory name. Note that Linux file and directory names are case sensitive.

To switch to a path that is not in the active directory, the absolute path must be specified.

The following is a short list of useful Linux directory and file commands. It is by no means a complete list, but represents some of the most common commands. Care must be taken with some of these commands, because they may change or delete the contents or location of a file or folder.

Command	Action
pwd	Displays the path of the active directory
ls	Displays the contents of the active directory
cd	Changes the active directory
mkdir	Creates a new directory
rmdir	Deletes a directory (if empty)
cp	Copy a file
mv	Move a file
rm	Delete a file

“Superuser” Access: The sudo Command

One more important Linux command is the infamous “sudo” command – one every aspiring hacker should know. The term “sudo” is (reportedly) short for “superuser do” and indicates to the kernel that the subsequent command is to be executed with root access (or sometimes as a user different from the one who is currently logged in).

Above, a user navigated to the Documents folder of another user, but was denied permission to delete a file, named “passwords”. When the command was reissued using sudo, the user was prompted for a password, then the rm command was successfully executed.

Chapter 6 Web-Based Exploitation

Now that you know how network exploits attacks work, it is time to also explore web-based exploitation. Nowadays, everything is connected to the Internet one way or another, therefore web exploits are extremely common. It would be difficult to find a company that has no web presence. In the old days websites were extremely basic, coded by using only HTML and no other more complex programming language. They were composed of simple static pages. Today's websites, however, involve complex programming, mixed databases, and authentication servers. Every type of computer, whether it's a smartphone or a desktop, is connected to the Internet.

Because of this heavy expansion into the online world, we need to understand and further develop web-based means of exploitation. For instance, computers used to have word processors and other tools such as Microsoft Office installed and used locally. Now, a lot of these tools exist in the cloud and thus no longer require any local installation. A common example of this is Google Docs. Everything is connected now, and it's important for the aspiring ethical hacker to fully understand the basics of web-based exploitation.

In this chapter we will discuss the basics of web hacking and some concepts such as spidering and code injections. As always, please take the time to explore all techniques and practice them until you no longer need to use any cheat sheets.

The Basics of Web Hacking

There are many web-based hacking frameworks and tools designed for web application hacking. However, it doesn't really matter what you use as long as you understand the basics, because most of them work exactly the same. The purpose is to have the functionality needed to attack the web. In basics terms, this works by accessing any website through your browser as usual, but you use a proxy to send the traffic. This way, you can collect and examine all the data you send to and receive from any application. Let's take a look at some of the most important functionalities you need to get from these tools in order to be an effective web hacker.

Intercepting Requests

Being able to intercept requests as soon as they leave your browser is a highly valued toolkit functionality. The general idea is to use an interception proxy as the key which gives you the power to modify any variables before reaching the target destination, which is the web-based application. This intercepting proxy is a tool which nearly all web hacking tools provide. How does it work, though?

At the foundation of all web transactions, there is an application hosted on a web server. Its purpose is to accept your browser requests and display the pages according to these requests. The requests contain a series of variables which determine the page that should be returned to the browser. For instance, whenever you are doing some online shopping, these variables dictate what you added to your shopping cart and which payment information to retrieve. As a hacker or penetration tester, you can take advantage of these variables, because with a web-hacking tool you can modify them. This means that you can create new variables, edit the existing ones, or delete them entirely.

Finding All the Web Pages

When you prepare for a web-based attack, you need to first prepare the battlefield. This is done with tools that give you the ability to find all the relevant pages, directories, and files that are part of the target web application. The tool that provides this functionality is known as a "spidering" program. All you need to do is insert the web page's URL and the spider will be unleashed. It sounds pretty dramatic, but you have to understand that this web information gathering method is not subtle.

The tool will make thousands of website requests at a time. The spider will receive HTML code every time it makes a request. That code is analyzed, and if more web links are uncovered, the spider will send more requests to all of those links. Eventually, all the website's information will be analyzed and cataloged by the spider. Web requests will be sent until every attack field is discovered. However, keep in mind that the spider will follow absolutely every link it finds. This includes any logging out links. When that happens, the spider will actually log out of the website without letting you know. This means that if you aren't careful, you might to lose out on potentially valuable information that wasn't discovered because of the log out link. Always analyze the content that was spidered to make sure all the areas you are interested in were explored.

Spidering tools also allow you to command which directories of web pages should be focused on. This gives you more control and allows you to analyze the target with more accuracy.

Analyzing Responses for Vulnerabilities

The third most important functionality you need to look for is the ability to analyze the responses that are coming from web applications. This process is similar, but it is applied to web-based application. The goal is to find vulnerabilities.

When you modify the variables with the help of the intercepting proxy, the target application will respond to you. The tool will then examine all of these responses to look for any kind of vulnerability in the application. Many vulnerabilities can be detected by an automated web-based vulnerability scanner, however some of them will not be noticed. Luckily for us, we are only interested in the ones that we can easily find. Why? Simply because a lot of them can be used to perform an SQL injection attack, for example. An automated tool might not find all of the critical vulnerabilities, but enough of them will prove to be useful to us.

Spidering

The concept of spidering is probably one of the most important ones in web hacking. In this discussion, we are going to be using a framework that is already installed on Kali, namely WebScarab. This tool is loved by many hackers and penetration testers because it is modular. This means you can customize it with the help of plugins until it fits your needs perfectly. Now let's discuss more about WebScarab in its default configuration.

As a result, we gain useful data that can be used to gain access to restricted pages or files. Open the terminal and let's turn WebScarab on by typing:

webscarab

Don't start unleashing the spiders just yet. First, you should make sure you are running the program with its "full-featured interface." Some versions of the tool start up with the lite interface, and that isn't good enough for our purposes. You can check to see if this option is ticked by clicking on the "Tools" tab. Now that the program is enabled, you will have to use a proxy by first configuring your browser. The purpose of this action is to

force all web traffic to run through WebScarab as if it's a filter. The tool will then be able to manipulate any ongoing web traffic.

In order to set the web browser to use a proxy, you need to go through its network options. In our example we will use Firefox, so go to Edit > Preferences and then click on the Advanced Tab, followed by the Network tab. If you are using a different browser, the settings path should be similar. Just look for any tab related to network options. Once you're inside the Network menu, click on Settings. A Connection Settings window will open, and you will use it to configure Firefox to use WebScarab as a proxy. Now check the box for "Manual proxy configuration" and type 127.0.01 inside the HTTP Proxy field. Next, you need to type 8008 in the Port field. Finally, you should check the "Use this proxy server for all protocols" box and then click "OK" to apply all of these settings.

From now on, all web traffic will be directed through WebScarab as the middle man. However, keep in mind that the tool needs to be active for you to be able to browse through any websites. If you deactivate WebScarab, you will get a connection error whenever you try to go to a website because we configured the network settings to use it as a proxy. Another thing you need to keep in mind is that all websites will display an "invalid certificate" message. Do not pay any attention to that warning, because it's normal to encounter it when using a proxy.

Now that you've configured everything, you can start the spidering process. Type the web address of your target in the URL field. As soon as the website loads, it will run through WebScarab. In order to spider your target you need to right click on the URL inside the tool and select "Spider Tree." You can now explore every file that is related to the website. Make sure to examine them well, because you might find some leaked information that can prove useful to your penetration test scope.

Intercepting Requests

Remember that our WebScarab tool acts as the filter between your web browser and the target's web server. All the Internet traffic is flowing through this tool, and this gives us the ability to interact with the data before it enters the browser and before it leaves as well. What does this mean for us? We gain the power to make any changes we want to any

information that is in transit. There are still many websites out there that are developed with bad coding and rely on hidden fields to communicate information from and to the web client. In such a case, the programmer probably assumed that the user could not possibly access these hidden fields. However, with the help of a tool like WebScarab, we can manipulate this information. Let's discuss a scenario to gain a better understanding of how we can take advantage of this functionality.

Let's assume we are shopping for some fishing rods on an online store that has been badly coded as described above. We browse through the website, choose our product, and add it to the shopping cart where we see we are going to be charged $100. Now, if we are running a proxy server, we might see a hidden field that is used to send the value of $100 to the web server when the "add to cart" option was pressed. Because we are running the website through WebScarab, we can see this hidden field and even modify the variable stored inside it. We can simply change the $100 value to $1. This is what can be achieved with the WebScarab tool, however, keep in mind that there aren't that many websites around that are this badly coded. No matter the case, it's worth going through such an example to demonstrate the power of intercepting requests with the help of a program like WebScarab.

Now let's use this tool as an interceptor. For this process you will need to switch WebScarab back to the lite interface. Go to the Tools panel and select "Use lite Interface." Next, you need to go to the "Intercepts" menu and check the options for "Intercept requests" and "Intercept responses." Now switch to Firefox, or the browser of your choice. You can now change the value of a field by allowing WebScarab to simply intercept the request and then finding the variable you want to change. Type the new value, hit the 'Insert" button, and you're done!

SQL Injection Attacks

Code injection attacks have been common in the online world for years. There are many types of code injections, but since our purpose is to master the basics of hackings we will only discuss the SQL injection, which is a classic still being used today. SQL Injections are used mostly to bypass web authentications, however, they can also be used to view and manipulate certain types of data.

Most web-based applications that run today use an interpreted programming language and have some sort of back-end database that is used to store data or generate some form of dynamic content. SQL is an example of a popular interpreted programming language and is used in many websites, such as online stores.

Think of the process of making a purchase on an online store. Let's say you're after a fishing rod. You go to an online shop that sells outdoor products, and you type "fishing rod" in their search engine. After you hit the "search" button, the application will take your data (fishing rod) and build a query in order to search through the database for anything that contains the words "fishing rod." Anything with these keywords will be returned to you in the form of a result.

By using SQL, we can interact with the information inside a database and even modify it if we choose to. Keep in mind, however, that there are several versions of SQL and not all online stores use the same one. For instance, a MySQL statement will not coincide with an MSSQL or Oracle statement. In this section, we will only discuss how to interact with applications that use SQL. If you understand the basics, you can always expand your knowledge by exploring MSSQL or MySQL as well.

