HACKING WITH KALI LINUX

The Advanced Guide about CyberSecurity to Learn the Secret Coding Tools that Every Hacker Must Use to Break All Computer Configurations with Networking, Scripting and Testing

DARWIN GROWTH

HACKING WITH KALI LINUX

The Advanced Guide about CyberSecurity to Learn the Secret Coding Tools that Every Hacker Must Use to Break All Computer Configurations with Networking, Scripting and Testing

DARWIN GROWTH

Hacking with Kali Linux

The Advanced Guide about CyberSecurity to Learn the Secret Coding Tools that Every Hacker Must Use to Break All Computer Configurations with Networking, Scripting, and Testing

Darwin Growth

Table of Contents

Introduction

Congratulations on choosing *Hacking with Linux: Underground Beginners Tools to Learn the Basics of CyberSecurity and Become a Hacker by Breaking into Every Operating System with Ethical Linux and Precise Computer Configuration* and thank you for doing so.

The following chapters will discuss hacking with Linux systems in detail. Hacking is an art of exploitation and can be used in various useful and dangerous purposes. This book helps us to understand hacking concepts in layman terms. Apart from a thorough explanation, we will also get an example that will help us to expand the horizons of the topic.

Hacking is usually complex and may take a lot of time to master. As a matter of fact, according to a recent anonymous study, it usually takes ten years to become a professional hacker. In the computer industries, there is obviously a lot of need for ethical hackers due to various reasons. For these reasons, you need to master hacking using Linux for better career opportunities.

This book delivers a lot of topics in a smooth way. We will first discuss the importance of Linux and hacking in detail and then move forward with a lot of concepts .

Why Linux is used in this book?

You may have your reasons to avoid Linux but as far as hacking is considered Kali Linux is the best bet you can take. Also, Kali Linux is an operating system that is open-source and can work out things in a better way, unlike Windows which always block hacking tools via a firewall.

How to get the most out of this book?

This book at first will give a layman explanation to the topic and in the next step provide commands so that there will be no misunderstandings of the subject. Also, at the end of every chapter, a clear explanation of the things we have learned is described. So, do follow it.

There are plenty of books on this subject on the market, thanks again for choosing this one! Every effort was made to ensure it is full of as much useful information as possible, please enjoy it!

Chapter 1:
Introduction to Linux and Hacking

This introductory chapter in detail will introduce you to the world of Hacking and Linux in detail. Hacking is a process to exploit or take control of a system. Whereas Linux is an operating system that is used for various tasks that a usual everyday operating system like Windows or Mac does. In this chapter, we will give a brief description of hacking and how it works along with a brief step by step theoretical introduction on why Linux is the best operating system for hackers.

Let us start the chapter now with a brief introduction to Linux in the next section. Remember to take notes while trying to learn this stuff as this is a layman's introduction to the topic. Try to explain the concepts you learned in this book to someone who never studied the subject by using your own words to make a good foundation on the subject. Let us start now the exciting journey about Hacking using Linux.

What is Linux?

Linux is an operating system that is so much related to UNIX one of the few pioneers in the early computing industry. One of the most important things for the success of UNIX is its excellent portability. Anyone can obtain the source code and write their performing system in back those days unlike commercial operating systems like Windows and Mac OS.

With the success of UNIX operating systems in the programmer's arena, its creator has started the GNU project to expand the possibilities of the project. A lot of programmers enthusiastically participated in this small world. Out of those programmers, a college-going student Linux Torvalds has started writing his code for the project. And within few months he has released the code which got the immediate attention of the other enthusiasts. Due to its robust and simplistic nature, Linux has become everyone's favorite within a short frame of time.

Its creator has used repositories to let people contribute to the project. Within few years Linux has expanded into a level of the commercial

operating system with the help of thousands of programmers voluntarily contributing the project.

From then Linux has expanded into various Distros and different editions developed by different enthusiasts. At present, Linux is one of the most used software by programmers, database experts and most importantly by hackers. In the next section, we will discuss in detail the reasons why Linux has become popular?

Why is Linux the Best Operating System?

One of the most important success notions for Linux is that it has a great adaptability for server-side systems. Database administrators are more comfortable in using command-line interfaces than Graphical user interface systems which have become common. Below we will discuss other reasons in detail.

1) Open-sourced

Linux is one of the few open-source operating systems that are available. It means that anyone can download it for free and can use it to develop custom or third-party operating systems, for example like Red hat Linux.

2) Degree of Modularity

Linux kernel consists of five different parts that can be changed or organized according to their actual needs. That is one can select or filter the functions that are important for them. This made individual users interact with the operating system more comfortable.

3) Hardware support

commercial operating systems need to update their hardware support after a few months. Whereas Linux operating system gives much before hardware linkage due to its large number of contributors that write code independently. Due to this reason, there are a lot of hardware systems that only work with Linux.

4) Security

People have a misconception that open-source systems are prone to vulnerabilities and easy attacks. But this works oppositely because Linux has more Authorization and administration security features than windows. Users can select their security features in both basic and advanced levels.

5) Multi-user & Multitasking

Linux can be used by different users and on different levels by the options they select. It doesn't decrease the speed or change the way the system works. Apart from multi-user functionality, Linux is also very good at Multitasking. That is performing a lot of tasks in the stack.

6) High level of portability

As we said before Linux systems can be connected with any other systems from high-end servers to low-level Arduinos. This is the reason why Linux is loved by system programmers to robotic developers.

In this section, we have given a detailed explanation about Linux and its characteristics that made it a favorite and famous operating system. In the next section, we will give a brief introduction to hacking and explain in the later section about why Linux is the most preferred system by hackers.

What is Hacking?

Hacking is one of the most controversial and creepy terms that has taken over our technological generation. A lot of years back when there are telephone lines and are used extensively for communication few people tried to exploit these networks of telephone lines with a system called phreaking so that they can make calls for free. This is one of the first methods of system exploiting that is known in a wide range to programmers who are developing software systems.

Hackers by a definition mean that people who are trying to exploit the system either a network or software or hardware by using different techniques either by a program or devices. Hacking has been divided into a lot of hierarchies and types which we will discuss in detail in the next chapters. But for now, assume that hacking means to exploit systems by code.

Who are Hackers?

Hackers are the individuals who try to exploit systems or understand the loopholes in the system to fix them. People always treat hackers as bad guys but try to understand that all the security administrators who try to protect the billion-dollar servers and databases are also technically called Hackers. In the next, we will discuss the most important characteristics of hackers in detail.

Important Hacking Skills to Have

This section will in detail explain the most important areas where a hacker should be perfect. We will organize these characteristics in such a way that it would be easy for the reader to go through this book. Let us start!

1) Fundamentals of the operating system they are using.

A good hacker will always have a sound knowledge about the operating system that he is using. It deals with a lot of technical knowledge like

memory and process management along with a lot of commands that will make the work easier. A lot of professional hackers will have a detailed knowledge of the Kernel they are working on. So, try to consume the operating system knowledge as deep as you can.

2) Scripting

A good hacker will always write his programs to automate the tasks that otherwise may take a lot of time to do. Get accustomed to a scripting language like python and start writing your programs. If you can't write your code there is less chance of being called a good hacker. So always try to experiment with things using scripting.

3) Knowledge about the Internet and web

The most basic task of hackers is to exploit networks and web applications. Thus, a thorough knowledge of these technologies is a must. Always get yourself updated with the latest server and web technologies that are being developed upon. Learn about port scanning and vulnerability testing in detail for making fast progress as a hacker.

4) Hacking tools

It is practically not possible to write your tool for every task that you need to perform. So, you need to understand the usage of a lot of hacking tools that are available to perform a lot of basic, moderate and advanced tasks. Always try to experiment with new tools and you can have fun exploiting systems.

5) Ethics

A hacker can perform both good and bad actions. However, remember that there is a lot of satisfaction in stopping the bad boys from making money using loopholes. Always understand what you are into before doing a

certain attack or exploitation. It's you that should decide to play on which side.

These are the basic characteristics that need to be learned or one should be aware of thoroughly to become a hacker. In the next section, we will in detail explain why Linux is the best operating system for hackers. Let's jump right into it.

Why Hackers Love Linux?

As we said before Linux is the popular operating system among Hackers and system administrators. Many reasons made hackers from generations to choose Linux as their default operating system. In this section, we will discuss this in detail.

1) Control

The normal windows have a graphical user interface that can be easy to work on with most of the users. But apart from easy interface windows and Mac restrict its users to manipulate the system or the organization they have created. Whereas Linux works on the contrary way. The command-line interface which is a basic building block of Linux can help users to manipulate the system they are working on in any way. This lets the users perform complex tasks and that's what hackers need all the time.

2) Security

For now, Windows has a huge number of applications being developed followed by Mac because there are a lot of novice users using these systems to perform their daily life tasks. This has made them easy prey for crackers and hackers who in a huge number try to find loopholes in the systems. But Linux has more security features among the all other OS and thus is often preferred by hackers who take their anonymity very strongly.

3) Changing the OS features

Linux, when compared to other lets its users change things as they like. People can sort out the important networking tools they use and can customize it on their desktop. A lot of other functionalities like Ram management and Mac address can be easily manipulated using Linux, unlike windows. This customization capability is one of the most important reasons why hackers prefer Linux. There are a lot of customized GUI interfaces like GNOME, KDE, MATE for Linux .

4) Expanding things to fit your preferences

You might have heard about Star Wars already. It is one of the most famous science fiction books that have changed the whole genre. It worked on a concept that one can create their storylines using the star war universe. Linux too works in the same way. By using the kernel source code one can create their Operating system called Distros in Linux world. This has made much easier for things to organize in a better way. And hackers too utilized this functionality to make things better for them. In the next section, we will discuss this in detail.

What is Linux Distro for Hackers?

As said before Linux provides the capability of creating Distros which are predefined systems. Some professional Hacker communities who wanted to give back to the community have created backtrack Distro for hackers. It has been a huge success and has become a pathway for novice hackers.

Backtrack provided a lot of open-source hacking tools pre-loaded in the system along with a lot of editing tools and IDE's. After a few years backtrack has discontinued and evolved in a new form as Kali Linux which is now one of the most used Operating systems by Hackers. It has a lot of hacking tools neatly organized. Apart from Kali Linux, there are also Distros like Parrot Linux that are used by hackers. In this book, we will use Kali Linux as default Distro to explain the concepts for a wide

overview. In the next section, we will explain how to install Kali Linux in detail. Follow along to understand things easily. Let's go.

Installation of Linux Distros

In this section, we will discuss how to install any Linux Distro with step by step instructions. We will also give a detailed analysis of topics like partition, boot loader, and others to get a good overview of the Linux essentials. Let us start now!

Essentials for installation

Step 1:

Get the Boot ISO file of the Linux Distro you need to install on your system. You can download it from the websites to load into a bootable CD or USB.

Step 2:

If you are interested to use windows at the same time in your system you can use double boot option to choose the operating system at boot up time. Anyone of them will be selected to boot according to your choice .

Step 3:

You can also use a virtual machine software like VMware in windows to boot into Linux. This is the most preferable way by hackers because it becomes tough to track when you are using a virtual system.

By this explanation, we have understood the different ways we can use Linux. Now in this section, we will look at the step by step installation of

any Linux Distro. We will assume for our convenience as Kali Linux as we are learning about hacking.

The Steps You Need to Install

1) Start the bootable CD or USB or virtual machine to enter into the Graphical user interface of the installation process. There is also an option to install the Kali Linux by using the command-line interface.

2) In the next step, the Boot file automatically detects the required drivers. And if there are any malfunctions drivers the system will not further proceed into the installation. You can google the error if you are stuck with any to get a step by step troubleshooting procedure.

3) In the next step, you can select your preferred language. Most of them would select the option with " English (us) ". Choose whatever language you want the interface to be .

4) In the next step, you can select the time zone and country. Select the options you want to use.

5) In the next step, we need to select the network monitoring settings. Connect to any wireless network if you want to. You can even select the network drivers that you may need to install in this step.

6) In this step, we will go through the most important step in an installation that is partition. The partition will help us to determine the file system we wanted to use. There is an option for ext3 or fat32, choose whatever you like.

And in the next step choose the hard-disk drives that need to be partitioned. There is an option for complete partition which will delete everything and do a fresh install. You can also use custom partition according to your needs.

7) In the next step, we can input a username and password for the operating system. Re-enter the credentials and start the installation process.

8) After some time, the installation procedure finishes, and we will be welcomed with a welcome screen of Kali Linux or any other Linux Distro you are trying to install.

That's it. It's all we need to know to install a Linux Distro on the computer. We are now full of knowledge and practically ready with everything to experiment with Linux and start hacking. Get ready to have fun with Linux basics that we are going to learn in the next chapter. A good overview of Linux structure can help us hack things efficiently. So, let's start to go!