Here's an example:

SELECT * FROM product WHERE category = 'fishing rod';

In this example we have the first verb "SELECT" that instructs SQL to search inside a table. The "*" symbol is then used to return all the columns inside the table. The next word "FROM" is used to specify the table. Finally, we have "WHERE" to specify which row should be returned and displayed. In other words, the "SELECT" command will find the "product" table and return all the rows which contain the words "fishing rod" from the "category" column. What's important to note in this query is that everything left of the equal sign (=) was created by the original programmer of the application, while everything on the left side is an instruction coming from the user.

We can use this knowledge to cause the application to behave in an unintended way. Instead of typing "fishing rod" inside the search box of the website, let's type:

‘fishing rod’ or 1 = 1--

In this example we use single quotes to close the string that contains the words “fishing rod” and afterwards we add a command (1 = 1--) that will be executed. The “or” statement we added in the search box is actually a condition in SQL that is used to return records when either of the two statements is true. The “--“symbols at the end of the line are used to tell SQL that everything beyond it should be ignored. This is way of preventing any other code from possibly meddling with our command. The new statement we made actually tells the program to return all the contents of the table where the category is equal to “fishing rod” or “1 = 1”. Since the “1 =1” statement is obviously true, we will receive everything that is contained inside the table. This might seem like a boring attack because instead of getting “fishing rod” results we simply received all the results, but it can be useful in a different scenario.

Remember that SQL is used to perform authentication for many web applications. Let’s explore a different example. Let’s say a friend of yours created a website that his business partners use to send or download important files. They all have their own unique accounts that are needed in order to have access to the data. This friend knows that you are an ethical hacker, so he asks you to perform a penetration test against his website. We are now going to use the same principle as in the above example in order to bypass the website’s authentication system. Start by typing the following text inside the username textbox:

‘or’ 1 = 1--

When you don’t know the account’s username, you can use the above statement which always results to true. By doing this instead of entering a username, most SQL databases will choose the first user account. In many cases, the first user on the list is the administrator who has full rights over the system. The best part of using this method, however, is that you don’t even need to know the account’s password. Type any random password, because the database will ignore it. Why? Because of the “--“ part of our statement. Always remember that everything after those symbols will be commented out and therefore not acted upon. This includes the password.

If you do know the username, however, and you want to specifically access it for whatever reason you can do it with the same command.

Simply type the instruction in the password field instead and because “1=1” is always true, the application will think the password is correct and you will gain access to the specified account.

Chapter 7 Types of Penetration Testing

Penetration testing helps test for weaknesses in a computer's security system. Usually, this vulnerability may be as a result of backdoors in the systems, errors in the software, or using the software in an intended way. Penetration testing aims to find these vulnerabilities and provide information on how to correct the situation.

When choosing the type of penetration testing, you need to be directed by the goals and the scope of the testing. There are three main types of penetration testing that you can choose from. These types include:

- White Box Penetration Testing
- Black Box Penetration Testing
- Grey Box Penetration Testing

Black Box Penetration Testing

Black box penetration testing simulates a real world cyber-attack where the attacker is not privy to all the ins and out of the computer system being tested. In black box testing a similar scenario happens, the tester is only given the IP and a few other important pieces of information and then asked to gather the information on his/her own and then test the system. The penetration tester is not provided with the programming codes or any other information that might be available to an insider.

Due to lack of inside information, this kind of penetration testing may take a longer period of time to uncover vulnerabilities and risks within a given computer system. Quite often the tester will have to try out several approaches before uncovering anything. Because of this, sometimes the black box penetration testing is referred to as "trial and error" testing.

Advantages

The following are some of the important advantages of black box testing:

- The tester gets the real weaknesses a black hat hacker will attack and this makes it possible to securely protect a computer system from such attacks.
- The result of this testing helps verify the discrepancies between the specification of the system and the actual

system.

- One does not require to be an expert to do it

Disadvantages

The disadvantages of black box penetration testing include:

- The test is difficult to design as it is more of a trial and error process
- It consumes a lot of time
- May not capture all the issues in the system

White Box Penetration Testing

In white box penetration, the tester is aware of all the ins and outs of a given computer system. In fact, the tester may have access to the architecture and the source code of the application being tested and other important details only an insider can have. Because of this information available to the penetration tester, this test does not take a lot of time when compared to the black box testing.

White box penetration testing is a simulation of an insider attack. Because of this, the result of the testing will be more effective when it comes to beefing up the security of the system against insider attacks, although may also provide important suggestions for protection against external attacks.

Advantages

Advantages of the white box testing include:

- It covers all the areas of the system being tested
- It makes it easy to verify logic decisions when carrying out the exercise
- It covers both the typographical errors associated with vulnerability and also the syntax checking

Disadvantages

The disadvantages of white box penetration testing include:

- It only looks at the system securities from an insider's point of view
- Since the tester has all the information he may be biased in choosing areas to test

Grey Box Penetration Testing

This type of testing is a combination of both the white box and the black box penetration testing. It is considered to simulate an attack by a hacker who has some inside information about the system. The penetration tester is given only limited information about the application being tested so as to get started.

With only partial information on the system being tested given a penetration test can use both automated and manual testing processes. The tester may start with automated testing using the information given then work using manual for areas he is not quite clear. This system can yield results from both the outsider and the insider perspective and thus help strengthen the security of a computer system against attacks from both sides.

Advantages

Advantages of gray box penetration testing include:

- Because of the limited information is given, the tester is in biased and non-intrusive
- The is not contact between the penetration tester and the develop and thus there is no risk of personal conflict

Penetration Testing Teams

Quite often a number of people team do penetration testing for any given system, especially when working on a large complex computer system. These teams are of different types depending on how team members do their work. The following are the three main types of penetrating testing teams:

- The Blue Team;
- The Red Team;

- The Purple Team

The Red Team
This is a team made up mainly of individual penetration testers. The teams' main goal is to simulate an attack and find vulnerabilities and risks within a given computer system. Their job also entails compiling and making suggestions of the best possible solutions to the identified risks and vulnerabilities.

The Blue Team
Blue team is often considered as the insiders' team. It is made up of computer security experts from within a given organization. Its main job during penetration testing is to repel any form of attack from the red team. People participating in this team have full knowledge on the system and work together to protect it from any form of attacks.

In an actual work situation, the red and the blue team work as if they were the two sides of the same coin. Because of this, the teams need to work together to protect the computer systems they are working on. This requires sharing or feedback and working proactively to develop new solutions to the systems.

The Purple Team
The Purple Team is the combination of both the blue and the red team. The main job of this team is to act as a link in between the red and the blue teams. The purple team acts on the suggestions of the red team to enhance the security tactics employed by the blue team. This helps build a cohesive working environment so as to ensure that all the security loopholes within a given system are patched. At the same times, the purple teams work with the two teams to develop new solutions to ensure that the computer system is prepared for advanced types of attacks.

Key Areas of Penetration Testing
The following are three important areas where penetration testing often takes place:

Network Penetration Testing
Here the penetration tester tests both the physical structure and the network infrastructure to find out if there are risks and vulnerabilities in

the system. The tester will have to put the physical structure to test first to find out if it has issues that may expose the network to security threats. In addition, the penetration tester has to test the design, operation, and implementation of the network to find out if there are security risks and vulnerabilities that need to be corrected.

Application Penetration Testing

Here the logical structure of the given application has to be tested. The testing here is simulated as attacks aimed at finding risks and vulnerabilities in the security controls of a given computer application. This testing is focused on applications such as firewalls and other software used to protect a given computer system. This is important because no security application is perfect at all the times, it is, therefore, important to find out vulnerabilities and risks so that you can beef up security by combining several complimentary security control applications.

The workflow or response the system

This testing focuses on the response to social engineering type of computer security threat. Computer security does not work by itself it needs human interaction for it to be 100% perfect. This penetration testing looks at how the people in a given organization interact with their computers and how they are prepared to prevent attacks. The testing also looks at the design of the workflow and how such a design can affect the security of the computer system.

Chapter 8 Hacking Wifi Passwords

Wi-fi hacker is a program that is readily downloadable for free. It allows you to hack into any wi-fi server within the area and that is recognized by your device, whether it is your laptop, PC, phone or tablet. You can easily hack and bypass the password and enjoy unlimited internet for free. The software is completely virus free, so there is no need to worry about infecting your device with a pesky bug. The software updates automatically so your version is always up to date, and it is compatible with all versions of Windows. You will be able to hack WPA, WEP, and WPA2 and it has preventative measures again WPS attack. The user interface is easy and user-friendly. The best feature of this wi-fi hacker is that you don't need any technical knowledge in order to use it effectively. Your path to internet freedom lies wide open before you. Enjoy!

Facebook Hacks

More and more these days you see people claiming that their Facebook pages have been hacked and in most cases it is true.Phishing is a form of hacking often used in these cases. The hacker opens a fake account in the name of the victim and sends a request to the victim. On accepting the request, all the victim's information such as Facebook email address and password are saved to a text file which is easily downloaded by the hacker. There we have it, access to the victim's real Facebook account.

Phishing is also a very common hack used when it comes to banking. You get suspicious emails requesting you input bank login details or requesting you to login to internet banking. Same applies. All personal information is saved to a text file, downloaded by hacker and Bob's your uncle he can go on a shopping spree at no cost to him/herself.

Keylogger is a common little program which is installed on to the victim's laptop. Keylogger collects all you saved email, password and important information off of the device and it is sent directly to the hacker's email address. Seems so easy and it is if you know what you are doing. If you don't know what you are looking for as a victim, then you will be none the wiser.

DNS spoofing is another popular means of hacking Facebook accounts. You need to be sure that you and your victim are on the same network. Use

DNS spoofing to change the original page to your fake page and gain all the access you need.