Chapter 2:
Basic Linux Commands

In the previous chapter, we had a brief overview of Linux and hacking along with a step by step installation of Linux. In this chapter, we will talk about a lot of Linux basic concepts like process management and file management with commands in detail. This chapter helps us to use the Linux structural concepts to exploit systems with efficiency. Before starting the concepts, we will learn about the help section in brief.

How to Find Help while Using Linux?

Linux is a pretty open-source operating system with a lot of commands that one can operate with. You can use the below choices to find help if you are stuck with any command or scenario.

1) Use the man page in the Linux system. This is the default help page for any Linux Distro. It approximately holds 2600 commands and its use cases. You can search among them to know about things you want to seek.

2) Use Stack Overflow when you are struck with any error or warning messages.

3) You can search in Linux forums or GitHub issue trackers to find any bugs or issues in the operating system. In this way, you can improve your knowledge exponentially.

In the next section, we will discuss various Linux basic topics in detail. Let's start our journey into the Linux world.

For a better understanding of these important concepts, we have divided the concepts into three main structures. They are described below.

1) User management

2) File management

3) Process management

We will discuss these three Linux building blocks in detail in the next sections starting with user management.

User Management in Linux

Linux offers a lot of options for maintaining its user groups. There can be both individual users with only reading abilities and individual users with writing ability. Groups can also be used for easy organization of workspaces and teams working on different projects on the same server system.

Why user management matters to Hackers?

Before learning in detail about the user management system in Linux it makes sense to know why hackers should know this. We will explain this in a simple scenario.

Assume that an attacker wants to exploit a server system of a big software company. He uses simple port scanning at first (we will talk about this in later chapters) to find open ports. With the help of open ports, he will try to find access to the system. But if he tries to attack an open port, he may get detected by system administrators easily. So, to make things easy he needs to find user groups with reading abilities and get access to the system.

In this similar way, professional hackers use the user management system to exploit the systems that they got access to. For this reason, a clear understanding of the user management system is important for anyone who takes hacking seriously.

User management system in detail

Linux uses a process called usernames to distinguish between different users. People can also use a password to protect their accounts.

There are three types of users in normal in a Linux system which we will describe in detail.

1) Normal users:

Normal users are the ones who can access their directory only. They can't access other directories, if they are permitted to access other directories then they are restricted to write any files. Normal users are given a mandatory UID which will help others to recognize the user.

2) Root users:

Root users are the ones who are the administrators of the system. They are called super users and have an Id which is 0. Root users can write and modify any part of the file. If a hacker can get access to a root user account, then he can completely delete the files that are present. Usually, server administrators are Superusers, so it is very tough for hackers to get administrative privileges of a system.

3) System users

System users are not real users but users that are created by the programs that are run in the system. For example, when the Chrome browser is started certain system processes will start with the name of system Id. It is important to track and sort these system IDs for better usage of the user system that Linux provides.

Below we will give a command that will help us understand the Linux user system:

linuxexample @ host: systemid 234 4

Apart from users Linux also offers group systems. Groups are important for the management of a huge number of users working on the same project. It also helps to organize things in a better way. By default, every user in the Linux system belongs to a group.

Every group is represented by GID in Linux. The only Root user can create groups and organize them in a definite way. However, a user can be in one or more groups according to specifications.

Below we give some commands which can help to know your current user ID and group id:

linuxexample @ host : get UID

linuxexample @ host : get GID

As discussed earlier every Linux system account needs a username and password. Passwords, as we all know, are prone to attacks and are the first thing that can be tried to exploit. Passwords can give one-way access to all the sensitive information for hackers.

Linux usually holds all passwords in two files. They are

1) /etc/password

2) /etc/shadow

The first one stores the password of the current user and can be easily read by the user.

Whereas the second one is more sensible and contains passwords of all the users in the system. This can be only read by the root user and will not be visible for normal users.

In the next section, we will describe various commands that can help us to modify user groups. Follow along:

1) New user

In Linux, if you are willing to add a new user to the system you need to enter the following command

linuxexample @ host : new UID 5363

Whenever you tried to create a user using the following command with a name you would be opted to choose a password which is then stored in both /etc/password and /etc/shadow. After the successful addition of a user, a separate UID will be given to that particular account.

Apart from that, a new home directory will be created for the user. It should be remembered that a default user group will be created on the user name. There is also a special directory called /etc/skel where all of the configurational files of the user will be stored.

This is all you have to know about creating a new user in the Linux systems

2) Change password

The password is the single pathway to access all the directories and files in the user system. You can use the following command to give a password to the user.

linuxexample @ host : pw UID 2435 to strange

It should be remembered that ordinary users cannot use their username as the password. However, root users do not apply to this condition.

3) Modify the user

Modifying is always a preferable option for hackers. Hackers usually insert an exploit or trojan in the directories and try to spread them into the whole system. For this reason, hackers should be aware of modifying a system.

user mod command is one of the most important commands that can be used to modify the home directories that are present. You can also use grep command to display the content that is present in the system directory .

- m option can be used to change the default directory of the user so that everything present in this directory has advanced privileges.

4) Delete the user

Sometimes hackers after getting what they want from the system will try to delete the user system to delete any log files that may be used to detect the attacker's identity. This is one of the most important commands to learn if you are looking to attack systems with huge security.

By using the user del command as shown below you can delete the normal user and if it is performed by the root user he can delete any user that is present in the system.

linuxexample @ host : UID del 239844

5) Add group

User Groups are created to make things easy for the administrators to make the mess clear away. In Linux, there is a separate directory called /etc/group that will store all the information related to user groups.

Below we give the command that can be used to add the new group. Follow along:

linuxexample @ host : add GID 3783

After entering the command, you can cross-check in the /etc/group to confirm whether a group is created or not.

6) Delete a group

Like the user system, it is also productive to delete the user groups if there is no use of it anymore. Hackers too evidently use this command to wipe out a set of user groups that they find easy to be get traced.

Below is the command to delete a user group:

linuxexample @ host : groupdel GID 3453

Remember that every directory and information that is present and related to every user will be wiped off. There are very fewer chances of getting the data back unless one uses professional backup and recovery tools.

7) View the User's

There is a special command in Linux called uses that can be used to check all the users that are present in the system no matter if they are alive or not at the moment.

Here is the command with an output for the user's command

linuxexample @ host : view UI D

Output:

2443 sample1
8942 example
0987   admin

4673 systemuser

8) Finger Command

Finger command is used differently and is used to find the awake user or group systems at the present moment. This can be highly beneficial when performing complex system tasks.

Below is the command for the finger functionality with an output:

linuxexample @ host : finger UID

Output:

2443 sample1
8942 exampl e

9) Cron Command

Linux system runs on services. Services are basic tasks that can be used by operating systems to perform their desired tasks. Cron command is a special set of commands that can be used to automate tasks like starting an antivirus automatically when you boot up the system or switching into a VPN profile when accessing a particular software.

Below we explain with an example about cron command in detail:

service crond start

This starts the cron service and lets us run things.

Service crond status

With this command, you can easily check what is going on.

All of these tasks will be stored in the /etc/crontab directory.

By this, we have explained a detailed explanation about the Linux user management system and in the next section, we will in detail explain about file management system which is one of the most pioneer branches that a hacker should be perfect at. Let us go!

File Management in Linux

Every operating system follows its own algorithms to organize files and called them a file management system. Windows users as a simple file management system that can be easily modified or applied using keyboard shortcuts or graphical user interfaces.

But in Linux, a set of commands should be learned to perform even simple tasks like moving or copying within the directory. This gives a good level of secure functionality to Linux. In this section, we will learn about all this stuff in detail.

Why do hackers need to be aware of file management in Linux?

Linux is an operating system that deals with files and directories in a whole lot different than windows. Hackers need to learn about modifying directories so that they can easily exploit the system when they gain access. We will know about a few of these now.

1) Absolute path

Every directory or file has a distinguished path that can be used to notice or manage things easily. There is also quite a complex successor of it called a relative path about which we will discuss in the next section.

For example, consider this path

/Srujan/downloads/red.mp4

This is called an absolute path because it all over points towards the file.

2) Current directory

When we are working in Linux, we often want to know the current directory so that we can easily modify things. You can use the following PWD command to know the details of the current directory.

vulnerhost @ example : cd /etc/get

3) Relative path

Relative paths are the upper and lower levels of the absolute path we are working with. They are represented by the dots and are called as special directories by the Linux creators. Below is a small example using the command to understand in a better way.

vulnerhost @ example : cd /etc/get
.....
vulnerhost @ example : cd /etc/

4) Touch to Create Command

Linux uses various methods or commands to process files. Here we will explain about creating a new file of any type using touch command.

Linux can create a lot of file types such as .txt or.MP3 by using the touch command as shown below using the command.

First of all, you need to be in the directory you wish to create the file and then enter in the following way:

vulnerhost @ example: touch sample.mp3

After entering the check command, you can recheck using the -l command for viewing the files in a current directory.

5) Delete the file

Deleting a file is a basic task any hacker would need to learn. In windows, you can delete with a click, but Linux offers a special security layer that will not let you delete any system files such as log files. To remove any files, you need to use the rm command as shown in the following example

vulnerhost @ example: del example.gif

6) Move or rename files

Linux provides a command that can be used for both moving and renaming files. Moving files may become essential to hide forensic investigators about the attack you have done. It may be also a lifesaver to easily get sensitive information.

This command can also be used to rename files. Below is the example that describes the following two use cases:

vulnerhost @ example : mv example.gif

[for moving the file]

vulnerhost @ example : mv example.gf to report.gif

[for renaming the files]

7) View the file

Normally text editors or IDEs can be used to view the file content. Certain file types for suppose like an MP3 can be opened by a music player software. However, Linux provides a command called the cat that will let us read the file in the same way that Linux kernel reads it. Below is the command for the cat command with an example.

vulnerhost @ example: cat songs.tx t

8) Head Command

Normally files consist of a lot of information and can cause crashes will opening using the cat command. To get rid of this disadvantage you can just see the first 10 lines of any file using the head command. This will help for a fast recheck of log files when there is an attack or delete your login information when you are the attacker.

Below is the command to view the file:

vulnerhost @ example: head songs.txt

9) Tail Command

If the head command lets the users see the first 10 lines of the files, the tail lets the users see the bottom 10 lines of the code. This can be used to easily organize the system programs by using their results or to see the final result of the system processes.

Here is an example that describes the following command:

vulnerhost @ example: tail songs.tx t

10) Make a directory

We have already described a directory as a file system that hierarchically stores files. This mkdir command can be used to create a new directory on Ur preferred location.

vulnerhost @ example: mkdir songs

11) Delete directories

Normally hackers delete a lot of directories just for fun. Or sometimes they do it to keep their traces off. By using rmdir you can easily delete the directory you prefer.

Below is an example that explains the command in detail:

vulnerhost @ example: rmdir songs

12) Copy Directories

Replication is one of the important concepts that hackers need to learn and should be perfect at. When you attack and get access to the system you will look for sensitive information such as usernames, credit card names that lie in the system. System administrators would get alert if any of the data is deleted or moved. So obviously a lot of hackers replicate the data into their servers or physical devices using the cp command.

Below we give an example for cp command in detail:

vulnerhost @ example: cp songs to movies

13) chmod to Change Permissions

Linux uses permissions to make things work in a better way. Usually, only root users can modify any file or directory that is present. Sometimes hackers will get access to the system but will get unsuccessful in performing system tasks due to no valid permissions.

However, Linux provides a command called as chmod that can be used to change permissions or give access to your files to other users. However, remember the fact that the root user can have access to all of your information.

Below we explain with commands about this functionality in detail:

vulnerhost @ example: chmod +x songsdir to movies

14) Find Files

It's usually difficult to find files in Linux than in Windows because it uses a separate file system, unlike windows that sort out files easily. Certain commands can be used to find the file you are looking for easily .

a) General search

This is the normal way to search in databases and searches every directory that is present to get the desired file you want. Below we will give some commands that will explain the general search in detail.

Finding an mp3 file named “beatles.mp3”

We enter the command find with the pathname and file name as shown below:

vulnerhost @ example: find file beatles.mp3

By this, the find command will start searching the required file and will give the results. If nothing is found for the name, then the empty screen will be displayed.

There is also an option with an asterisk that will show every file with the extension. Suppose we only give .mp3 extension as a file name using asterisk then find command will search every mp3 extension that is present in the directory.

Although find is used extensively to search for things in a Linux system it is often slow. The reason for this is that it starts from the root directory to search the file name. For this reason, there is another command called as locate that will reduce the search time. We will learn about locating in the next section .

b) Database lookup

Linux contains system files and databases that exist with them. As explained earlier it is difficult to search every application database due to their length and huge numbers. For this exact reason database lookup is introduced in Linux.

This will search and input the database files that are present according to the search term. Before using the locate command you need to use updated so that everything will be refreshed to display the fresh results.