Little Life Hacks to Save Your own PC

Torrent files can potentially be harmful to your PC and compromise your security. Videos are often downloaded using torrent files. The problem with torrent files is that the user links provided are often fake and if they contain potentially harmful matter, then it is not traceable. A quick hack here is to use TS or Torrent Stream Magic to play these movies in real-time instead of downloading them. If your internet connection is good and speedy, then there should be no problem viewing. This also saves endless hours downloading movies that are unwatchable due to awful quality.

Password Hacking and Cracking

There are three types of password hacking namely Password Hashing, using software to hack and Online account hacking.

Password Hashing

Passwords that you type into your computer are stored on the disc in the form of hashes. They are not stored as clear text but are encrypted, and you will need root/sysadmin privileges to access them. On a Windows operating system, these hashes are stored in the SAM file on the local disc whereas on a Linxus system they are stored in etc./shadow files. Decrypting and cracking these passwords is time-consuming and you will have to ensure that you have full access to the said PC for as long as you need.

The first way to do this is using Dictionary - using a dictionary to find the password hidden in these hashes is the quickest and easiest method. The system runs through a dictionary of words and attempts to gain access to each and every one. Doing this manually would seem almost impossible, but your PC is able to run through these in minutes and crack the password.

Secondly is Rainbow Table - This process basically double checks what Dictionary has already found. It rehashes the password and checks it against the original hash. This is a time-consuming procedure.

Using Software to Hack

There are many different types of software out there that is available to hack passwords to accounts. They use commands and information to find the password and crack it. All you do is supply the required information, and the software does the rest. Many passwords can be hacked within minutes, but not all can be hacked at all using this method.

Some of the software available to hack account passwords are John the Ripper and Ophcrack

John The Ripper - This software is able to crack passwords on the Linux system using one command line. This software uses the dictionary method, and if that does not work, it uses combined dictionary words if all else fails it uses a hybrid of dictionary words and characters. Still, no access than in applies the Brute Force method, and that gets through almost anything.

Ophcrack - this is a free rainbow table based password cracking system for Windows and can be used on Linux systems as well as Mac. It can only crack the password if you have the hash file available for the operating system. Without this hash file, it is useless.

Online Account Hacking

Online hacking tools use information gathered online about an account to crack the password for the account. This is possibly the easiest way to hack a password if you have the available information required.

There are a number of online hacking tools available including Brutus and THC-Hydra.

Brutus - considered the fastest online hacking tool to crack passwords. It works on Windows systems as well as Linux. It is an open source tool and is best for doing online hacking of a number of types of accounts.

THC-Hydra - a widely used online tool which is capable of hacking web form authentication. When paired with other powerful tools such as Tamper Data is can become an almost unstoppable means of cracking almost every type of online password authentication mechanisms.

Using Hardware to Hack

Some machines are designed to crack passwords of any machine that they are hooked up to. They are extremely powerful systems that can hack

passwords in a mere fraction of the time it would take the normal hardware.

Some popular hardware includes Botnet and Asic:

Botnet - this hardware functions using the Brute Force method and can crack password as well as networks in minutes.

ASIC - Application-specific devices that work to crack the passwords. They work faster than 100 CPU working together.

Hidden Software to Hack

Your password and account information is stored on any PC or Smartphone that has any of this hidden software. If you log in using a device that is not yours, even if you log out, that information is stored, and you could become the target of a hacker.

Keycounter - this operates in much the same was as Keylogger to store any account information and passwords entered through the keys on the PC or Smartphone.

Hacks That are Becoming More Prevalent Everyday

Hacking techniques become bolder and more intricate each and every day. Hackers are probably the most persistent people around. They bide their time and wait patiently all the while gathering useful information.

Extortion Hacks

Extortion hacks involve hacking into systems and threatening to release sensitive information on companies and individuals if “ransom” is not met. The hackers use the fact that this information could destroy you to get what they want. The downfall for the victim here is that if they do decide to pay up, it does not mean that the hacker still won’t release the information. That is a chance that you must be prepared to take.

These hacks prey on the fears of companies and corporations, and if the information is leaked, it could cost them billions as well as lawsuits from their clients.

Data Manipulation/Change Hacks

Hackers change or manipulate digital data in order to compromise the data’s integrity. They do not delete or release the stolen data. Many of

such hacks involve theft. Data manipulation can be extremely hard to detect as the changes are so subtle, but they consequence considerable. Just imagine a hacker getting into the files of a financial institution or the stock market and manipulating ever so slightly the data. Adjusting the trade market up or down every so slightly. Imagine the effects this could have on the economy. It could be catastrophic for all involved. Data manipulation of military files could have devastating effects. Sabotage of the weapons system could very well compromise the integrity of the weapons and change how they function.

Chip and Pin Hacking

Hackers have a tendency to keep evolving and developing their skills and techniques. As they become blocked down one avenue, they pursue another and another. They always find a way in. With the new chip and pin cards, the magnetic strip/chip prevents any information stored on the cards to be accessed. Hackers have been blocked in this way of obtaining account information, but they now target online shopping markets where transactions are done via telephone or the internet with no need for pin or signature. Theft of the banking detail information is now enough to target online shoppers so please always make sure you use as secure a site as possible.

More Backdoors

More backdoors mean more chance for hackers to enter their "playgrounds."

Telephone Hacking - Phreaking

Phone or Voicemail messages are intercepted without the consent of the phone's owner. For those who are famous or have a lot to hide, this can be a significant risk. Phone hacking involves mainly remote access to voicemail systems as opposed to the actual telephones themselves. Fixed line hacking means intercepting the call to listen to the call in progress. This can be done by either placing a recorder on the phone line or placing a recorder or short range transmitter into the handpiece. Mobile phone hacking can be used to intercept calls in progress and listen in or to take

covert control of the cell phone, gaining access to text messages and activity logs. Bluesnarfing is unauthorized access to a mobile phone using Bluetooth. As Bluetooth range is short, you will need to be in close proximity to the phone. Phone hacking is a form of surveillance and is illegal in most countries. Phreaking is where a hacker accesses telephone number for routers for individuals or corporations to gain free calls and free internet connectivity.

Security of any device is a careful compromise between ease of use for the user and safety. For many, the ease of use of the instrument is the primary concern and security is an inconvenience to the user. The consequence for this is the fact that many devices such as mobile phones are easily hacked. If you want an entirely secure device, you will have to put up with the inconvenience of having passwords and pins to authenticate.

Sneak Attacks

Fake Wireless Access Points - This is probably the easiest hack to accomplish. All you need is some software and a wireless network card, and you have a wireless connection which you can run off somebody else. Areas, where there are these free wireless access points, are a hunting ground for hackers. The pose as the free wireless access point and filter out whatever valuable data they can from all the devices connecting. Passwords, account number, telephone number, you name it, these are still sent in plain text to receivers.

You can never trust a free wireless connection. Never share confidential or sensitive information over a wireless network.

Cookie Theft - cookies store information of sites navigates throughout a session or over numerous sessions. Cookies store all the data you have submitted while using these site, account numbers, passwords and contact details. By stealing someone's cookies, you become them for all intents and purposes. You can shop online as them and use their credit card details for payment.

Chapter 9 Networking To Achieve Targets

In three words? Study, study, study! Believe it or not, it is simple as that. Why do people fail in a process? Well, they don't define their target. Ok, so if you define the target you all set right? NO! Your target has to be realistic. Here is my target. I said to myself, I might be a restaurant manager, and making about £30K, but working every weekend, working 10 sometimes 12 hours a day, hardy having a weekend off, working on most Friday, Saturday evenings, and many times even on Sunday.

I had a huge responsibility. I had to deal with all the customer complains. Had to do the rota for 52 people. Organizing interviews, recruitment process, and trial shifts. Ordering uniform, as well as stock: including food, drinks, cleaning equipment, and maintainence equipment. Dealing with third parties, such as suppliers, or maintenance contracts. Running the shift, and organizing people's breaks. Counting money, and stock. Participate in P&L meetings (profit & lost), calculating GP (gross profit) and wages percentage hourly, (send people home when not busy). Also had to schedule meeting agendas, and come up with cleaning schedules, deep clean schedules, how to manage waste and deploy quality control, portion control, new menu ideas, organizing deliveries with third party companies. Dealing with Streamline in case the PDQ machines didn't work, so we can take credit card payments, and so on…

I knew I have to get out! People who think they are going to open a restaurant and become rich, it's an illusion! It's one of the stupidest ideas. Some people wanted to open a restaurant with me, even coffee shops and sandwich bars; I always said no. Not because I am not capable, no. I don't want to do it ok?! So, I have decided to go and study something.

Of course, at the time I wasn't sure it's IT what I want, so thought about being a lift engineer first. I have read about how lift engineers have to be always on standby shifts, and working like 22 hours a day when they on, which I find too much, but turnes out it's part of their reponsibility, in case someone gets stuck in the lifts. Later I also learned there is a huge risk that lift engineers have to take on. Nearly every month there is a lift engineer who dies, while trying to fix a lift. Can you believe that? I think life is too good to take such a big risk, so moved on. Then thought about being an electrician, or microwave specialist of some sort, but then realized it's not for me either. All I wanted, is to have a laptop to work with, and preferable

in a nice environment, making a lot of money, while my evenings and weekends are free☺ It's true! I remember friends told me ''keep dreaming'' So I thought about IT, something to do in IT right? At the time I have £6K saved money, so I thought I could spend half of it for decent education of some sort, some IT education right? So I googled: IT JOBS ☺

Then I realized there are over 40 different kinds of roles out there, or at least on the webpage I landed at the time. Software engineer, helpdesk specialist, IT Service Delivery Manager, IT Security analyst, network technician…

I was confused. But, I know one guy who was studying to be an electrician, and he was a good friend. He seemed to be educated, so I asked him.

''What do you know about the IT field?''

you know what he said? Well, he said right away that IT is very crowded, it's very difficult to get in, maybe 5-10 years ago was easier, but now, it's too late. I believed him, it was a mistake, so for the next two weeks, I kept on researching what kind of job I supposed to do. I found nothing! Instead, all I heard in my head is: ''IT, IT, IT…'' but how?!!!

Then I remembered something. About two years back, I had a mate who I use to drink with every night (not anymore), but at the time we use to drink few beers, pretty much every day.

He had a flatmate at some point, and he was some sort of an IT guru. Unfortunately, he left from my friend's place, and I have not seen this guy since at least a year. I never knew his number. I am not even sure of his full name, right? So I called my mate and said,

''hey, you remember this guy, the IT guru guy, who used to be your flatmate? What was his name again?''

My mate said;

''of course I remember his name is Bilal''

So I said;

''do you have his number? I need to talk to him''

My mate said;

''no number sorry''

So I said;

‘’Do you know someone who knows his number?”

He said;

‘’there was a polish girl named Magda, who he always used to call, but she is now gone back to Poland, but I know her on Facebook.”

I was like wow, ok all I need is her facebook profile page so I can contact her. Which I did, and she gave me Bilal’s number, who happened to be leaving close by me, but before I called him, I had a plan.

The plan was this. I will ask him when he is available, because I have not seen him for a long time. I will invite him for a dinner, and ask him for his advise.

- Ask him what the hell I supposed to study?
- How much will it cost me?
- How long will it take me to get there?
- What kind of money can I expect once I get a job?
- How long does it take to get a job if I religiously study hard?
- Most importantly, because he knows me, do I have a brain power to succeed?

When I met him, he asked me;

‘’hey, how is the restaurant business? Are you still a manager?”

I said;

‘’yes, unfortunately”

so he asked me why, and I said all the responsibilities, and downsides I just shared with you, when he cut me off and asked me;

‘’So, how much are you making there?”

I said;

‘’£30K”.

Do you know what he said? He said;

‘’no no no, you have to leave that place, common!”

and started laughing. And so it was also Bilal who told me about both CCNA and Network +. That's it. This is my story. I know it's boring, but the point is that you must have some sort of mentor, who you can ask and say ok what's next? Now, you don't have to have a mentor, but this is how I did it. So to recap, if you know someone in IT, try to approach him/her, but don't go crazy about your questions, instead ask him out for a drink or a dinner, and offer to pay for it. In the meanwhile, you go ahead and find out what you want right? Networking!

I do understand that you might don't know anyone in IT, I get it. But I am pretty certain that you do know someone who knows someone very well, who works in IT right? That is where you have to plan, to make your move. Now, here is the thing. You might ask me: do I still talking to a friend who gave me Magda's Facebook page? No. Ok, so do I still keep in touch with Magda? No. But I must be still in touch with Bilal right? The answer is NO again.

Did I use Bilal or the others at the time? You might say that, yes, but what I did is this. Networking, and convincing people to help me to get what I want. Simple as that. Everybody needs help sometimes. I am telling you: everybody. But do not expect that people will look you up and tell you what to do. It is you, and only you, who can decide which way you plan your future. Again, people tell me I was at the right time at the right place right?

Well, I just explained I had a tough job, I got paid lot less, and I had no clue which direction I should go within IT. I also didn't know anybody in IT, but made few phone calls, and Facebook chat, through two people, and got a number in the end. I wasn't at the right time at the right place. Instead, I pushed it all to my direction. Well, technically, all I did is this: made two phone calls, one Facebook chat, and paid Bilal's dinner. No big deal, anyone can do it. If I was able to do this, I am sure you can too. In case you don't want to, or you can't do exactly what I did, I hope you can take a way something from my story, and apply it to your life. Is it ethical how I networked my way around to get in touch with someone who is a pro in this business. In the end, I didn't hurt anyone, so I think so. Maybe I used a little Grey hat technique, but grey hat is called grey hat, because the intentions were for the purpose of good.

Chapter 10 How To Get Things Done

I have recommended to study IT, for at least 50 people in the past few years, and the reason I did it, is pretty obvious. Still, do you know how many people have taken my advice? Well, try to take a guess. I mean I do have experience, and all, I know what I am talking about, but still, I was only able to convince two people, and even those two are struggling with their studies. One of my best friends Francesco, taken classes and even bought the CCNA books. Still, he has never read them. The problem, is that he bought the books now over two years ago, and still did not read them. Anytime we talk on the phone, I ask him;

‘’Have you started reading the Cisco books yet?”

of course, the answer is always the same;

‘’not yet, I don’t have time, because of…”

blah blah blah…

The usual problems, with the flat and girlfriend, or too many overtimes, and these kinds of things right? So, I have to listen to all that, but then I ask again;

‘’ok I see, so when you are going to start reading the books?”

of course, I know I am already annoying him, but I keep on trying, until I get a strategic answer. So, I always begin explaining how I do it, how I read all the time, watching video courses all the time, because at the end of the day, all the topics are out there. Sure, you have to pay for them, but they are all there, so how to get things done right?

I have another memory which involves another friend of mine. I remember: me and my ex, and my mate, 3 of us, all Hungarians seating on a train half drunk, and we are on our way to a huge Hungarian Party. So we just seating on the train, having fun, do some chit chat and came up Cisco, and studying. So my friend asked me if I started studying yet because I was telling him a week before I will and all, so what’s the current situation and all right? Well, he was already smiling at me, you know the type of smile when someone takes you for a fool right? - but I replied anyway. I said;

‘’I actually received the books yesterday, and today already began reading the first one.”

Then he asked me;

‘’How many pages did you read yet?”

I said;

”32”

Then he asked me;

‘’…and how many pages is the actual book?”

I said

‘’it’s over 900”

‘’so when do you plan to finish that book?”

I said this;

‘’Look, I have managed to read 30 pages in one day, so if I only read 30 pages every day, I should be able to read the first book in 30 days.”

Then he said;

‘’yeah but reading once a book… you not gonna learn everything”

I replied;

“Of course not! I am planning to read the book two times at least. Within two months I should be good to go.”

Unfortunately, the reality wasn’t like that. I remember I was forced to say something clever. I had to keep myself to what I say, and I truly began reading every day. It took me over a month to read the book for the first time. Anyways, the second time while I was reading it, I have also taken notes of everything that was highlighted in the book, or if it was marked as important. Because I was taking notes, I have learned even more, but the second time around, it was about two months to complete the book, so actually I have only read the book twice. But, it has taken me more than three months, instead of only two. So next, I booked my exam for three weeks ahead, and began reading my notes I have written only. Basically only the highlights.

3 weeks later, I went for my ICND 1 exam, and of course, I have failed. The passing score was 839, and I scored 690. Bad! Lot’s of money I lost too, but I said to myself, I only have to know about 20 % more. Everything

on the exam was pretty familiar already, so basically nothing like I never heard of, but maybe I didn't take enough notes from the book.

So I said: I would give it a go again. So, I started reading the book for the third time. This time, I knew so much, I finished the book within two weeks. I skipped all those I have highlighted before. Also went back to my notes, and I kept on reading those, but since I failed the first time, four weeks after, I have rebooked the next exam. So I went and tried for the second time right? I remember I was so confident, I felt very positive about passing the exam, but when I got to the exam center, I started sweating and didn't feel well. It's always the same ever since by the way.

Anyhow, I started the exam, the timer began to count backwards, like in any other Cisco exam I tested since. I felt like I had it all. It felt like I am going to pass it with no mistakes. Am I going to score 1000 points out of 1000 right? Wrong! Guess what! I have failed again. This time, the passing score was 820, but my score was 790 only. I got angry, because they never tell you which question you didn't know. All they provide is an exam score and which topics on average I scored how much in terms of percentage.

It's still the same, and I don't think they intend to change the way, this is why Cisco Certifications hard to get. They make it hard for a reason. Whatever. Cisco and their games, it's always the same. The books are expensive; the courses are expensive, the exam fees are crazy expensive, routers, switches, firewalls, anything that the brand Cisco written on, it's not cheap. My friend told me about the website, called CBT Nuggets, he said I am very close to passing the exam and don't give up. All I have to do, is watch the CBT Nuggets video training related to CCNA, and I am going to be ok for the next exam. He was right, I watched the CBT nuggets course for ICND1, and a week later I passed the exam! This time the passing score was high as the first time went: 839, and I passed it with a huge score of 842! ☺ Just about. But, a pass is a pass! If the passing score is 839, and you pass with the score of 840, it's going to give you the same certification as you would pass the exam with the score of 1000. In the other hand, if you score 838, when the passing score is 839, it's a fail, same like you would have no points achieved whatsoever.

Another tip btw, if you want to know what they ask in any Cisco exam, I can tell you exactly what you need to know. Trust me! I have been over 12 Cisco exams.

Now that you know what you need to study, and how to get it done, let me break it down to you once again. In summary, all you have to do, is break it down. That's it, that's the secret, and here is why. If I tell you that you have to read 1000 pages, (ICND1 books are now over 1000 pages by the way) you going to be like, ''common man!, I don't have time for that!" Sure, I know, I heard it all, but here is the thing. Once you break it down to small chunks, it will sound so much easier. For example, you have 1000 pages to read. Don't think like you have to read it all in a day, you won't be able to do it. If that's your plan, I find it unrealistic. You have to be realistic here, so here is what you can do. Plan to read every day 20 pages, so you know that you will finish the book in 50 days right?

Some days you might be able to read even 25 or 30 pages, which is a bonus for you. Maybe on Friday night, you should read 40 pages, and Saturday morning read another 40 pages, so if you go out on a Saturday night, and you suffer from a hangover on Sunday, and you are unable to read even a page, you are still ahead of your plan! Should you skip the Monday too? No!

From personal experience, I can tell you that skipping more than a day without studying, like two or three days, it's going to be more difficult to get back to it. Seriously! How long is going to take to become a Cyber Security Specialist? Honestly? I don't know; everyone is different. But I take it as you have no background knowledge at all, and no experience, if you are persistence and start studying every day at least two hours, you can become a cybersecurity specialist within 5 years easy!