Below is the command for locating command. You can use the file directory that you prefer or command will search all directories that are present.

vulnerhost @ example: updated

vulnerhost @ example: locate songs.mp3

c) Find the execution file

Execution files are special installation files that are used to make programs run for the first time. Windows use this extensively but Linux can also run them with certain software. You can also search execution files in Linux with a command called. This will display the path of the system file.

Below is the command example for this :

vulnerhost @ example: exec demon.exe

In the next section, we will discuss in detail about compression technologies present in Linux. Let us go!

15) File Compression

Users use compression technologies to reduce the file size. Compressed files can also be encrypted easily to store sensitive information and can be opened with only a password. Winrar is the most famous compression utility present in windows. However, Linux is open source and uses other software's which we will explain below in detail.

a) gzip

The usage of gzip is pretty simple and straightforward. All we need to do is enter the following set of commands with the file name we are trying to compress. This utility is mainly used to compress configuration files as it is good at making a set of small files into a compressed package fastly. Below are the commands:

vulnerhost @ example: gzip start beatles.mp3

file compressed successfull y

b)tar

Tar is another famous compression utility tool that is very famous in Linux. It also works as gzip utility but has additional integration capabilities that gzip doesn't offer. The best thing about tar is it compressed and integrates at the same time. Thus, for hackers who are trying to exploit and compress a lot of files at the same time, this is the best choice. Below we will give some commands that will help us understand how it functions. Take a look at it:

vulnerhost @ example: tar start beatles.avi

file compressed successfully

By this, we have completed a brief overview of various file management system concepts in Linux. In the next section, we will discuss process management in detail. It is obvious by now that Linux runs by processes. Learning about the process can help us work more efficiently. Let's dive into it in detail.

Process Management System

So before going into further details, we must know what a process is and why it is important in the context of Linux and its system functions.

What is the process?

As deep it goes process is just a term that explains that the operating system is currently filtering things to process the task. Processes are dynamic and nowadays a lot of computer systems are capable of handling multiple processes. Supercomputers are said to process trillions of them.

Linux being a kernel modified system has certain free will restrictions to processes. Usually, processes in Linux consist of three cycles namely

starting, running and blocking. We will explain these three states in detail as shown below.

a) Starting state

The start state, in brief, describes that the process is getting ready to be allocated by the CPU and other resources to run.

b) Running state

Running state explains that the process that we are currently dealing with is running with a certain part of resources. There are tools like task manager that can show the process monitoring.

c) Blocking state

The blocking state explains that a particular process cannot be run anymore. They may have been killed on purpose or can be crashed due to errors and warnings. Whatever the reason may be blocked state initiated the killing of the process .

Processes, Procedures, and Programs

We have already discussed processes in detail. Procedures are processes that are aligned systematically and linearly. Whereas programs are a set of procedures that can be combined to create a good system software.

There are some important characteristics of processes that hackers should be aware of. We will explain some of them below:

There are two types of processes. The first of them are mutually exclusive processes and the second one is synchronization processes.

Mutually exclusive processes are little skeptical processes because you cannot run them in the background or correlation with others. For example, like a recovery software or like using a printer to print papers.

Synchronization processes are usual processes that are that can be run in the background. You can consider a media player process for this example.

Commands for process management

Usually, the Linux system runs an abundant number of processes. When you start and boot up into the system tens of programs get initiated. It may be an antivirus or backup system software. To look at all of the processes that are running in the system you may enter ps command with parameters.

vulnerhost @ example: ps PID 34534

Some of the parameters that are present are listing, displaying process id and CPU percentage used. You can even make processes sleep, pause and give priorities. We will discuss some of them in detail here:

a) When we enter ps command we will get total processes that are running. The first line describes the names of the process and the PID that is assigned to them.

What is PID?

Like User I'd (UID) we have discussed before PID is a number that is assigned to a particular process. These are not permanent and will get collapsed when the process ends, unlike permanent UID.

b) The second line describes the initiation time of the process and the percentage of the system power it is consuming. This is important for

hackers because whenever a process is taking a lot of system power one can end it easily using the kill command which we will describe in the next section.

c) The third line can be used to declare priorities for the processes. For example, when you are performing exploitation and backup at the same time you can give priority to one of them as you wish to give more system resources. This will help hackers when they are doing injections to a lot of databases or networks.

And at last, we will learn about the termination of processes. A lot of processes can decrease the system efficiency and will make Linux buggy. So, for a certain interval of time, you need to kill some processes by using the kill command. Kill command will stop all the processes at once by using killall or will just end the process you want to.

Below is a command that explains how kill works:

vulnerhost @ example: kill example process

d) You can even restart the killed processes for once using the same command. This just acts like a recycle bin for the processes.

vulnerhost @ example : restart exampleprocess

With this, we have completed our brief explanation about process management and for hackers, this is important and can help them use their resources efficiently.

In this chapter, we have given a brief introduction to important building structures of Linux that are user management, file management, and process management. In the next chapter, we will learn about scripting and in particular about shell programming in detail. Before trying to enter into the next chapter practice the commands, we have discussed in a Linux

device. The practice is the only way hackers can prosper. Let's go and learn shell now!

Chapter 3:
Basic Shell Programming

In the previous chapter, we had learned about Linux essentials for hackers in detail. In this chapter, we will dive into one of the hacker's secrets weapons that are scripting. There is quite a small difference between programmers and hackers. Programmers use scripting to build systems whereas hackers use scripting to exploit systems. Without creating their scripts, a novice hacker can never become a professional Hacker but will remain as a script kiddie who just uses other tools to crack systems. Thus, scripting knowledge is a must in the checklist for anyone trying to master hacking. To help you out this chapter will introduce a lot of bash scripting concepts with real-world coding examples. Let's have fun with some scripting now!

First of all, we need to know about the shell in detail.

What is a Shell?

A shell is that cursor you observe when you first connect to a server using a password or when you make yourself connected to a system using remote desktop tools like SSH. In other words, if you want it to look solely from a programming point of view you would be delighted because it acts just as an interpreter between the user and system just like how an operating system does .

But it just sends the input advises from the user to the Linux kernel and sends the output that is the result back to the system user.

Types of shell

There are types of shells that exist according to the Linux official documents. Out of both the first one stands for a GUI whereas the second one stands for CLI.

There are a lot of shells that have been manufactured with the Distros like Bourne shell, C shell, korne shell, and Bash shell.

Out of all different types of shells that are present bash shell is one of the most famous that ever existed. It is pre-installed in almost all the famous Linux Distros. It also acts as an interceptive language that helps the Linux kernel understand the instructions we are giving logically. In the next section, we will look at this in detail.

How does the bash shell work?

There are two types of modes that one can work shell with. Out of which one is an interactive mode and the other is a script mode.

a) Interactive mode

In this mode, the Linux user can enter the functions or the bash code one by one and wait until the result is given. If there is an error in the middle the user cannot proceed further. It just works interactively like in an old handheld video game.

b) Script mode

In this mode first of all the bash code will be written in a text file and then will make to run the script file using the command-line interface. While using this mode the user can get all the results that he was looking for all at once. Hackers need to be more perfect in script mode because it will be easy to exploit systems fast using this way. However, programmers that are who create systems will prefer interactive mode more.

Before knowing more about the grammatical structure of the shell it would be better if we have a good overview of the advantages of the shell.

Advantages of the shell

1) It is very easy to learn inline programming languages that differ a lot in both execution and implementation.

2) It has a lot of help documents that will help the hackers to rectify the errors as soon as possible .

3) It has an added advantage because it is an explanatory language. That is, it need not be compiled before running. So, hackers can easily cross-check the code before trying to implement it on the victim's system.

Apart from this shell is also fast and works efficiently. Due to all these reasons, hackers should mandatorily learn about the implementation of the shell.

In the next section, we will give an example shell script that will help us to understand the basic grammatical structure of shell programming. Let's go!

First shell script

Let us create a shell script of the name sample.sh. create a shell script using the following command.

cat sample.sh

Location of the shell program

echo " This is very regressive"

Now we will explain this in detail. Line by line .

a) #! This represents the starting of a shell script that we are trying to write.

b) If it starts with only a hash # then it is called a comment. Comments are annotations that are used to make it easy for reference or for other users

that want to look at the code. It may seem unnecessary to write comments for small shell scripts. But it is a good practice to start writing comments.

c) echo is a shell default command that lets the interpreter display the content that is written.

Here to run the shell you need to use the following command:

bash sample.sh

And then the output will appear

For this example, the output is as follows:

This is very regressive

There is also another feature that will let you run the script with additional permissions. As we discussed earlier Linux has a set of permissions and if you don't provide with necessary permissions the script may not run perfectly. So, to provide permission use the following command

In the next section, we will start discussing the debugging of the shell scripts. Debugging is one of the most important programming tasks. Even hackers need to be perfect at this because wrong debugging of code may result in bad adaptation of the task.

Debugging the shell scripts

Normally when you enter a wrong default command in the script such as shown below in the code.

vulnerhost @ example: ech 7898

This code will not run and show an error as shown below

the ech command is not found

This is exactly what debugging is. Debugging features informs the user about the errors in the script.

There are also a lot of shell debugging tools that perform the tasks we do in a command-line interface. Tools like bashdb are famous for this. In the next section, we will learn in detail about a handful number of important bash built-in commands. This section will help hackers understand the basics of shell programming effectively. Let's go!

Built-in Shell Commands

Before entering into a deep discussion about the built-in commands it is important to know that these built-in commands cannot be used as variable names. Variables are an important functionality of shell programming that helps to define things.

Linux provides a command called type that will let you cross-check whether a command is a built-in command or not.

The command works as follows:

type echo

The output is as follows:

echo is a built-in shell

Another example,

type trum p

The output is as follows:

Trump is not a built-in shell

Also, remember that two dots that is (••) is used to determine the successful working or execution of the script. Here are the in-built commands we are going to discuss in detail.

1) Alias

Normally Linux commands are a little trickier to type. I suppose you have to type echo every time it may be difficult. For this reason, you can use an alias to give shortcut for a command.

Below we describe the command that needs to be entered to make alias work.

example@ linuxwar : Alias groupecho

However, it should be remembered that aliases work only until the shell environment is open. That is if the shell is exited there is no way to access it again. Also, the alias functions are stored in the bashrc directory of the user environment. Aliases are an easy way to increase productivity. Hackers use a lot of aliases to make deciphering the script a lot trickier.

2) Unalias

As you might have guessed already unalias is used to delete the alias systems that are present. By using this command, you can delete any alias command that you have created before.

Below is the command that will let us understand how it works:

example@ linuxwar : unalias groupecho

You can also use -a to delete all the aliases that are present at once. However, as we said before ending a shell environment will delete all the aliases that are present but using unalias. will help you to delete things while you are still scripting.

3) bg,fg,jobs

A lot of shellcode is done in interactive mode. Sometimes when you are trying to exploit a system you need to perform various tasks at once. These tasks are called jobs in Linux terms. So for everyone's convenience jobs are divided into two types. The first one is a foreground job where we can see the procedure that is going on. The classic example of foreground jobs is the installation of system programs. You can't handle other jobs while doing foreground jobs.

Solely, for this reason, background jobs are developed. Background jobs can help things run in the background. Hackers should be well aware of this because they are ought to work with multiple processes.

Below are the commands for the job functionalities:

example@ linuxwar : bg job1

example@ linuxwar : fg job2

example@ linuxwar : view jobs

4) cd

Cd is the classic Linux shell command that is famous for its huge usage. When performing tasks users usually are thrown into the root directory by

the shell. Huge usage of root directory can make it scattered and messy. For this reason, Linux users use CD to change their directory and perform actions.

Below is the command for the change directory:

example@ linuxwar : cd /etc/rea d

5) Declaring variables

Variables are classic programming declarations. They are usually used to declare a position for the data. Variables also have a type declaration known as data types. With this, we can easily assign the type they are ought to use. There are many data types such as int, float, string. We will discuss all of these programming concepts in detail in the next section with examples.

6) Break

Scripting languages usually include Conditionals and loops that are used for repetitive and logical tasks. They can be used for both of them aligned. While doing repetitive tasks it is obvious that there should be some endpoints for better interaction and processing.

For this reason, shell language uses a statement called break that will stop the task of the logic it has provided satisfies. Break statements can also be used to print the statements using the echo command.

Here is an example for break command:

example@ linuxwar : beep.sh

for(i=0)
x>1
y>2

```
if(b>2)
break :
```

7) Continue

In loops where a break can stop the loop at once, there is a statement called continue that can help to switch the available loops. Suppose if there are five loop statements in the shellcode by using continue the loops can be interchanged. This will help to create a detailed exploiting code that can compromise systems and do multiple cross re-checks.

Below is an example of the continue statement:

```
example@ linuxwar : beep.sh

for(i=0)
x>1
y>2

if(b>2)
continue:
```

8) Eval

Linux and shellcode usually consist of a lot of arguments that need to be processed. There will be a lot of problems if strings and variables are parsed in the same way. For this reason, a command called eval is introduced in the bash shell.

eval command replaces the arguments that are present with the variables that are pointed out. You can even use eval command to parse strings into commands for execution as shown below.

```
example@ linuxwar : eval beep.sh
```

9) Exec

Execution is a process that is said to start the task. Every installation file is an execution format because it starts a new system shell in the background. Hackers should be aware of execution shells because they perform a lot of initiation and analysis tasks.

When the exec command is entered in the Linux command shell the screen or the interface that we are working on refreshes out. Exec can also be used in script files to start dependency installations as we used in the first chapter to install kali Linux.

This is the command that explains exec command in detail:

example@ linuxwar : exec beep.s h

10) Exit

A shell window is complex and deals with a lot of tasks. However, when you complete the task it is a good practice to exit the shell. If not, the processes would still be running and may result in unnecessary system power consumption. For this, a quick command called exit has been introduced in the shell language for this exact reason.

Exit command also clears all the tasks that are present. So, make sure that everything is fine before making this happen. You can also exit individual processes or programs with a shell script.

Below is a simple command example for exit:

example@ linuxwar : exit shell.sh

11) Export

Usually when the system boots up the first shell command is created in the kernel system. This is called a parent shell. And the next ones that followed are called child shells unless the parent shell is exited or killed.

So, while working with the different numbers of shells we will deal with a lot of variables. And sometimes we may need the same variables that we used in the other shell environments. For this exporting of variables, the shell provides us with an export option.

After using the export command all the child shells can use the parent variables. However, remember that the child shells cannot use their sibling's variables that are the other child shells that are present.

Here is an example that demonstrates this process:

example@ linuxwar : export example.sh to /etc/dir

12) Kill

Killing processes is an important skill to learn for hackers. Processes have three distinct distinctions. One of them is an interaction that is a usual shell interface. The second one is a batch process where everything that needs to be applied is done in a sequential process. And the last one is monitoring the process where everything that is being done is monitored. For example, a task management system.

When you are running a bunch of these processes you may get distracted with signals that they come with. For this reason, killing processes is a good process if you find that they are unnecessary. When you are trying to exploit a system you need to kill the antivirus process that is running in the background. You can even use the killing process to stop the logging files that record your every move.

Below is the simple demonstration of kill command:

example@ linuxwar : kill process

example@ linuxwar : killall

13) Read

Read command can be used to read the bash scripts when you are performing the tasks. Or it can be even used to perform a thorough check of the shellcode that has been written. Read statement is a basic shell command and can help hackers interpret and cross-check things easily.

Here is the command with an example:

example@ linuxwar : read bash.sh

14) ulimit

Priority is one of the most underused functionalities of the shellcode. Priority can be both incremental and decrement also. By using ulimit the hacker can increase or decrease the priority of the process.

Why prioritizing processes is necessary?

When a user is dealing with a lot of background processes that are constantly functioning this may decrease the processing speed of other processes. For this reason, administrators prioritize anti-virus software's at first level of the priority. With this method, any boot level executions can be eliminated.

However, a lot of system administrators don't take this problem seriously and make hackers exploitation easy. Below is the example command that explains how to prioritize the processes that are present.

example@ linuxwar : ulimit PID 2345

Always remember that PID is the most necessary thing that needs to be used to prioritize.

15) Test

Shellcode consists of a lot of loop and conditional codes. Before experimenting with these repetitive tasks with a system shell it is a good practice to check them in the old shell. For this purpose, the test command is introduced.

Below is the command that takes care of the testing:

example@ linuxwar : test PID 3634

With this, we have completed an explanation about some of the built-in shell commands that are present in Linux systems. This should have given a good overview of the hacking environment to you.

In the next section, we will discuss some of the program concepts that need to be learned before writing the shell script. But before learning about it let us learn about the installation of a bash shell, the most famous shell environment.

Installation of bash environment

1) you can use wget to get the system files that are present in the server. The below command will download the files from the mirror websites and will help users install them in their system.

wget bash.com/download

2) in the next step you need to mention or input the configuration of the system that you are using. Otherwise, it may not get installed.

3) After installation, you may need to check the settings and input the default directory. Normally it is entered as the root directory. Also, the shell versions can be easily known using the help command.

With this, we have installed the bash environment and good to go to learn about some fundamentals of shell programming. Remember that these topics very much coincides with python scripting which is another good alternative scripting language for hackers.

Fundamentals of Shell Programming

The shell consists of a group of systematic instructions or commands. Let us go and learn about some of the basic components that comprise the shell language.

Variables

Variables are a piece of memory in the computer random access system that is used to store the data. As discussed before variables are the most important components of a programming language and it is often called while writing functions or templates.

Usually, there are two types of variables:

a) Local variables

b) environmental variables

Let us discuss the functionalities of these variables in detail along with few command-line examples.

a) Local variables

Local variables are the one can which can be used in a private or single environment that is these cannot be used in other shell scripts even with a reference. These types of variables are used in short shell scripts.

b) Global variables

Global variables are also known as environmental variables. These variables differ from the first one because these can be used in any shell script with a reference. For using the global variables, you need to export them to the local shell script file.

Variable naming

Variables present in the shell language should follow some varied instructions while naming. Remember that shell in-built commands like exit cannot be used for the names of variables.

Here are the instructions that need to be followed for naming a variable:

a) In shell language, variables differ from the capital and small letters.

b) A variable name should never start with a number or special character. Doing this may give an error saying that the variable name cannot be initialized.

Here are some of the various examples that can be used

love

dud e

ra344

And here are some of the variable names that cannot be used

1hjsd
#fege

Variable assignments

Variable assignments are the assignment values that are used to give a value to the variable.

It works in the following way:

variable name = variable value

You can insert a lot of data types in the variable value. Data types are the ones in which variables are defined. Some data types consist of integers, floating-point numbers, and even strings sometimes.

Here is an example that describes the assignment value:

sample = 2 2

Special variables

Special variables such as usnet can be used to delete a defined variable from the memory. In this, we can store the random memory management.

There are also special variables that start with a $ parameter. These variables can be used to define additional parameters that the system may require during the process execution or advanced shell analysis.

Here is the example for some of the special variable commands with a $

$dude = ' string'

The biggest advantage of using special variables is that they can be easily filtered and aliased with the help of the character that is present at the beginning of the variable.

Arrays

The array is a famous data structure that is capable of holding multiple items of elements. Programming languages use a lot of arrays because they are easy to implement unlike other data structures like trees or graphs and also they are fast. Shell also supports arrays to input elements. In this section, we will discuss arrays in detail.

a) definition of array

Normally arrays consist of a subscript that defines the number of the element along with the name of the array.

Here is the command for an array example:

example[]

b) Giving value to an array

All elements that are present in an array can be given a value using the symbol. You can also give the value using the individual array assignment like as shown below

sample = “America”

You can insert any data type in arrays just like variables and the use of arrays can be very essential when you are dealing with loops and conditionals with complex code in it.

You can even connect both arrays to get the desired results. This scenario is shown below for your better understanding:

sample[2] = valu e

Constants

As we all know already that constant means something that cannot be changed. Constant values exist always and can be used to explain values like pi that have a constant numerical value. Whenever you try to change this constant variable an error or warning will appear in front of the shell that says this cannot be possible.

Here is an example of the constant command:

pi = 3.1427

Namespaces

We already have discussed variables in detail and namespaces mean that variables that are in a defined scope. These are created for a reason that whenever users try to create variables that are of similar type a conflict always occurs and makes things difficult to organize.

For this exact reason, namespaces are invented and are used to define citations and references which can be used multiple times in a shell interface or a shell script.

Here is an example that explains in detail about this concept:

Operators

Operators are the most important regions of a scripting language. Operators can help to mix or change the variable values. As of the shell, programming goes there are a lot of operators that can be used. We will discuss some of them now in detail:

1) Arithmetic operators

Arithmetic operators deal with mathematical calculations such as addition and subtraction. These are important for programming because they can add up things and multiply variable count easily.

Here is an example command for the arithmetic operators:

```
>>> 2+3

>>> 2-1

>>> 6 * 2

>>> 7/3

>>>  4 % 7
```

2) Relational operators

Relational operators are significant operators and can be used to change things easily. They can be used to compare two things easily. Few of the relational operators are AND, OR and NOT. These relational operators can be easily implemented in any shell language code.

Here is a command-line example that deals with relational operators:

```
>>>> 2 ! = 7

>>>> x === y
```

3) Assignment operator

The assignment operator just gives the value to a variable or loop code. By using this operator one can easily assign things to the element.

Here is the example for the assignment operator:

x = 7

With this, we have completed a brief exploration of the scripting world. Shell language is a must for any hacker that is serious about his job. You can also implement these concepts with python programming for doing advanced tasks in hacking. In the next chapter, we will start with an exploration of going into a hacker's mind and how they plan things. Let us start!

Chapter 4:
Hacking Procedure

This chapter is a pathway to help you start thinking like a hacker. To stop attacks that would come frequently you should make yourself accustomed to the hacking methodology. In this chapter, we will in detail explain the phases that one needs to perform to call oneself a hacker. Let us start to the exciting world of the hacking process.

a) Foot-printing the system

b) Scanning the targets

c) Getting access to the system

d) Using the access for exploitation

e) Continuing the access

f) Creating backdoors in the system

In the next sections, we will in detail explain the six phases in detail. We will give out some example tools which can be used for individual phases .

1) Foot-printing the system

A good hacker would always at first try to know a lot of information about the target he is going to attack. This collection of information about the target is known as reconnaissance. Many hackers use social engineering techniques to get information from the users themselves.

A good hacker has good communication skills that can help him to manipulate things to get information about the target he is trying to attack. To say using an analogy a hacker works like a detective to track the target. He looks at all the publicly available information and will form a roadmap for a better strategy to attack.

As said before hackers manipulate individuals to perform tasks like resetting passwords or sending one-time passwords using social engineering techniques.

A lot of hackers also use Google search in-depth to get as much information about the target. This is one of the most important phases of hacking.

Kali Linux provides software such as nmap and burp to perform reconnaissance .

2) Scanning the targets

This is considered the second phase of the hacking process. In this step, we will try to scan the target and find any ports that are open to getting a successful linkage to attack. We will also use a concept called enumeration in this phase to get a lot of advanced information about the users. All this useful information can be further analyzed by hackers to get varied results.

In this phase, the attackers usually start network scanning using the available network tools like Nmap. These network tools are made available to run on systems so that the available open ports can be detected. Open ports are vulnerable and can help us to create a backdoor to the system.

However, the attackers should keep in mind that fast searching of the systems or sending a lot of packets can give a huge increase in network traffic and can make the system administrators alert. For this reason, experienced hackers extend this phase for at least a week so that they send packets slowly in such a way that the very advanced intrusion detection systems can never detect the attack that is going on.

In this phase, we can even analyze the ports to know about the operating systems and technologies that are being used. A lot of hackers after this stage will search databases like exploited to find the open vulnerabilities for the version of the software. If lucky, you can find a vulnerability that can be further used to attack the system.

Many novice hackers use automatic scanners like burp suite to detect the vulnerabilities that are present. Even though of being advanced scanners they will not accurately detect them always. They can be used for learning the basic implementation of scanning but not as a sole tool that can scan the targets. That is all about this phase and let us move on to the third one that is when we get successful access to the system.

3) Getting access to the system

This is an important step in the hacking process. After having a brief scan and obtaining information about the systems in this step hackers will start attacking the system using various methods. A good hacker always chooses his way of attacking according to the environment that he is attacking on. A novice hacker can read hundreds of books but if he cannot use this information depending on the environment and resources, he has then there is no way that the access will be cracked.

There are infinite ways of getting access to the system. Out of all these, the most classical way is to use social engineering abilities to trick the users that are present in the network area. It may be by sending an attachment to the receptionist or by getting connected to the modem of the LAN network using someone's landline phone. Getting access to the system doesn't result in successful exploiting because of less or void permissions. Some introduction detection systems can detect your access to system providers with a message.

After getting access to the system a hacker will further move to the deeper areas of the network that is to the closer areas of the root directory for full

administrative privileges. Follow along with the next section to understand what one can do using the exploitation abilities.

4) Using Access to Further Exploit

After having successful access in the next stage hackers try to stay as much as the time in the system. An attacker usually tries to extend his capabilities or reach in the area and tries to acquire the root privileges which can help him get additional use cases to perform.

The main reason why hackers can get succeeded in this phase is because of bugs and vulnerabilities that are present in the web application systems or the login interfaces that the system users use. Professional hackers use hardware hacking devices like keyloggers to know passwords or secret root directories. In the next section, we will describe the most important phase of hacking in detail.

5) Continuing the Access with the Systems

Hackers are crazy and like to do things that can be repeated. When a hacker compromises a system, he tries to expand the time he spends therewith using tools called rootkits. Rootkits are hackers' tools and will delete everything or footprints that he leaves while hacking effectively. Apart from this hacker also has a fudge to get access as many systems as possible. For this character trait, they usually try to get access to /etc folder and access all the user passwords that are present. Rootkits will help the hacker in extending his connection or relation with the system in a definite way.