Give or take a few years, but if you can afford to study every day for about 4 hours, you can reduce the time, for probably about three years. It doesn't mean that in 3 years you 100% became a Cybersecurity specialist, but you will increase your chances.

Chapter 11 Hacking - The Effects Everyone Suffers From

As the public sees it, many of the effects of hacking are going to be bad because the public doesn't always see that hacking can be good.

There are pros and cons to everything and hacking is truly no different. When you hack someone, you are always leaving them open to the malicious effects of what hacking brings about whether you mean to or not.

When you do hack a computer, you are creating a breach in the computer's security. This is placing the victim's sensitive data and privacy at risk. These hacking activities are usually done to gain access to confidential information that one tends to keep on their networks such as social security numbers, bank account data, credit card numbers, and personal photographs. There are a few hackers that tend to use this information to harm the one that they have hacked. Then, there are others who simply "take" this information to prove to their "victim" the major security issues that they have to get them to be fixed so that the personal and sensitive information that they have taken cannot be taken again.

Once a computer's security system has been compromised, there is also the possibility of the loss or even manipulation of data. A hacker can go in and delete any sensitive information that has been placed on a network once they have gained access to it. Once your system has been hacked, you're at a great risk for all the data that you have on your computer being lost or manipulated in a way that can and most likely will harm you.

One of the biggest things that everyone associated with hackers is identity theft. Identity theft is when someone who is not authorized takes your identity. Your identity is but not conclusive to your social security number, date of birth, or anything else that would identify you as you. This is usually done with a malicious intent and used for the hacker's personal gain or interest.

When you've been hacked, the hacker can track everything that you do on your computer thanks to the advances in technology. The key-logging software is what is used to track every keystroke that you make on your computer. Thanks to this software, a hacker can instantly gain access to your passwords, your bank accounts, and anything else that they can use to harm you, all thanks to one little program.

DOS means denial of service attack. This happens when a hacker gets into your network and your computer. This can make the computer's resources unavailable to any of the authorized users. Usually, a DOS will attack a website which will then make the website unavailable for a long period of time. This then causes the users of the website to be inconvenienced—as well as hampering with the business of the website.

Along with identity theft, stolen information is a big thing that happens when someone hacks your network for a malicious reason. This can be hazardous to anyone, but most particularly to business that ends up being hacked because the sensitive information that they do not want getting out to the public is then released. Not only that, but email addresses, client information, so on and so forth can be stolen and compromised.

National security can even be put at risk when it comes to hacking. Hackers who hack into the government's networks then have access to the defense system as well as many other systems that will cause there to be grave consequences on the welfare of the nation. When someone hacks into the government, not only is the nation's security at risk but so is the well-being of the citizens of the United States.

Another effect of hacking is fraud. Hackers can turn computers into zombies by infecting them with internet enabled computer viruses. These computers are then used for activities that are considered fraud such as spamming and phishing attacks on other networks.

How do you know when you have been hacked? Your computer will most likely decrease in its performance speed. You may also begin to notice files that are not supposed to be there. These files may increase in size as well as be modified without you ever touching them. You may also begin to notice that there are changes in your network settings or even frequent disk crashes.

The only way that you're going to be able to protect your computer is by installing a reliable antivirus software as well as making sure that your firewall is enabled before you begin to connect to the internet. Also, make sure that you install the system updates on a regular basis.

Chapter 12 I2p

I2P, otherwise known as the " Invisible Internet Project " is another option that people can use to hide their online IP address. It shares a lot of the same characteristics of other networks in that it routes traffic through neighboring peers. The developers have stated that their main goal is not necessarily one of 100% anonymity (a goal some say is impossible), but rather to make the system too troubling and expensive to attack from the outside. It is an anonymizing network with several layers of encryption wrapped around all the data that travels through the system.

I2P VS Tor

You might think this sounds a lot like Freenet, but the similarity is actually more like Tor's network. I2P offers interactivity with websites, blogs, forums, chat, search engines and all without the need to install any of them locally. Such are the hallmarks of I2P. Websites that exist in the I2P network are called Eepsites, and are hosted anonymously with I2P being a strict requirement to access these websites. In that vein, it is similar to the .onion sites accessible only via Tor. Every PC that is connected to the I2P network shares in the forwarding of encrypted packets of data through proxies prior to the final destination. Each subsequent proxy prunes a layer of encryption at various intervals until encryption is removed. The bottom line is this: No one knows the origin of said packets, a trait also shared by Tor. While it is true that both Tor and I2P have different goals in mind, there exists many similarities:

- Both exist as anonymizing networks
- Both use layered encryption to funnel data
- Both have hidden services
- Tor has Exit Nodes and I2P has Outproxies

Benefits of Tor over I2P

- Larger user base than I2P; support from academic sources, constant improvements in stability and resistance to attacks
- Funding is sourced from many countries around the globe

- Large number of Exit Nodes

- Translated into many languages

- Optimized for Exit Traffic

- Memory more optimized than I2P

- Written in C

Benefits of I2P over Tor

- Hidden Services much faster than the Tor network.

- Not as many DOS (denial of service) attacks as Tor.

- Compatible with peer-to-peer file sharing (Tor is not).

- Tor tunnels last a long time compared to I2P. This ensures less attacks as the number of samples a hacker may use are limited.

- Every peer routes data for others.

- Offers TCP/UDP.

- Written in Java.

As you can see, both networks are safe enough for anonymity, as long as you aren't a world-hunted target. To this, a user's anonymity is typically broken due to their own sloppy behavior--their overconfidence being the weakest link in most cases (using the same login names on many websites, mixing these with Tor and non-Tor websites, and enabling JavaScript/Flash). Since I2P is not built to act as a proxy to the WWW, you should use Tor if you want to surf anonymously. The outproxies on I2P, as you've probably guessed, are similar to the exit nodes on Tor, but they do not have the greatest support and tend to be unstable. Thus you should use Tor for anonymous web browsing and I2P for I2p eepsites. One option is to use *Foxy Proxy* to test it yourself. Be aware however that since there are fewer outproxies than Tor exit nodes, it may be easier for an

adversary to identify your activities. It all depends on how much risk you want to assume and what the ramifications are if you are caught (and in which country).

You can also use I2P for BitTorrent and iMule as well as other P2P applications. Like Freenet, you will find that I2P will grow in speed the longer you use it without interruption. Torrents will be faster. Data will come down like lightning. Tor users will thank you for it. There are already too many torrent users on Tor that clog the network and make it difficult for people in dire straits who need anonymity for their political actions far more than the next Incubus CD.

While I2P is a technical powerhouse for anonymity, it can be a bit like a house of cards. Once the Ace is pulled from the bottom layer (by you), it can be rendered moot. I2P is just a tool, as is Tor and Freenet. It is not an invisibility cloak. Do something stupid, like move too much when a pack of Orcs are looking your way, you're bound to get an arrow in a place where you least expect it. Thus, act smart by being proactive in anonymity:

1.) Turn Off Javascript

Yes, it bears repeating, with arms waving in the air and shouting at the top of our lungs. Javascript is the bane of not only Tor, but other networks that rely on cloaking your IP address. Leaving this beastly plugin ON allows code to be run on your machine, code that will decloak you. Look at your browser settings and disable it. Also disable cookies. Super cookies are deployed in the wild to track down Tor users. Don't let it happen to you on I2P. Javascript can reveal a ton of metrics that fingerprint a user. Display resolution, page width, font and so on can be sent to an adversary by stealth. If you're in doubt, take a look at the web API at Mozilla:

https://developer.mozilla.org/en-US/docs/Web/API

2.) Silence is Golden!

Don't say a peep. Sure, you can talk. But refrain from discussing: the weather, your geography, your hobbies, your city politician that was just arrested for soliciting hookers. If someone says, "Hows the weather in your town?" You say: "Sunny." Every time. Alternatively, you may

misinform. The CIA does it, why can't you? Their entire organization is built on secrecy and deception. Don't get too choked up about a few white lies. Spreading misinformation about trivial things like the weather and the local politics can really put a nail in an adversary's coffin. Ditto on employment. If you are asked about your work and you're a programmer, say you're a mail sorter down at the Post Office. They're not going to ask you about the latest Elvis stamp.

3.) Rotate Usernames/Nics

The desire for convenience often gets people in trouble. They use the same usernames on multiple sites/forums. That's fine for the daytime, open web. Not so much for the darknet. It breaks anonymity. Take forums for example. When your username becomes infamous for a wealth of knowledge, change it. Create a new one. Don't tell anyone. Entropy rises when many users swap information like this on a frequent basis. Maintain separate personas: one for the darknet, one for regular internet. Memorization is better than writing it down.

4.) Never turn off your router

I never turn mine off. Ever. If it is constantly going on and off while Freenet, Tor, I2P or IRC is running, after a while clues will surface as to who I really am, provided a sufficiently determined adversary has the resources to do it (NSA). The cost in power is negligible, so don't go cheap with anonymity. As the saying goes: out of speed, anonymity and reliability, you can only pick two, but make up for the lost component by acting *smart* .

5.) Power in Numbers: Bandwidth

Don't be stingy with your connection. The more you participate in the storm of users (Freenet, I2P), the more cloaked you will be. It is better to run 24/7 if you can. This makes it more difficult for an adversary to discern if you sent a file to someone else, or if you are merely the middle man to some file sent by a total unknown on the other side of the globe. Besides this, leaving the program running just makes it a lot faster network in general for other users. Think *Safety in Numbers* .

6.) Optional (but smart)

In the *browser settings* , set browser.safebrowsing.enabled and browser.safebrowsing.malware.enabled to false. Search goliaths like Google and Microsoft do not need to know the website URLs you visit.

Get into the habit of flushing the cache--cookies, etc. You can set this to do it automatically upon exit of the browser.