If the hacker is gaining money with this method, he may get accustomed to the fact that many are trying the same. So, he will make sure that the vulnerability he has found is not available to anyone. For this reason, he makes shell scripting code that will spoof the other attackers and make them not access the system. Hackers also in this process exploit as much as they can and will back up important files or sensitive information into

their directory using network packeting tools and delete those traces forever.

6) Creating Backdoors in the System

After getting access to a system for a long time and understanding every pathway and directory system intelligent hackers create backdoors to continue their exploitation even if the vulnerability is patched. It is often difficult for security administrators to determine a backdoor until it causes system damage because they are often cleverly inserted into the system by hackers. In this section, we will discuss backdoor and how to make one.

How to make a backdoor:

1) First of all, look at the system as you are in-depth and try to change the system code in a way such that you can easily get access to the system for the next time.

2) Backdoor injection tools will have the ability to send the password changing information using its exploitation tools that are present.

3) Backdoors can also be created in a clumsy manner and of a lot of variables with weird names so that the programmers can never detect the original attacker. This anti-spoofing mechanism will lead to a change of the system code which will be easily obtained by the hacker using the other backdoors he has implemented.

By this, we have given a complete tour of how a hacker's mind works. It may feel overwhelming sometimes, but hackers work it out in a hard way. So, if you want to be a professional hacker you need to create your working process or follow this straightforward methodology that has been said by many famous hackers.

In the next section, we will discuss the ethical hacking toolkit or prerequisites a hacker should be aware of before starting web hacking and network hacking for testing the quality of the systems. Follow along with this checklist and use it whenever you are starting an attack.

a) Get permissions

First of all, if you are attacking a system with a ton of security and intrusion detection systems you need to get valid permission from the system owners. Otherwise, this may land you in trouble even after using a lot of safety tools because forensic investigators of the industries are always working hard to find the traces of the attackers.

b) Don't use a lot of tools

Usually, hackers overwhelm themselves with learning a lot of tools. Tools are just a way to make the process work. You need tools to automate things but not to change your perspective on looking at things. For this exact reason try out as many as tools that are present and select the best tools that are working for you.

c) Analytics

A lot of software's now a day are providing well-reported analytics of the performance of the system for an easy understanding of the situation that is going on. Hackers should be aware of all of the technical terms dealing with analytics for better productivity and understanding of system analytics.

d) Reporting

Usually when a test is performed penetration testers use manual skills to pitch a report of the attack. It is always best to do a manual report because in no way a machine can think about the effect of this vulnerability to the

organization in a humane way. However, it is time- saving to use inbuilt features in the web application interception software to report the pen testing reports.

By this, we have completed a detailed explanation about how hackers work and even given a checklist of things that need to be done by or testers. In the next chapter, we will have a detailed introduction to web hacking and some of its tools. From the next chapter, we will be dealing with practical things so get ready to have fun with hacking. Let's go!

Chapter 5:
Web Hacking Tools

After a brief discussion of the hacking procedure in the previous chapter, we will now go a long discussion about web hacking in this chapter. As we all know in today's world both web and mobile applications are the pioneers of technology. A lot of hackers try to find loopholes and exploit them for their personal use. So, a thorough understanding of the web is necessary for security professionals and wannabe hackers.

For this reason, we will go in a practical approach to web hacking tools. We will discuss web hacking tools like Uniscan in detail. Let us enter into the world of web hacking. First of all, we will give a small introduction to the web and protocols.

What is the web?

The web is an interconnected system of networks that displays both static and dynamic information in the form of web applications nowadays.

What are the protocols?

It is just a way to transmit information between the client and the server .

Http and HTTPS are the famous protocols that are used for web communication. We will look at six tools that do different tasks.

Scanning of Webservers

Web servers are used to store information in particular. They consist of a lot of information both static and user-based information. If a hacker can get access to a web server, he can exploit any information he wants to.

Usually, hackers do a brief fingerprinting test about the webserver before attacking. This is one of the most important hacking processes that need to be done. If webserver has any potential vulnerability it would be easy to crack into it using a payload.

There will be a lot of web vulnerabilities that need to be checked on the target server. It will be time-consuming to check every one of them manually. So we can use a tool like Nikto to automate the work.Nikto is one of the famous web hacking tools that are pre-bundled with Kali Linux. It scans a webserver using its huge database that consists of potential vulnerabilities of web servers.

Here we will describe some of the excellent features of the Nikto web server scanner.

1) Saving reports XML, HTM L

All the reports that are obtained using the automatic web scanner can be easily converted to XML and HTML formats.

2) Metasploit usage

Metasploit is a console tool that can be used to make exploits. With this tool, you can insert Metasploit exploits.

3) Mutation techniques to fish for content on web servers

There are techniques such as the mutation that can easily sniff or duplicate the content that is present in the web servers. Web servers' fish these things to display good results.

4) Subdomain guessing

This web scanners also use techniques in a way such that the subdomains that are present can be easily found out. These web scanners also sometimes web servers that are not in the scope.

5) Doing a test based on a tuning paramete r

In this tool when we encounter a vulnerability or bug, we usually test it out. The testing of it sometimes does in a varied structure called turning parameters that has a huge ability to concern the things.

Below is a brief process that takes place when an automatic scanner starts.

A) Starting nikto on a webserver

For the starting of the web scanning server, you need to have a host address and hostname along with a tuning mechanism. By using this command, you can easily detect the versions of the webserver or the programming language that has been used

Here is the command for the starting of the Nikto :

example@ linuxwar : start Nikto www.exampleweb.com

B) Running all tasks

Usually, there are a lot of hosts that we can attack. Hackers try to do things at a fast rate by attacking all of the hosts at once. For this reason, Nikto provided a tool that lets you insert the word file so that you can scan all of them at once.

Here is the command that can be used to run all tasks:

example@ linuxwar : run Nikto 193.3234.33.2 3

C) Running against multiple hosts

Where the prior command attacks on different servers at once with a single address in this process we will use different network addresses while attacking the host interfaces.

Here is the command that explains this process.

example@ linuxwar : run hosts host1 host2 host3

With this, we have given a complete introduction to the manual web scanners and in the next section, we will start learning about Wordpress and its vulnerabilities in detail.

Hacking a WordPress Website

Normally websites are developed from scratch using different web programming languages like PHP and javascript. But normally not every small business can afford good web programmers to write separate code for them.

So, a lot of internet users rely on content management systems. And out of a lot that is available WordPress is the most famous. It is used in more than 25% of the websites that are present .

It offers good security features along with a lot of themes and plugins that can be used. However, WordPress is not fully safe from a few vulnerabilities. There are more chances of an XSS or CSRF vulnerability to be found. And the worst part of using WordPress is plugins and themes can be used to insert malicious code. A lot of hackers use this strategy to steal information from the WordPress servers.

To get rid of this problem, we can use a tool called WPscan to scan WordPress websites.

a) First of all, before starting the Wordpress scanner test you need to update the system so that there will be no way that any outdated vulnerabilities can be found.

b) After using the update, you can start the real start with the scanner. All you need to do is to enter the Wordpress URL that needs to be scanned.

Here is the command that needs to be used

example@ linuxwar : start wpscan www.exampleweb.com

c) In the next step, we can use the tool to get the list of users who are present is the Wordpress system. Wordpress consists of a directory of systematic users that maintain or a part of that website. For this reason, this scanner should be used as an enumeration tool whenever it is possible.

d) There are also options in the scanner that lets you brute force the system for root privilege or stop the enumeration system that is present on the website.

If you are the owner of a Wordpress website, you can use this tool to check the security of your website and if it doesn't turn out well you need to install web server security technologies like cloud fare for an additional layer of security mechanisms.

websploit

Webservers in common consist of directories. Directories consist of files. It should be noted that not all directories are visible to everyone. These are called hidden directories and can be only visible for the root user.

Hidden directories consist of sensible configuration files that can compromise the system within a very short time. These hidden directories can also consist of private password details. We use a web split tool for making a cross-examination over the available networks.

This software is made of python and is free to download from the wget package manager system. After installing, start it using the tool name in the Linux shell.

Below is the command using apt shell command that will install the websploit framework:

example@ linuxwar : wget websploit

Web sploit consists of a lot of modules such as wireless and network modules for example. It should be remembered that web sploit works in coincidence with the Metasploit. Metasploit an exploit maker tool and can help users insert exploits in various files. We will learn about these Metasploit functionalities in detail in the last chapter.

Now we will look at the procedure where hidden directories can be discovered.

a) Before starting you can filter out the error options to wield out some of the most famous errors like 404 error not found.

b) It is already installed in Kali Linux and can be found in the module’s directory. The directory scanner module which is one of the most

important modules in the websploit tool can be used to find out the directories and its syntax forms .

Below we explain some of the commands that are present in the directory scanner module which can be used to scan hidden directories:

1) Show - This command will display all the web modules that are present. When hackers deal with a lot of exploits they often get confused and mess up things. For this exact reason, web sploit consists of inbuilt modules that are used to find vulnerable directories. And this show command can help us find some of these for us.

example@ linuxwar : show websploit www.exampleweb.com

2) Verbosity

Verbosity is a simple statement that lets us set the number of results that can appear on the Linux shell. When we start searching hidden directories usually a lot are found and can make things confusing. To get away from this problem we can use verbosity command to display the custom directories. There is also an option that will make us look at all the things in a static form.

3) And the next important command is RUN which helps us to run the exploits with the websites we desire. We can also use this network transmitting system.

example@ linuxwar : run websploit www.exampleweb.co m

When you follow these commands with perfection then there are huge chances of websites getting compromised.

Cloud flare web sploit

We even have a second set of webs sploit commands that can be used to resolve cloud technology. Cloud fire is one of the most important security layers for websites and is now maintaining and securing the utmost two million websites from dangerous attacks.

First of all, to use the cloud flare module you need to find for it in the web sploit modules list as shown below:

example@ linuxwar : websploit select cloudfare www.exampleweb.com

Now after getting the interface you can install cloud flare in any of the sample websites to check whether it works or not. The working process of cloud fare deals with changing the original network address of the system to one of its servers. Thus, if there are any injection attacks or brute force attacks it would stop or ban that address at once. Cloud fare acts like an intrusion detection system for the websites at a very low cost.

Why the cloud flare is still easy to bypass ?

As we said before it just spoofs the attacker with an IP address. Many hackers started collecting hundreds of Cloudflare addresses and started to abandon them whenever they attack. Some tricks can be still used like using this cloud flare scanner to find all the IP addresses that the website hosts with.

In the next, we will learn about uniscan one of the most important web fingerprinting tools.

Uniscan

Uniscan is used normally for the remote code execution or remote file insertion of the vulnerability scanners. It also can perform network commands like ping, traceroute, software detection.

Here is the command that searches to determine the operating system using the uniscan

example@ linuxwar : uniscan select domain

Uniscan also provides a tool like NMap open port detection. It specifically checks the os version of the server and scans the service.

Uniscan also provides a way to report the scanning reports using the export options as shown belo w

example@ linuxwar : uniscan export domain to domain

With this, we have completed a brief introduction to uniscan and would now leave for the next section which will deal with the listing of subdirectories.

Sublist3r

Websites consist of a lot of subdomains. Usually, domains that are in the scope can be used easily to manipulate using applications like burp suite. For suppose, Gmail has a lot of subdomains and if we can find access to one of these, we can easily manipulate the whole website.

This is the reason why subdomain enumeration is one of the most important concepts hackers should learn. We have a lot of tools that will help us find subdomains. In this section, we will use a sublist3r to do the task.

Sublist3r is not present in the Kali Linux tools list. For this reason, we need to install it from the git repository. Below we explain how to install sublist3r. You can use this method to install any third-party applications that are not available in the Kali Linux repository

Installing sublist3r

1) Select the directory you need the tool should be installed using the cd command.

example@ linuxwar : cd install sublist3 r

2) GitHub is an online repository that makes things easy for programmers when cloning the application. It is different from package managers because one can actively contribute to the application using git console.

Here is the command that can be used to install sublist3r

git clone (URL)

3) Now every git folder has a requirements file that will help the system to install the other tools that are needed to be installed to make the software work. These are called dependencies. Hackers should have a good understanding of this because of many encounter errors.

We will let you understand dependencies with a perfect example. Imagine that you are trying to install a java application like Android studio. If there is no java installed in the system you cannot install and use the Android studio. That is what a dependency stands for.

In the next section, we will explain the working of the sublist3r. Follow along to learn about it in detail.

Starting the sublist3r tool

Run the following command to start the subdomain searching tool.

example@ linuxwar : run sublist3 r

We will get a lot of options that can be chosen from this tool. We will even have a help section when entered -h that explains the commands that can be used.

Here are the functionalities that this tool can perform in detail:

a) Domain -d

You can enter this parameter to insert the domain you want to find subdomains for.

b) Brute force

This parameter can be used to start a brute force attack using a lot of domain lists that are entered in a text file. This can be particularly used when you have a lot of domains to test.

c) Ports

Ports are the functionalities that can be used for easy sub domain referencing. This parameter can help the user find vulnerable subdomains

using the open ports .

Apart from these basic parameters, you can use output functionality to get the results into a text file from a shell interface.

We will now give some example commands that will let you understand subdomain enumeration in detail:

1) Python sublist3r.py -d amazon.com

This command will start an execution that will display all the subdomains that are present after using the

2) You can use this command to brute force the first 100 domains that are present in the text file.

python sublist3r text.txt

Through these simple techniques, you can find subdomains. After finding the subdomains list you can use techniques like a recon to further dig a lot of information about them.

While trying to hack a web application, hackers should prefer this methodology to easily catch the easy way to get onto the application. That's it we have completed a brief explanation about the available web application tools and in the next section, we will start a detailed explanation about network tools. Let's go!

Chapter 6:
Network Hacking Tools

The most important and complex to handle while hacking is dealing with networks. Network in layman terms is just a system of interconnected networks. The Internet is the biggest network that has changed lives. Companies and a lot of industries run with interconnected networks. Whenever a hacker gets successful in entering a network, he will try to hack the other subnetworks too. We will in this chapter learn about a lot of network concepts and commands that will make hackers crack the networks easily. Let us go!

What is a Network?

A network is a group of systems that are bound to work together or in a total sense used to exchange information from each of them. For the appraisal of this definition, we use a lot of technical devices that are used to exchange information. Some of these devices are routers, modems, antennas, wires and even groups of satellites that continuously track geographic variants for the working of GPS.

Kali Linux consists of a lot of network tools that can be used to connect to an embedded system or for being used as a server maintenance tool. We even have used the network card configuration and wireless integration during the installation of the operating system. In the next section, we will discuss ifconfig one of the most important network tools that can be used to learn about the network details that we are dealing with. All we need to do is to send packet signals and we will learn about in detail.

ifconfig

ifconfig is usually the default command hackers use to know about the network information. It will display a lot of information like Ethernet address, physical MAC address, IP address, and even the network mask.

There is also a section that describes the number of packets that are released and received. Another line describes the collisions of network

packets. While some of them may be useless for hackers they can be used to determine the network strength of the system they are trying to exploit.

Below is a command and output that shows about the ifconfig in detail :

ifconfig

Here are few things that ifconfig command can do:

a) ifconfig can be used to specify the IP address with a netmask. This command can be used when performing a wireless packet injection using the network routers.

Here is the command

example@ linuxwar : ifconfig netmask 223.2.1.2

b) ifconfig on a whole can also be used to determine the broadcast address that the system is on. It can be further manipulated with the deviation of the netmask.

Here is the command

example@ linuxwar : ifconfig broadcast 212.11.1.1

c) ifconfig can be used to end the network devices. Just like killing the processes sometimes it becomes necessary for hackers to end the network drivers or devices they are connected to get rid of sniffing or leaving any traces.

Here is the command for switching off the Ethernet driver

example@ linuxwar : ifconfig eth0 212.1.1. 1

In this way, we can use ifconfig to switch on or off the network drivers. However, ifconfig often only helps us to understand the information that is already available and will not help us to manipulate any network information. For this, we have to use advanced sniffing or clickjacking software's where we can manipulate the configuration files and resources that are present. In the next section, we will discuss some of these complex network manipulation tasks in detail. Follow along!

Manipulating the network configuration file

Usually, when we run an ifconfig command everything that is acquired or obtained by sending network packets is stored in a configuration file. Configuration files are special types of files they maintain a certain order so that the system can detect it. Not every file need not be a configuration file.

However, when we boot or switch off the system everything that is the input protocol information will be deleted forever. So, instead of rekindling the entire procedure other time it is best to write into a configuration file which can be easily found in the, etc folder.

In the configuration file enter the network address and network mask in detail. It should be important because the manipulated network configuration file can be used to do a fingerprinting about the system.

Routing and gateway settings

A network card consists of a gateway and also consists of a routing protocol that looks at how things are functioned here. So before starting the network hacking details, we will learn what a gateway is.

Gateway is like an entrance to the network system that we are dealing with. We usually have computers and these are called hosts and they have an immediate physical address known as MAC address. Gateway works as

a gate or checking point that checks the network packets and sends them to the servers the user is trying to contact. It does the same when a response is received. For this reason, gateways are the most important part of network systems.

Why are gateways important for hackers?

When you are willing to use a VPN or proxy server then you need to enter the gateway. Otherwise, the packets will just pass through the default router gateway.

Here are commands that can be used to change the default gateway:

example@ linuxwar : gateway = 214.133.1.1

In the next section we will discuss routing and why is important for the better performance of the network systems.

What is Routing?

Routing is a network protocol system that sends packets in a definite way so that the time that takes to transfer the packets reduces. When a lot of packets are being sent it usually takes a lot of time and can result in less network bandwidth. For this reason, efficient routing protocols are being developed for better transportation of packets.

For this, we need to create a routing table and should calculate for the flags that may be present in the network system.

In the next section, we will discuss network hosts in detail. Follow along!

1) /etc/hosts

In the early worlds of computing people used to enter the IP address to send or receive any information from the system. But after the successful introduction of the host system, it is no longer used. The host is just a text interpretation of the manual input address.

There is a host file that is present in the etc folder where all the DNS profiles can be added. Nowadays this is usually made by google DNS server which consists of every web address. Also, hosts can be used to know about the number of packets transmitted.

We now discuss here the hosts' directory and give some commands:

2) Search hosts

In this option, we can use a command to search any name server that is present in the DNS profile. When we use this tool, we will get the input address of the website we are searching for. This will help us to find other important fingerprinting technologies.

Below is the command to find the hosts that are present:

example@ linuxwar : search host 23.1.12.1

3) Statistics

Statistics that are present can be used to display the host information. Hosts are very important for a successful connection to the server. You can use various tools that can help us deal with these functionalities.

Apart from using it is a network tool hosts are very favorite of software crackers. Usually, when the software is reverse engineered and cracked by hackers it will have an ability to connect to the internet and redo everything. This is where hackers make use of host profiles. They will add

a line of code in the hosts' files to redirect the software to the localhost. With this, if there is any interruption of services that will be regained.

In the next section, we will discuss one of the most important and easily used network tools that are ping.

4) Ping tool

Hackers often when trying to deal with networks after getting access to the system will try to do work on the ping tool. This is because the ping tool sends an SMP request to the tool and will let the packets received. When you enter the ping command in the Linux terminal the tool will start analyzing the packets and will display the response packets that are receiving. For this reason, the ping tool is often considered the initiation of networking tools that need to be mastered.

Here is a command that explains the working of the ping command:

ping www.hackkali.com

a) when we enter this command, the network will start analyzing the packets that are flowing and will give the following output.

128 packets received 192.674.34.2
64 packets received 192.675.34.2
.....
.....

A ping is a command tool that displays the content in the shell so there is no way you can stop the tool unless you close the shell window. You can further check the ping statistics using the following command and can also be exported into a text file.

192.674.34.2 ping statistics

With this command, all of the statistics that deals with the domain will be displayed. In the next section, we will explain about traceroute another important network tool that can trace where the packet has traveled.

5) Traceroute

Networks are used to send information from one system to another that is present in the same network or to other systems that are present elsewhere. However, have you ever wondered how this information will be passed on?

The transportation of the information is done using packets and routers. Packets are basic traffic that exchanges the information. Traceroute in the basic idea will inspect these packets and will trace whatever they are doing. This is an advanced concept that deals with things that networks are ought to do. Check yourself about the packets that are passing through using the traceroute command.

example@ linuxwar : traceroute 192.23.2.1

With this, we have completed a brief explanation of the network hacking tools and in the next chapter, we will have a brief explanation about hacking hierarchies.

Chapter 7:
Web Hierarchies and Cybersecurity Ethics

In today’s world, it has become very difficult for people who are more concerned about their privacy and security. Hackers tend to work in different ways to exploit systems by using known vulnerabilities. A lot of information is available for some of the most famous vulnerabilities like XSS, SQL injections and CSRF vulnerabilities to understand and exploit them using one's code.

Often hackers use automatic vulnerability scanners to find loops in the web application or a network system. However, there are a lot of hierarchies that are divided based on the motives of the attacker and their goals. In this chapter, we will help you understand all the hierarchies that are present. Follow along to know about hacking hierarchies in detail. This is a bit of theoretical subject so try to think about them in your own words for an easy understanding.

Why Do Hackers Fit Into Hierarchies?

Often people and security researchers face a lot of people who are trying to attack corporate and personal systems. Many times, white hat hackers who in common terms try to protect the systems decide the danger of an attack with the attacker steps and logfiles that they left while trying to exploit the system. With the help of this information, they tend to decide the motivation behind the attack. For better forensic analysis security researchers from a long time are using hierarchies to organize the level of attack. Hierarchies are important for a better understanding and analysis of the attack that took place.

There are seven types of hierarchies as explained below. We will describe each of them in detail in the next section. Follow along for a detailed explanation of each of the.

Hierarchy 1: Script kiddies

Script kiddies are usually the high number of users who call themselves hackers but have very little technical and scripting knowledge. This

hierarchy of hackers are often not so talented and can never break into a system without a step by step procedure or explanation that is often found in hacking websites and forums or social networking groups like YouTube and Facebook.

But they should not be taken of less importance because there is a high chance of script kiddies exploiting system if it consists of outdated technology that is viable to a lot of vulnerabilities.

Hierarchy 2: A group of Novice hackers

Novice here synonyms to quite good. A lot of hackers spend their time in hacking or cracking forums trying to exchange their knowledge and exploiting things together. This hierarchy of hackers due to it for fun. They often try to crack websites like Netflix and try to sell it to them for cheap prices. These novice hackers use cracking tools with brute force ability to constantly login with a bunch of usernames and passwords they have collected using a SQL injection vulnerability.

As we talked about the process you might have understood that this group of hackers purely depends on luck. They cannot exploit usernames or passwords that they don't find. For this reason, people should use secure strong passwords that cannot be exploited by this hierarchy of hackers.

Hierarchy 3: Hacktivists

Hacktivists are advanced hackers who use their knowledge and hacking skills to give sensitive or shocking information to the world that is otherwise is not possible to know. Anonymous a famous hacking group falls under this category. They try to give information about the government or shocking emails that will make the population understand the problems the world is facing. Wiki leaks are also one of them and have shaken the world with their leaked emails of various country presidents. However, this hierarchy of hackers are very rare and are always with a motive that cannot be judged due to its sensitivity.

Hierarchy 4: Black hat hackers

Black hat hackers are the evilest group of the hierarchies and use their skills to exploit normal users. They use a lot of social engineering techniques to lurk the user to give their sensitive information like passwords and credit card numbers to them. They often rely on a lot of malware tools like Trojans, keyloggers to enter into the user system and acquire the information. They use a lot of techniques and strategies to exploit systems.

Black hat hackers are highly professional and advanced hackers who are very difficult to get caught because they use their sock proxies that can go undetected. As far as they make a mistake it is highly impossible to know their identity. And the worst thing is there are more than 5% of hackers who solely sell the stolen credit cards in the dark web. Security analysts and web programmers should be aware of the technologies and tools these hierarchy users use and should develop intrusion detection systems in a way that they will be stopped or even caught.

Hierarchy 5: Criminal gangs

These are a group of black hat hackers who work in a group. This makes things worse than before. Criminal gangs use a lot of hacking resources to originate cybercriminal gangs. They try to smuggle narcotics, guns and other illegal stuff in the dark web. They are very professional hackers who could spoof the packages that are being sent as genuine using their hacking techniques. These criminal gangs are also responsible for huge black markets on the dark web. Criminal gangs work so efficiently that it is even difficult for the FBI to catch their whereabouts.

Hierarchy 6: State-sponsored hackers

Hackers are not ethical people in general but are patriots most of the time. You might have already seen some middle eastern hackers writing their country slogans after hacking celebrity social networking accounts. A lot

of countries mainly Russia and China hire a lot of professional hackers to hack into other country databases where legal or sensitive information can be found.

These hackers can get into any traffic signals or webcams and can control them. They are very anonymous people that work for the benefits of the country and even indulge in cyber warfare with criminal gangs on the dark web. Hacking is a strange and gloomy world if you want to look deep into it. A lot of people fight around the corners of the internet to get access to the farthest point of the internet. This is where everything is present, and these hierarchy hackers work for it.

Hierarchy 7: Automated tools (Bots that spread an exploit)

It is to be noted this hierarchy doesn't consist of humans. A lot of systems cannot be accessed without personal access to the system. For this reason, some highly professional hackers nowadays are creating very small worms (like robots) that can automate or think itself and access the system. These are very dangerous hierarchy tools that are used to attack nuclear power stations and other highly secured places. It is very complex to understand this hierarchy right now because less information is available in the public domain but there are reports that worms with malicious malware are the next huge weapon for hackers.