Refrain from using Foxy Proxy to selective proxy .i2p links. You don't want to be sent to the clearnet. If an I2P website is a honeypot, your Firefox browser can send a unique identifier in the referrer, in which case... anonymity broken.

At this point you're probably thinking this is way more headaches than it is worth. And you'd be right...in the beginning. But anything worth doing is usually hard at the outset. I as well as my colleagues do all of these things only because we have done them for years. We do them every day. Are we thinking about them? No, not in the least on account of smart habits done daily. Do you think intently about starting your car? Pulling out of the driveway? No. But it's a good bet you were petrified to do it when you were sixteen. And pulling out of your driveway is a very complex action, as are the aforementioned suggestions. Just one of your brain cells is more complex than a 747. Don't waste any of them.

Torrents and Eepsites

First things first. Install not only the *NoScript* plugin, but also the *Cookie Whitelist* (Buttons). Ideally you want to block everything when surfing Eepsites. There are a multitude of add-ons on the *Firefox* site but you do not need all of them. You only need the ones that preserve your anonymity.

Install *QuickProxy* , also at the Firefox site. Restart. Then open the proxy settings using the edit tab and then browse to "Preferences" and "Advanced". Then "Settings". Change your proxy settings to:

127.0.0.1 for HTTP Proxy, Port 4444 and 127.0.0.1 and port 4445 for SSL Proxy. Ensure Socks v4 is checked.

Click "Okay" and exit out. If you've configured it correctly you should be able to click the QuickProxy icon (lower corner of browser) when you browse Eepsites. You can also paste in .i2p websites and hit "Go" the old fashioned way.

Torrents

An option for torrents is to use I2PSnark. If you're a beginner, ensure the service is running by opening a terminal and inputing:

$ i2prouter status

If it is not running, start it with:

$ i2prouter status

Then browse via Firefox to

http://localhost:7657/i2psnark/

At the main I2PSnark page, you can see it running. Now you can create a torrent. Move a torrent and the data into

~/.i2p/i2psnark

The other option is to paste the data you want to seed to the same directory, and in my case, this is usually PDFs and technical manuals. At the Tracker option, you can choose whatever method you wish or create an entirely new torrent. I2PSnark will create the new torrent and set it in a queue. All that remains to be done is to click Start in the top corner and away you go.

Chapter 13 Preventing Cyber Attacks

What can you do to prevent cyberattacks? Do you have the right systems and procedures in place to protect your company against an attack? Between 2017 and 2018, many organizations suffered from some form of cyberattack. Most of these were attributed to inappropriate security measures. Some organizations simply did not have a robust security platform in place, so hacking them was basically as easy as hacking into an individual's computer at the local library.

Types of Cyber Attacks

Human behavior is one of the worst enablers for cyber hacks. It is very easy to allow a criminal into your secure platform. All they need is to gain the trust of someone, and you are finished. Therefore, it is important to learn how to identify threats and from there, how to protect yourself from those perceived threats.

There are two broad categories of cyber attacks: semantic attacks and syntactic attacks.

Semantic Attacks

A semantic attack is about social engineering. These attacks are performed by altering someone's behavior within the organization targeted by hackers. The software involved plays a very small role, unlike in syntactic attacks. Semantic attacks are basically about perception (Noor et al., 2017)

Phishing is one of the most popular semantic attacks in which hackers send an email hoping to collect some information from the victim. You might not be aware of the phishing attack until it is too late, because the hackers clone emails from correspondence you interact with regularly. These are people you trust, so you barely crosscheck to make sure the emails are legitimate.

Once you click a link in the email, you are asked to provide some information to help them verify your account. In doing so, you willingly provide all the access credentials hackers need to take you down. Some phishing attacks can also include viruses and worms. However, the modus operandi is to dupe you into believing the email address is legitimate, willingly providing the information hackers need. The worst bit about

social engineering is that some attacks are a combination of semantic and syntactic attacks, and as such, the effects can be devastating.

Syntactic Attacks
A syntactic attack comes after your network through different channels. These attacks are often carried out through malicious programs. The most common programs used for syntactic attacks are as detailed below.

Trojan horses - A trojan horse is something that looks harmless. You will allow it into your system, unaware of the danger it possesses. Today, trojan horses can be sent using several methods, including hackers cloning an email. The email will look like it comes from someone you know or trust, but its main purpose is to steal your information or destroy your system - whichever reason the hackers sent it.

Worms - Worms are unique. They do not need the action of another program to spread through your computer or network. Worms are often deployed as secret agents. They collect and report information about your network to the hackers. They spread very fast in a network and can cripple it as soon as the hacker accomplishes their goals.

Viruses - A virus is basically a program that is attached to another program or file. They replicate when you access the infected program or file. Viruses are common in shared and downloaded files and attachments sent through email. When the virus is activated, it can send itself to every person on your contact list.

How to Protect Your Business

You need to implement a good security plan and some strategies that will help you secure your platform and protect your interests. In light of the adoption of the GDPR, a lot of companies are making changes to their operations. (Perhaps the threat of heavy fines might be working after all.) One of the benefits of the GDPR is that it allows the average consumer to take back control over their data and how it can be accessed. With this in mind, customers can also report whenever they feel the company is not doing enough to protect their data. To ensure you do not find yourself on the wrong side of the law, we have included a few guidelines that can help you protect your networks and prevent a cyber attack.

Threat Identification

Make it a habit of reporting any threat to your system. Something as simple as unauthorized access might not mean much to you until it is too late. Nothing is ever too small to report when it comes to cyber security. The subsequent loss of information or denial of access to important services is proof of this.

These days, a lot of companies handle information that is very sensitive. This is information that would attract most hackers, especially when they realize your systems use weak security protocols. Remember that hackers are always trawling the internet looking for vulnerabilities that they can exploit. You should not allow them this opportunity.

If someone is going to hack you, at least make their life difficult while attempting it. Take the appropriate precautionary measures to keep the important information about your company safe. Identify and report threats as soon as they happen so that the relevant parties and authorities can look into them and clear your conscience about them before things get out of hand and you lose everything.

Expect an Attack

In the digital world today, it is prudent to expect that an attack is always imminent. This way, you will go about your operations expecting an attack at any given time. With this in mind, the business operations will be carried out with all checks and balances in place.

Try to determine the kind of information you handle and classify those that might be extremely important to hackers from those that are not. Hackers might come after your company for any kind of information. Some might camp in your systems hoping to find a leeway into another company's systems, especially if you deal with other large corporations as third parties.

Astute risk assessment processes will help you make sure you have the right solutions for your problems as soon as they arise. You might not be sure about the type of information you handle, which might be alluring for hackers, so the best way is to make sure everything is protected.

Employee Management

No one has the best insight into your business like your employees do. They are the people who keep your business running and alive. It is only fair that you keep them happy and motivated to work towards the same goals your business has.

In the digital era, loyalty is hard to come by. Your desire to have employees who will do all they can to protect the sanctity of your organization might not be achievable. However, you can take steps to ensure that you never have to risk being shot in the foot by the people you trust. A motivated workforce is always a good thing.

Other than motivating the employees, try to ensure they are aware of their roles in the organization and about the data protection that's required by law. Ensure everyone understands their responsibility and the limit of their liability for the data they handle or protect. Some people freely give away information at times inadvertently, because they are not aware of the risks involved or of the legal ramifications of their actions. Properly educating employees on their legal responsibilities can save you in the long run.

Try to foster an environment where people take responsibility for their actions. This encourages employees to be honest and realize that they're in control of something. They are caregivers and protectors of something important. That being said, you must also take precautionary measures by installing an additional layer of security beyond what you expect employees to do on their part. Your employees might not always be working towards the same goals as you. Where possible, use a password manager to make sure everyone is using an appropriate password.

Two-Factor Authentication

Everyone is using it, so why not implement it for your company? You may have noticed that most of the applications you use have switched to two-factor authentication. From Facebook to Gmail, everyone is adding an extra layer of protection for your data. Try to do the same for your company.

Two-factor authentication helps to secure your systems and data by adding an additional verification step to access accounts. Encourage all your employees to use it. Once you enter the password, you receive a message

on your phone, without which you cannot access the accounts. This makes it difficult for attackers to go after your system, forcing them to find an alternate way to do so.

While you might not be able to stop hackers from trying to attack your systems, you can do your best to dissuade them altogether. Making the access process as inconvenient and difficult as possible is one of the best ways of achieving this.

System Audits

When was the last time you conducted a system audit on your network? Are you certain about the health status of your network? You need an in-house audit and an external audit to make sure your system is not compromised.

Via a thorough audit, you can learn so much about your vulnerabilities you are exposed to. An external system auditor will also advise you on your current state of affairs in light of industry regulations, so that you can improve your systems and operate a compliant business.

When you start your company as a small firm, things like system audits barely make sense to you, and it seems like you're just spending money that you don't have. You might even consider it once in a very long time. However, as the business grows, you will get a the point where the need for a system audit becomes mandatory. An audit helps you reduce the risks of being hacked. There are so many experts in the industry who can assist you with a system audit, including people who have been in the cyber security industry for many years. Their understanding of cyber security will work to your advantage and help you protect your business.

Signing Off Policies

If you issue mobile devices, tablets, and laptops to your employees, ensure they sign them off before they leave the company. This is important so that privileged information is not leaked. You must also look into encryption protocols for any information that is passed through your networks and devices. The idea here is to maintain confidentiality and integrity.

Insurance Policy

It is prudent in this digital age to have insurance against cyberattacks. Hackers are all over the place, and considering the nature of data and information you process, it's strongly advised that you find an insurance policy that suits your operation. When discussing the risks involved with your insurer, you can learn a lot about the challenge ahead and take that as an incentive to address the possible risk scenarios. An insurance policy will cover your business in the event of a cyberattack.