By this, we have completed a brief and thorough explanation about hacking hierarchies in detail. In the next section, we will discuss in detail about cyber ethics and some of the famous malware attacks in detail.

Cybersecurity Ethics

The cybersecurity field has expanded its horizon by leaps and bounds. As new software systems started to develop there came a lot of importance for the cybersecurity department due to potential vulnerabilities that may

make the companies lose money by some anonymous attacks. For this reason, a lot of industries started offering security solutions for example like Cisco security solutions to protect their clients from potentially dangerous attacks.

For this reason, they started to recruit a lot of system engineers who have sound knowledge of database security. Decades later now cybersecurity is one of the pioneering fields in computer technology. There are a lot of software and tools that provide automated solutions. And there is still a lot of necessity of manual labor.

In this chapter, we will discuss the ethics of cybersecurity in detail. First of all, recite a simple fact that everyone who deals with security is called a hacker. We will now discuss the three most famous types of hackers that are distinguished for a better understanding.

a) White hat hackers

b) Black hat hackers

c) Grey hat hackers

That's it. We will now discuss each of them in detail.

White hat hackers

These are the type of hackers who try to protect databases and servers from being exploited by the bad boys. They usually try to find vulnerabilities in the system and try to fix them as soon as possible. They use different hacking and network tools to track the resources and systems they are dealing with. White hat hackers are a role model and will inspire a lot of novice hackers to walk on the good side.

Black hat hackers

These are the type of hackers who try to exploit systems using different techniques. These guys are usually professional and will follow a lot of precautions to not get caught. They create their defective mechanisms like trojans and worms to exploit systems. Black hat hackers use services like VPN, Tor to hide their identity.

Grey hat hackers

Grey hat hackers are a special category of hackers who are not into the bad game but are willing to help the bad guys to play. These types of hackers usually have fun in detecting vulnerabilities. When they detect a vulnerability, they will sell that information in a dark web which will further be abused by many black hat hackers. However, these people will not exploit the system by their won due to various reasons.

Through this explanation, we have got a deep understanding of the different types of hackers. In the next section, we will have a brief description about penetration testing.

What is Penetration Testing?

Penetration testing is a technical name that lets users find loopholes in the system to fix them. Usually, security researchers perform penetration testing attacks to help the company.

Penetration testing tool kit

Kali Linux provides a lot of tools for penetration testing in its resources. As explained before there are a lot of stages that need to be performed to confirm that the system is completely safe from any attacks. For this purpose, you need to perform all the penetration tasks like scanning, vulnerability testing, mock exploiting. It is better and safe if you can maintain a backup procedure for all the data that is present.

In the next section, we will discuss some of the famous cyber-attacks that had happened. This is theoretical information and can help you understand the scope of hacking and threats hacking may possess to both economic and safety prospects.

What are cyber-attacks?

The Internet is a weird and dangerous place. A lot of people try to find the real place of the internet which is buried deep beneath the dark web. The dark web is a place that cannot be accessed by normal browsers like chrome in any way. To access dark web websites, you need to use the TOR browser, about which we have discussed already.

Dark web consists of a lot of websites that sell stolen information by hackers. This is where hackers who have found a loophole in a famous system will try to take advantage of it by selling it to other hackers. A lot of cyberattacks happen for two reasons. Out of them, one is money and the other is cyberwar between countries.

You might have heard about ransomware virus that had spread into millions of systems a few years back. This is a perfect example of a cyber-attack. Here are the top three cyberattacks that have happened in the last decade or so .

1) Yahoo hacking target

Yahoo is a good pioneer technological company that deals with search engines and services like mail and news. However, whatever the reason maybe it has been a victim to one of the largest cyberattacks that have ever been.

In three years, yahoo user accounts have been compromised for more than three times and millions of accounts were just available in the dark market for sale.

This is the single reason why the company has put on sale and was bought for less than what it deserves. Seems like hackers have taken advantage of a broken hash file structure that is present is the yahoo databases.

2) Equifax cyber attack

Equifax is a credit card issuing company and has suffered a major breach where hundreds of thousands of credit card numbers have been stolen. The hacker has tried to sell these credit cards in dark web markets and the company didn't state unless the vulnerability that is responsible for the breach has been fixed .

3) Ransomware attack

Just a couple of years back ransomware virus has infected a lot of businesses in the European Union. This virus has used an existing vulnerability that has been patched by the windows way before the attack. But for varied reasons, many businesses didn't update their systems and got locked out to the ransomware system virus which threats that the data will be deleted unless money is paid within a set of timeframes. This is the reason why system administrators should keep updated with the system and should get ready to follow journals for pointing out existing vulnerabilities.

Apart from these China, Russia, and America usually has a lot of cyberattacks going on every second for various reasons. Cybersecurity space has become crowded and a lot of individuals, businesses, corporates, and governments are trying to get control over them. It is obvious one should be aware of the misjudging or threats of hacking and should try to learn and follow cybersecurity ethics. That is all about this chapter. In the next chapter, we will discuss hiding the attacker's location and information using TOR and VPN. Let us go!

Chapter 8:

TOR & VPN in Linux

Hacking is a risky task. Novice hackers are always easy to get caught if they don't use varied precautions. Almost every professional hacker hides his original identity with different tools or his written code to get detected. Several tools are included with Kali Linux to help you stay anonymous while attacking systems. However, remember the hard fact that tour government, Isp providers and sometimes even the VPN services that you are using can track you. As you get significant experience in the hacking field you will develop various strategies that can help you spoof your identity with ease and conviction. For now, follow along this chapter to know in detail about TOR, VPN and how to spoof your MAC address in detail. We will give a set of commands and examples in detail for your better understanding of the topic.

How to Use the TOR Network in Kali Linux?

Normally if you want to install Tor in any of the windows or Mac systems you need to install the tor browser bundle that will start an anonymous server and routes all the traffic through it.

But in the Linux terminals, we will get an opportunity to start the tor routing server from the command line itself.

Use the following command to start tor bundle service:

start tor

First of all before connecting to the tor server check your IP address. Because you need to recheck whether the Tor server is working or not look at the IP address.

What is TOR?

TOR is a chain of interconnected computers that are present from the different locations around the world that are used to spoof the location of

the system. Few network engineers who have the motivation to make the internet secure and stop getting monitored by government agencies has started this TOR project.

How TOR works?

Whenever a request is sent from the TOR service or ToR browser the request is sent to one of the TOR networks. You might have confused now because this is how proxies work and how it is different from it and how it can be different from it?

This is where TOR achieved something no one ever did. TOR service, unlike proxies, doesn't route through one network but a bunch of interrelated anonymous networks thus making the detection very difficult.

Tor browser bundle

If you are not skeptical about the tor service, you can use the tor browser bundle which sends the request through the service. Every hacker should learn using the TOR browser because it makes detection very very difficult and also users can look at the dark web and its important contribution to the hackers.

What is the dark web?

The dark web is like the down layer of the internet that is often untouched and undiscovered by normal search engines and browsers due to various reasons. TOR websites have a .onion link and are very statically built websites.

The dark web is famous for black hat hackers because everything that goes around there is illegal and theft. We did not advise you to do anything illegal, but it would be a good case study to look at the people who ethical hackers will be fighting on.

Are there any things better than TOR?

As of now, the TOR browser bundle is the best way to hide your identity or spoof things. But virtual private networks (VPN) can also be used to maintain anonymity and from a different wide variety of servers. We will talk about virtual private networks in detail in the next section.

How to use VPN in Linux?

Before discussing the installation process, we will, in brief, discuss the VPN technology.

Virtual private networks are at first used in private industries and government institutions to maintain a group of people even when they are off-site. However, people have found a way to share their servers with other people without transferring any information about the sender and receiver. This made VPN popular and useful for a lot of users and mostly for hackers because of its ability to hide the location of the user.

Why is VPN useful to hackers?

a) Virtual private networks hide the network address of your system and link it with another so that you will have anonymity.

b) Virtual private networks can help you get past through a lot of firewalls and intrusion detection systems that are built-in industries.

c) Virtual private networks not only help you hide your information but also helps to make sure that all of your network information that is being transmitted is encrypted. Not sure how this works? Let us give an example.

Imagine that you are using a public WiFi network where a lot of other users are connected. Not all WiFi dongles have WPA2 advanced security configuration so your network packets that consist of a lot of sensitive information including your passwords, credit cards can be easily compromised by someone who is on the same network and using wireless networks sniffing tools like air crack.

Due to these complications, virtual private networks are recommended to be used when you are not an in-home network. Now in the next section, we will look at how to install any VPN in any Linux systems.

Installation of VPN in Kali Linux

1) First of all, install the tools or certificates that need to be used to install the VPN. Normally a CA certificate should be downloaded and uploaded to the system. This certificate consists of a hash code that will let us connect to the server with an anonymous linkage.

2) In the next step, we need to enter the network manager to start the VPN connection. When you started a new VPN connection enter the gateway details that are provided by the VPN provider.

3) In the next step, you can give the authentication details that briefly consist of your credentials in the VPN service provider application or website.

With this, we have completed the starting of a virtual private network. There are a lot of good VPN service providers like open VPN, Cisco VPN, hide my ass. Choose the one which gives a huge number of servers and security. VPN is a must of every hacker nowadays due to increased surveillance from governments all around the world. You can also use a VPN for peer to peer network communications such as downloading torrent files and seeding them. That's it in the next section we will learn about changing the physical address of the system that is MAC address.

How to change the MAC address using Linux?

First of all, we need to know about system addresses. Every system that is ever manufactured has a serial number to it called a MAC address. Every system has a unique address by default, unlike the network address that often interchanges between the systems that are connected.

Usually, during network surveillance, IP addresses will help the attacker find the location of the system which may be easily spoofed by Virtual private networks and almost every company uses a VPN for this purpose.

However, a lot of people don't change their system address due to various reasons. First of all, the warranty will become void and any necessary help will be not provided by most of the industry providers. For this reason, a lot of users will not change it.

However, hackers for whom anonymity is their important consideration should be well aware of the procedure that can make spoof a system address. Below we will describe the method in detail.

What is spoofing?

Spoofing is just faking the receiver that the address is different. This on a whole will not change the system specifications but will show some random or manually inputted information to the attacker or forensic specialists.

Spoofing a MAC address

a) First of all, before trying to spoof the address you need to know what your MAC address is. It differs from system to system. You can even find it in the warranty booklet. But as we are geeks, we will use the Linux command shell to find the MAC address of the system we are working on. Follow along!

b) First of all, enter into the Linux command shell and inter the ifconfig tool. After successfully starting the ifconfig module enter the below command

ifconfig ma c

This will display an output that shows you the MAC address of your present system. It will also give the manufacturer details along with the network packet structure it uses.

c) Now you need to install a tool called Mac changer that can spoof the system address. Install the Macchanger using the following dependency injection command

wget macchanger

d) After installing the Mac changer, you are good to go to use the commands that will change the system address both randomly and manually. We will discuss both of these functionalities in detail below.

e) Random MAC address just changes your MAC address into a random number that is per listed in the code.

f) Custom MAC address will, however, make you change to ur desired MAC address using the following command.

root @ host : change MAC to as:23:1w:2w:3e

Whenever you use the changed MAC address there is very little chance of being identified or traced. By this, we have explained all the topics that can help you deal with maintaining your anonymity while hacking. Before ending this chapter, we will have a brief explanation about proxies for a better understanding of this topic.

What are proxies?

Proxies just act like a middle man between the client and the server. And moreover, proxies can be used to send data through the modem to an anonymous server. Proxies are available free of cost on the internet, but they are of no use because of their structure and configuration?

What proxies should hackers use?

Hackers should get acquainted with SOCK5 proxies which can be used for a limited period. They are not available for free but can be purchased in proxy markets or you can even make one server. SOCK5 proxies are secure and even have a location configuration such that there will be less blacklisting of the proxies.

There are also proxies called upstream proxies that can be used in brute-forcing web application software like the burp suite.

With this, we have completed a brief introduction to everything that relates to the security of the hacker. In the next chapter, we will discuss some of the famous Linux tools in detail. Let us go!

Chapter 9:
Advanced Kali Linux Hacking Tools

This chapter is a final implementation of all the concepts we have learned in this book. There are a lot of hacking tools available now. Linux Distro Kali Linux provides approximately 350 tools from various categories. We will in this chapter discuss some of the famous hacking tools that are used for web hacking, network hacking, and password cracking. Remember that hacking tools are just an easy interface that will let us complete our work fastly and efficiently. Good hackers don't always rely on tools but create their tools to exploit the system as soon as can. However, hacking tools are better options for security testing and other tasks like fingerprinting or brute-forcing. We will now discuss some of the hacking tools in detail. Let's get started!

Burp Suite

In today's world web applications are the most attacked ones by hackers. They are somewhat easy to break into when compared to network systems and can be easily manipulated to cash out easy money or sensitive information.

Hackers use brute force tools like Hydra that are available in Linux to brute force (that is to send a lot of requests automatically) login pages. Security researchers should test web applications in depth to clear any vulnerabilities that are present.

To make this vulnerability testing process smooth and easy port swigger has created a tool named as burp suite that has been white hat hackers favorite since then. In this section, we will discuss the components of the burp suite in detail. Let us start!

Note: Burp Suite is a tool that can be used by hackers to manipulate pages. So always take the permission of the website owners that you are trying to experiment on. Otherwise, you can use sample test websites that are available either online or as Linux iso.

How does the burp suite work?

Burp suite uses a proxy mechanism to send requests as a middle man unlike acting as a client. This process will help the software to analyze every protocol it uses and every request it sends and the subsequent response it receives. By using this information burp suite can be used to send repeated or manipulated requests that can help the users to understand the process that is going on.

In this chapter, we will discuss in more of a practical way about the burp suite in detail. We will look at a scenario to understand the tool we are learning.

Practical scenario:

We have a login page for our website www.amazonkali.com that uses https protocol. Our novice hackers' task is to log in to the website using the payloads that are present. Let us do it!

Try to do this assignment by yourself for the first time while using the tool and if you are unable to get the task done follow the below section to understand the process that goes on.

Solution or strategy for the task:

First of all, after the successful installation of the burp suite, you need to enter the CA certificate in the browser options to make burp suite work on https websites. This is necessary to be done because https use an encrypted protocol that can be only read by the proxy interpretation tools when a CA certificate is installed. For the installation of the certificate, you need to start a proxy first.

Follow along with the instructions briefly:

a) Open the burp suite proxy tab and enter the proxy 127.0.0.1 as an interception address. After entering the details, you need a select a browser preferably Mozilla Firefox because chrome spends a lot of computer usage and being a hacker coordination of processes is an important thing for smoother results.

b) In the Mozilla Firefox, proxy settings enter the same interception address and start the proxy server using the intercept on/off button. With this, every request or response will first go through the burp suite proxy server and will get recorded.

With this, we have set up the burp suite with the browser and we are now all set to exploit the www.amazonkali.com website. Follow along for the procedure.

Hacking a login page using burp suite:

1) In the first step start the intercepting proxy and enter the URL address in your browser. When you press the enter button you will see a request pop up in the burp suite proxy tab. You can look at the GET request and understand that the browser is requesting a burp suite to accept this request and send it to the original server. When this is being done our burp, console stores the request and response information.

2) A website consists of a lot of subdomains and this may become a problem when we are trying to intercept using a proxy. A lot of unnecessary requests will be processed and will make the console tab chaotic. For this reason, the burp suite gives a scoping tool that will let us select the main domain for testing purposes. All the out of scope sub-domains will be filtered and will not be sent through the proxy service.

3) Now accept all the requests that have been sent by the browser. Now go and look back at the browser and our homepage will be displayed. This homepage has a login form and we need to brute force this with payloads using brute force hoping for a successful cracking.

4) Look at the requests that have been monitored and you can observe that all are GET requests which are used by the client to let the server know that the system is asking information. We will now use intruder a tool in the burp suite to brute force payloads to the login form.

What is an intruder?

Intruder in common words is an anonymous person that enters the house without any permission or for theft. This is the exact way how an intruder works. When we use this tool burp suite sends requests fastly and anonymously so that the system won't detect it as malicious.

Step by step procedure

1) Now enter some fake data in both username and password fields and send it through the proxy server. With this procedure, all the data will be sent and the request will be of POST category. The post is an HTML request category where the arguments are sent along with the request.

2) Now select all the post requests and send them to the intruder tab. In the intruder tab, you can select the entered username and password arguments using a dollar sign. After the arguments becoming highlighted user can select the payload procedure type. There are a lot of procedures like a single hammer, cluster bomb, and pitcher fork.

We will explain these three terms in detail here:

a) single hamme r

Here only one argument is selected and is brute-forced using the payload. By using the single hammer one can easily

b) cluster bomb

Cluster bomb highlights two arguments in a way that the arguments are sent.

c) pitcher fork

Pitcher fork also highlights two arguments but uses the payload in a way that the arguments are given in a co-linear way.

After selecting the type of attack, we can go into the next interface and select the payload that we need to send into the login page. Before knowing about different types of payloads we need to first of all what a payload means.

What is a payload?

The payload is a systematic collection of commands or syntactic statements that can be used to exploit or crash the system while brute-forcing.

Payloads present in the burp suite

a) SQL injection payloads

Burp suite consists of SQL injection payloads that can easily crash an injected database to enter into the system.

b) XSS payloads

XSS is one of the most frequent web application vulnerabilities and can be easily found out using the XSS commands present in the burp suite.

c) custom payloads

With this option, you can create payloads that are random with the alphabets and numbers. With this payload, you can create a lot of complex crypto passwords that can be used to crack advanced systems.

d) Runtime payload

Usually, payloads are generated but if there are a lot of payloads that need to be inserted you can use this payload to insert the list in the runtime memory for faster execution.

e) recursive payloads

Recursion is a system that sends the payloads in a varied significant signature process. Although being insignificant of nature these payloads are used to effect systems like cloud flare to get access.

After entering the required payloads enter into the next section to start the brute-forcing process.

In the next interface select the numbers of threads and the speed on which the payloads should be sent. Also, you can insert upstream proxies that will change in random so that even if the intrusion detection systems block the access you can access using other proxies. You can even use the tor system proxies as upstream proxies for additional security and to avoid detection.

Now click the start button and you will get an interface that will let you analyze the hacking process. If the login was successful you will get 200 success information in the status bar. If the login was not successful you will get a 404 or 303 error. In this way, you can easily hack a login web page with a burp suite.

In the next section, we will discuss Metasploit one of the most famous exploit binding software that can help us to spoof any system.

Metasploit

Metasploit is one of the most important hacking tools due to its huge number of features that can be used on a target. The best thing about Metasploit is although being a tool that offers a lot of features and it is available as open-source. It matters because the burp suite which we discussed before has a premium license and restricts some of its features like automatic scanning for free users. Just like burp suite Metasploit also offers a professional license.

The major difference between both versions is that in the free version you can only use 32 hosts at a time. This may be quite difficult for hackers trying to exploit large systems at once. So choose the version according to your preferences.

Metasploit is pre-installed in the Kali Linux. If you want to install Metasploit in other Linux versions use the following command

wget Metasploit

Metasploit also gives web interface access which can help us to access all the hosts we are using. Create an account and manage everything about the exploits here.

Practical scenario: Use Metasploit to make an exploit app that consists of malicious code which can take control of an android phone and can read its files, contacts, and messages and send them to a web server of yours.

Don't forget to try it out by yourself before looking at the solution that we describe here.

The process to create an exploitable app

a) For this practical exercise, it's better to use a virtual machine to leave no traces and an android emulator to check the app before sending it into the victim via a mail or by a person.

Why only android app can be made?

Usually, android is an open-source Linux system and is easy to exploit using tools like Metasploit. Other famous mobile operating systems like iOS use package managers with extensions IPA unlike app of android. Although there is a module splitter that can split the IPA files as of now there are no remote execution tools for Apple operating systems. So if you are trying to trick a user with Mac OS you need to find other ways.

However, if your victim is an android user then you can follow the below instructions to get the exploit into his device:

b) First of all, start the Metasploit in the device using the Metasploit command msfconsole

c) when the Linux shell shows the Metasploit interface select the payloads options. As we discussed earlier payloads are already proven bugs or vulnerabilities that can be achieved on a target running on a particular version of the software.

d) Here our target machine is android that is a Linux kernel machine. From the payloads shell search for msfvenom payload using the following command:

root @ hostname : msfvenom payload select

e) It gives five arguments that need to be filled out with information. Here we will discuss those five parameters in detail with commands.

a) -p

This needs to be used whenever you are trying to create an exploit using Metasploit. Here our payload is msfvenom

b) LHOST

This is the argument that describes our input network address. We have already learned about finding the IP address of our system using the ifconfig tool. The IP address is essential because we need to make a regular connection between the host and the victim so that the data can be transferred.

c) LPORT

Just like the previous one, this describes the port that we are willing to offer to this Metasploit program so that the victim app can send us data and other sensitive information.

d) R

This is where the apk format should be selected using the options. We are dealing with raw format information so this should be mentioned. If you are dealing with system software's execution files should be selected.

e) Location

This argument helps us to select the apk that we are referring to. You can simply give the location so that the Metasploit can start making it as an exploit. But before this process, we need to make some certificate installations so that everything runs in perfect. We will learn about this process in detail in this section.

Why certificates should be signed for android?

Installing signed applications is a mandatory thing in iOS however android doesn't have that restriction. But from the latest versions of android google made things difficult for hackers.

In the past with the help of remote execution hackers used to install trojans and worms with malicious content with a click. However, nowadays it has become a lot difficult because the user needs to grant the permissions manually. For this reason, you need to even polish your social engineering skills before trying to send the exploit to the victim. Make them believe with your words that this is a necessary application that needs to be installed. That's what all hackers do to manipulates things for their exploitation.

We have a wide variety of signing tools like jar signer in the Metasploit interface. Select any one of them and use the following command

root @ examplelinux : msfvenom signer -ssh 23.2.2.1

The signer tool has the following attributes which will be explained in the next section in detail:

a) Type of certificate

There are a lot of certificate signs that need to be reviewed. You can use either an SHA way or by RSA way.

b) -verify

This command will make the tool to verify the app with the certification that the user has selected.

Now after verification, you need to use aligning tools that can mix up the exploit that you have developed with the apk tool.

c) align

Aligning is a process of inserting the exploit into the application. There are a lot of exploits that are available in the Metasploit database. Or you can even create an own shell script that can send back information to our server. For the visual demonstration of this topic we will explain about a shell script that performs the following functions:

a) The shell script should collect all the user contacts that are present on the phone.

b) The shell script should identify any new messages that are received and should send them to the Metasploit server.

Few might have got a doubt about how the Metasploit server works. It consists of a URL that is inserted into the exploit and we need to enter the same URL into the browser in that network. In this way, we can access all the information that is being sent to the server.

d) Packing

After aligning the exploit into an app, you need to repackage it so that the apk looks perfectly normal. There is maybe a small marginal change in the size of the apk. To get undetected by the antiviruses you may use additional security options that can spoof the phone security.

You can use the following command to package the apk and exploit:

root @ example : pack location seems.apk

After packaging the app, you should find a smart social engineering technique to send it to the victim's system. You can use an email with a rar file to send it to the phone. And when the victim successfully installs the application on his phone the app starts running in the background and will send all of the required data to the Metasploit server.

That's it about the exploit and its implementation using the Metasploit interface console. In the next chapter, we will give a brief introduction about the network sniffing tool known as wire shark and end this chapter.

Wireless Network sniffing tools

In a whole lot of kali Linux tools that are available, this stands among the most popular tools because of the huge expansion of wireless networks in the everyday world. From Bluetooth devices to wireless echo devices there are a lot of wireless devices that can be easily sniffed if they are connected to an unsecured wireless network.

What is sniffing?

Sniffing, in general, is a term that is defined for peeking into other stuff. In technical terms, sniffing means to look at network packets that are coming from other devices using tools like wire shark and air crack-ng. We will discuss both of these two tools in detail in this section

a) Wireshark

Wireshark is a network sniffing tool that tracks every packet that the network is dealing with. After starting the sniffer tool you need to wait at least 24 hours so that the sniffer catches a sufficient number of packets for analysis. During analysis, one can easily find all the sensitive information like passwords and credit card numbers. There is also a chance of using sniffing tools to hack unencrypted files and emails that are being sent.

This is the reason why hackers should use encrypted mail services and virtual private networks for better security.

b) aircrack ng

Aircrack ng is another network sniffer tool that is extensively used to crack WiFi passwords. Usually, wpa2 WiFi routers are considered as the most secure network routers, unlike WPS routers which leave a bug to easily hack their passwords. This aircrack ng uses this vulnerability to boot scan the dictionary attacks and connect to the wireless network. Aircrack is one of the most popular wireless network programs that are available in the market right now.

By this, we have completed a detailed tour of some of the most important kali Linux tools with an overview of practical applications that can be done using these tools. We hope that with this chapter you have gained a lot of meaningful information.

This is the end of the book and I end this book with a clear explanation of what a hacker should try to be. A hacker learns skills and applies them with utmost hard work to crack into systems. Cracking doesn't mean to be exploiting and using them for their mischief purposes. Cracking means checking whether the walls are built strong or not. That's it that is what a hacker needs to remember all the time. All the best to our adventures of hacking!

Conclusion

Thank you for making it through to the end of Hacking with Linux, let's hope it was informative and able to provide you with all of the tools you need to achieve your goals whatever they may be.

The next step is to use these concepts in real-world and exploit environments or protect them with goodwill. All the best!

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