Cyberattack Resilience

The nature of risks you are exposed to once your business is connected to the internet is tremendous. Hackers can have extremely detrimental effects on your operations. A lot of companies today depend on the internet, social networks, and technology to remain competitive in their industries. You need to make sure your company is cyber resilient, so you can avoid risks associated with business downtime, revenue loss, and many other costs you might not be aware of as yet.

The size of your company does not matter. Anyone can be a victim of a cyber attack. Taking preventative measures to protect your business will help you gain an advantage in terms of securing your business by reducing your risk exposure. Besides, an astute security profile will also work in your favor, helping you improve your brand image and business reputation, and it can improve your appeal to investors.

Software Updates

One of the simplest ways of protecting your business from attacks is making sure you use updated software. Tech giant HP revealed that applying a software patch at the right time can prevent at least 85 percent of targeted cyber hacks. Software developers often release patches for their programs as frequently as necessary, and more often in response to prevailing cyber threats in the global business world. With this in mind, make sure you get the latest update of whatever software you are using. Regular updates keep your systems protected from vulnerabilities. That is why developers release updates from time to time.

Penetration Testing

Not all hackers are bad people. Some hackers are good for your business. To ensure you run a technologically healthy and sound business, you

should consider hiring an expert to perform penetration testing and assess the vulnerability of your systems. This is something you should do regularly. You can do it monthly, quarterly, or even annually, depending on what works best for you. The results of these tests will help you identify where your weaknesses lie, and the consultant will also advise you on how to deal with them.

The Need for Proper Training

If you have the best and most secure system in the world but your employees are unaware of how to manage it, you serve no purpose. Training is important to protect your businesses. Most employees unknowingly welcome hackers into your world. They lack the basic understanding of security policies and practices, and how to avoid attacks.

Many companies have their employees signing into computers at cyber cafes with their official business accounts, and at the same time, they forget to sign out and erase their browsing history when they're done.

Other than training your employees, you must also remind them frequently about the policies they have learned and how to enforce them. Ensure everyone adheres to the set guidelines or your employees will be your weakest link, as they always are. Alongside training, make sure everyone learns the importance of taking responsibility for their actions. Employees must protect their departments and dockets. Data access is a critical aspect today that should not be taken lightly. Once everyone understands their responsibilities and accountability for devices in their care, you will have an easier time mitigating cyber hacks.

Protect Your Emails

Among other attacks, phishing attacks are mostly propagated through emails. This is an elaborate form of social engineering where the hackers convince the recipient that they are someone they should trust. Considering that emails are the primary form of communication at the moment, there are many risks involved in using unprotected emails. To protect your emails, you should invest in an anti-spam service that screens your company emails.

Virtual Private Network (VPN)

It's advised that you purchase VPN software and ensure all employees install it. If they need to access the company services and they are not within the premises, they must first connect the VPN. VPNs encrypt all information that is exchanged through them, improving your security. With a policy like this, all communication takes place over an encrypted channel. Some organizations even run VPN services at work, making it difficult for anyone to breach their systems.

Disaster Management Plan

Make sure you have a solid disaster management plan in place. In the event of a data breach, you should have a recovery plan that will restore your business to full operation in no time while you try to solve the issues behind the scenes. A disaster management plan is not a one-off thing. The plan must be tested periodically and updated to meet the current business demands and highlight resilience to present cyber attack risks.

Privileged User Access

Everyone at your company cannot have the same level of access. Some people only need limited access to enable them to carry out their operations. This especially applies to data access. Some elements of the data in your possession should be restricted to employees with high privilege access.

In data management, you must make sure you have the right controls so that everyone has unique administrative abilities over the data systems your business runs. Sensitive information should only be accessible to very few people in the business.

Another challenge that you will experience is the proper management of removable media. These are the easiest ways for most cyber threats to breach your system. Someone walks in with a USB drive and plugs it into their work computer, hoping to copy their favorite playlist for work. However, the USB drive is infected, and just like that, their computer also is. The infection will soon spread and before you know it, if this was a targeted attack, your business is under siege.

Insist on scanning removable media before it's used in your network; or alternatively, ban them altogether. Encourage users to share information across networks. Networks have firewalls in place that can prevent the transfer or sharing of compromised files. Today most companies have very fast internet access in their offices. Even at home, most people are connected to reliable internet services. You can share gigabytes of data in a very short time. Instead of copying the file, upload it to a cloud storage facility, and share the link for the user to access it at their own time. This does not just save you from waiting for the file to download, but it also saves you on space.

Chapter 14 Advanced kali Linux concepts

Using abusive services

Services are the most important mechanisms that Linux operates for a better functioning of the operating system. Even windows have services that run-in background. Basically, services are processes that run in the background until you use it. For example, consider a proxy server like Burp suite that will intercept every information that goes on in the browser and if you click No it stops the service and nothing goes there. In windows, which is quite well dominated by graphical user, interfaces services are easily closed down by a click. Whereas in Linux we need to start using command line to start, stop and restart services.

Why services matter to hackers?

Hackers should be well learnt about services because when you are trying to exploit a system you need to stop services that can interrupt what you are doing. Clever administrators use services to make hackers confuse. So, you need to understand the services that are making your exploitation difficult and stop them as soon as possible. Some advanced hackers install their own services after exploiting the system in a way that they will receive valuable information from the host regularly. In the below section we will explain with command line examples that will help us understand dealing with services.

1) Starting a Service

To start burp suite as a service go to Linux terminal as a root user and just use the following command.

root @ kali:service burpsuite start

This will start the service and you can check it using the ps command.

2) Stopping a Service

Stopping a service will completely abort everything that service is dealing with. So always, be careful while stopping a service as any unsaved data will be lost. Now use the following command to stop the service.

root @ kali:service burpsuite stop

You can check using ps command where you will not see anything related to burpsuit service.

3) Restarting a Service

Restarting a service just reboots everything about a particular service. Data will be lost and new service arises all on its own.

root @ kali:service burpsuit restart

This can be used when any service is struck or stops abruptly.

Now in this below section we will use the Apache web server and MySQL to explain how services can be useful for a hacker. This is a very basic and introductory level of abusing services. If you are an efficient hacker, you will understand hundreds of services and will try to learn about them in time and time to be a professional. Now let us start exploring these below services.

1) Apache Web server:

Apache is a famous web server that is being used by several hosting companies for deploying their web services. It is a well known open source web server that is well structured and of good security. We will use this apache web server to learn a few things that can help us as a hacker.

Step 1: Starting Apache

Apache webserver can be started using the following command. Normally in windows and Hosting environment there will be a GUI that lets us start the Apache web server. But in Linux we need to enter the following command as a root user.

root @ kali: service apache start

This will start the web server in the background, which can be accessed from the localhost. You can check if everything is going well or not using ps command.

Step 2: Accessing the local host

Now after starting the server you can go to your local host address that is http://127.0.0.1 using your browser to access apache. You will be

welcomed with an apache page that asks your permission to show the default page.

Step 3: Modify the webpage

Now for a practical example, modify html file to your desired and save it using any text editor. After few seconds come back to localhost and refresh. Boom! You can see the modified webpage. This confirms that service is being run on the background.

How an apache web server can help hackers?

Programmers to create a local host website during development phase usually use Apache web server. This can be linked with WAMP to further expand it with Php or MySQL servers. However, hackers can use it to learn about loopholes in websites without being blocked or banned. Hackers can also use Apache web server applications like Vulnerable App to expand their hacking skills. Almost every Hackathon program use the Apache web server for making their Hacking boxes.

Logging system

Being a hacker, you will certainly visit networks with high-level protection and maintained by hardworking security engineers. And if with all your skills you have exploited the system. After the attack, obviously a forensic investigation will take place and will try to find how an attack has been planned and executed. Everything of this investigation will be based on logfiles that you have left while exploiting the system.

Linux unlike windows is not vulnerable to exploits and attacking's because it has good logging system that records everything the user does. But some smart hackers use different techniques to make themselves undetectable by reading logfiles. We will explain in detail about how hackers need to develop skills to manipulate the logging system.

rsyslog

rsyslog is a definite daemon program that takes care of log files to be created in the UNIX or Linux system. Every Linux distribution uses different techniques to deploy log files. Arch Linux uses a different process unlike Debian rsyslog function. As we are discussing about kali

Linux that is a Debian system we will continue with rsyslog explanation along with few examples.

To know more about rsyslog we need to open its configuration file with any text editor. Please try to find syslog using find command and open it using your favorite text editor. And when you have successfully opened it please go through it and find Rules section. You will find some bizarre text like the following.

kern.* -var/log/kern.log

This is where log instructions are given to the Linux kernel. When we look at it thoroughly, we will find a basic command that log functionality uses. It is as the command shown below.

facility.priority action

We need to describe these three things in detail to get a thorough overview about the concept.

1) Facility

Facility is something, which is being logged. For example, mail designates about the mail system. There are few that comes under this category as explained below.

a) mail

This explains about the mailing system that is present in kali Linux. This precisely says that mail usage is being logged

b) user

All user related instructions or functions comes under this category.

c) kern

All messages that deals with the kernel comes under this category

d) lpr

All messages that deals with the inbuilt printing system comes under this.

2) Priority

If the facility describes which messages to log, priority decides on what to log. There are different types of messages that can be used to a better

logging system. We will describe some of them below.

a) debug

This is used to log the things that happen as it is.

b) warning

This is used to log things that work but can go wrong.

c) info

This is used to log about normal information that exists. This can also be used to log date and time.

d) error

This can be used if something badly goes wrong while doing a work in Linux.

3) Action

This is quite simple to understand than the rest. It just means that the logs should be sent into this particular category. We may manually assign folder but it's better to leave them, as it is to go to var folder for better management. We will give some example destinations that logs are sent normally

a) Kernel files:

These are normally sent to /var/log/kernel . You can just go to the directory and open the log file using leafpad to analyze them.

Now as we have learned everything we will just look at an example that deals with all of this.

mail.warning /var/log/warning

This precisely means that mail system warning message logs will be sent to /var/log/warning path.

Automatically clean logs

Log files can make up a lot of mess if you use them extensively. We need to make a strategy to keep how many logs depending on the time interval. However, we can use logrotate function in kali Linux to configure few functions that can help us clean log files.

Open logrotate.conf file and modify the text file to create your own log system according to your own necessity.

How to spoof log files?

You might wonder being a hacker how people get rid of tracking when they attack any target host. Luckily, Linux provides few functions, which can help us to spoof log files that is to modify them in a way such that network administrators cannot detect what happened during the attack. This process is called shred. We will explain about this process in detail in the below section.

Step 1:

Shred function just fills the log data with randomly generated UTF-8 code in the logged data again and again to make it as unusable data. To check shred function just click the below command in the Linux terminal as a root user.

root @ kali: shred

Step 2:

To make any file into unusable shred file you need to call the shred command with the file name. That's it. With a single click, all your data will be made into a difficult data that cannot be read or understood by anyone. The command is as below:

root @ kali: shred (insert file name here)

root @ kali: shred desktop/kalishred.txt

Step 3:

There is a special function in shred command that can help you shred the file as number of times you needed to be. But the only negative thing to worry about this is when you try to shred a file by 20 times the time taken will increase exponentially. So always listen to your senses when trying to shred a file multiple times. -n command describes the number of times function. Command is shown as below:

root @ kali : shred -n 20 /desktop/kalishred.txt

There is also another way to make logging stop. When you have control over system as a root user, you can simply disable the service by using the following command. We can use three commands start, stop and restart for this service.

a) start

This starts the logging function allover again.

root@kali: service rsyslog start

b) stop

This stops the logging function in a split of a second.

root@kali: service rsyslog stop

c) Restart

This will first stop the logging function and will start again as a new variable.

root@kali: service rsyslog restart

Automating tasks with job scheduling

As a hacker, the most important skill you need to learn is to automate things. Whenever you attack a system or exploit a system, you need to get ready with a ton of things that will automate things for you. An automated backup or automated deletion of logfiles everything needs to be done for a better productivity and results. In this section, we will discuss in detail about automating tasks using kali Linux.

crontab

Crontab is a function that is available in kali Linux that will let us schedule an event or job for a particular time. We can enter the data from minutes to years to start a crontab task.

root @ kali : crontab

Click -help to check the functions of the crontab in detail.

Scheduling a backup task

Backup is one of the essential thing to do whenever you are dealing with an important data. When data is backed up, it can be used as an alternative

if there is any leakage or corrupt in data. So administrators always prefer backing up the data. But it is a difficult and boring task to backup manually every day. So we can create an automatic backup with the following command.

00 1 18,28 ** backup/desktop/backup.sh

Here first 00 stands for the top of the hour. And ** to any day of the month.

Crontab shortcuts

Below we will display a few shortcuts that are used in crontab automatic task scheduling.

1) @yearly

This will make the task to run once a year.

2) @ weekly

This will make a task to run once in a week

3) @ midnight

This will make a task to run at midnight every day.

Starting tasks at startup with rc

While startup certain scripts start their tasks automatically using rc scripts. This will help them prioritize in the process and will give good results. If you are willing to add a service to start automatically on a startup, you can use the following command.

root @ kali : update-rc.d servicename enable/disable

Protecting you with TOR and VPN

It is obvious that the most important thing for any hacker is his anonymity. Now days due to restrictions of Government and constant spying had made people to find alternate options to maintain anonymity like TOR and VPN. Before going to learn how to maintain your anonymity in Kali Linux, we will have a good explanation about all the options we have for securing ourselves in this matrix world that is all connected.

Why Anonymity matters?

Imagine if your country has blocked your internet access to social networking during riots and all of your people want to use it for better communication. You can do with a VPN or TOR bundle and not are detected. However, tracking can be done in any other way if they want to. But make sure to follow this for some better peace. In the below section we will learn about anonymity services that has different uses.

What is a proxy server?

Proxy is a middle man between you and server that you are trying to reach. Imagine if you want to deliver a package from New York (your place) to Colorado (Server place). Instead of going and giving the package all by your own, you will ask your friend to deliver it. Here your friend acts a proxy for you. This is how the proxy server works.

There are many proxy servers like Socks4, http, https and Socks5.

How a hacker can use proxy server?

When doing a password attack you will normally be blocked by the website due to too many requests. In these situations, you can use a bunch of free proxies to randomly occupy the proxy address and attack the login page. This is a famous technique called cracking that is used by novice hackers to get an access into the system.

What is a VPN?

A VPN is a quite common advertisement that you might have used while watching ads in YouTube. A virtual private network abbreviated as a VPN acts like a middle man but delivers your request in encrypted form to the server in such a way that the server can't identify you. And when the server sends you the response it again encrypts it and sends towards you. Imagine this example to get a better understanding of how a Vpn works. Imagine that you want to deliver a Love Letter to your classmate. But you don't want any other person to read it other than your best friend. So, you write a Letter in quite a different way that no one can understand and sends by your friend to your classmate. Remember that your friends know how to read it. He will decrypt it to her and she will send a response in the same way. This is basically how a VPN works.

In the next section, we will describe about how internet communication works and will give a practical example that will let us understand the fact that Anonymity is a must.

How the internet works?

Every internet connected device has an IP address that can be easily tracked using different techniques by the government. When u send an email or surf internet without any Anonymity services, you are just being a product to Tech giants like Google. They will collect a lot of information from you and will sell you as adds to the businesses. Apart from that, every movement of yours will be tracked and can help them create new products.

Normally when we click on an URL the packet that contains your request will also contain the IP addresses of both yours and the server that you are trying to reach. In the communication process, it will travel through different routers called hops before reaching its final destination. When a packet is travelling, it can be easily sniffed and can be used to acquire information about you.

For an example, use traceroute command to check how many hops that a particular website takes as below.

root @ kali: traceroute bing.com

You will get an output that shows the number of routers it needs to travel to reach the final destination. When the packet is travelling, anyone can sniff it and can attain sensitive information about you and your request.

What is TOR?

Concerned with security of Internet few independent security researchers has developed a network called TOR network that will encrypt the hop we are going through. TOR basically makes your request go through its servers all the while making your data encrypted and untraceable. This will dramatically increase the security of your system. But remember that this may make your networking slow as it needs to travel between

encrypted servers. But when you are trying to attack a target host, it is best to use TOR network.

To access TOR as a command line interface you can enter the following command.

root @ kali : tor service start

This will start the TOR bridge circuit for you and will make every request that is going on from your system to travel through TOR servers to reach destination server.

You can also use TOR project bundle that consists of browser to use it for your daily purposes. A good thing about TOR browser that nothing of your information is tracked.

Is TOR the safest?

Unfortunately, you can't fully depend on TOR because there are rumors that some of TOR servers belong to NSA organizations. If at all your packet travels through one of their hops, your information can be easily retrieved. So, try to use it with Sock5 proxies so that you can never be tracked.

In the next section, we will explain about proxies in detail. Proxies are the middle man and can be used for secure and safe communication. They are even extensively used for password attacks.

Kali Linux uses proxy chains a networking utility to manage proxy services in the operating system. We will learn about in detail in the next section.

a) Basic command

root @ kali : proxychain < rules here> < arguments here>

b) With proxychain we can proxy whatever service or process we want to. This will just an ip address on its top.

root @ kali : proxychains nmap -sV -Pn 192.232.2.1

c) You can set the proxies in proxychain configuration file and can use it to rotate whenever possible. You can find free proxies form many websites online. You can even buy premium proxies for a less rate in many markets.

d) Open website with a proxy in a browser

This is a special command and automatically opens a webpage in a browser with desired proxy address. Command is shown below.

root @ kali: proxychains chrome www.bing.com

e) By default, if you add more than one proxy in the configuration file it will automatically move between the servers. They are used by different proxy chaining methods. The first one is dynamic chaining and the second one is random chaining.

(i) Dynamic chaining:

This will help us to connect the web using chained proxies that are in an order. All the proxies are connected according to the order that they are placed in the configuration file.

(ii) Random chaining:

This will help us to connect to the webservices using proxy chains and all the proxies are connected randomly as in the configuration file.

A little more about the Virtual private network

We discussed before about the functionality of a VPN in detail before. Before choosing, a good VPN try to look at the number of servers and countries it is offering. Some VPN services work slowly due to their latent proxy chaining methods. A Vpn can not only be used as an advanced proxying service but can also be used by organizations and universities to have off campus authorization easily.

Services like Shibboleth does this for International universities. Nordvpn, Hma pro Vpn are the best virtual private networks that we can recommend because they delete the log files automatically and will be no chance of getting trace your activities.

Encrypted mail:

Free email services like Gmail and yahoo work well and gives us high storage facilities. But we are often vulnerable because our email data remains unencrypted and can be easily obtained by sniffing or other techniques that malicious hackers use.

So to get rid of this try to use mail services like protonmail for a small price to make all your all mail encrypted. This is how we can protect ourselves from the tracking and become a hacker that everyone wishes to be.

Conclusion

Congratulations! You've come a long way since you first opened this book! It might've been difficult but progressing through the cyber-security field can be extremely rewarding and satisfying. You should not be ready to start with penetration testing on your own without the training wheels. You will become a professional ethical hacker in no time if you put the work into it.

The journey is not over yet, however. Don't rely on this content alone, because penetration testing is such a developed topic that you can write entire bookcases on it. This guide should clear up the mystery behind ethical hacking and guide you through all the basic penetration testing methods, however reading a book is not enough. You must take action! Develop your skills further by taking advantage of all the online resources on hacking and join a community with the same interests as you.

With that message in mind, let's go briefly through everything you gained by reading this book:

It's important to understand basic terminology and what a penetration test actually is. We also spent some time exploring the mind of the black hat hacker, because as an ethical hacker you will have to walk in his shoes sometimes in order to create accurate simulations of a real attack. Do not take unnecessary risks, and always perform a test only if you are fully authorized to do so.