ANDY VICKLER

LINUX

LINUX SECURITY AND ADMINISTRATION

ANDY W

LIN

Linux

Linux Security and Administration

Table of Contents

Introduction

If you are new to using Linux, it will be difficult for you to find the right information online. This book has all the information you need to help you install the operating system and show you how you can use it either on your system or a virtual system. The book also has information about how you need to configure user access and other information to maintain the network and server's security on the Linux system. You do not have to know anything about Linux before you use it since the information in this book will guide you every step of the way!

The book introduces the idea of using Linux on a virtual system and provides information on the different distributions of Linux. You can use this information to determine which distros work best for you and download that onto your system. You will also learn about the importance of a root account and the other accounts on the server. The book also provides information about the methods used to control access to users. You will learn how you can grant and revoke privileges to users to help you protect the data.

The book covers how you can secure the information, files, and folders in the operating system. You will be introduced to a list of tools you can use to secure the data on your systems and how you can encrypt and decrypt information using these tools. You can also use passwords to encrypt and decrypt the files and folders on the server and network if you need to.

Since Linux is an operating system, and the data is stored on a server or network, you need to test the network and server's strength. This book will shed light on the method you can use to identify any vulnerability in the system. It will also let you know how you can use scanning to identify the holes in your system. You can use the information in this book to determine how to overcome those vulnerabilities.

Thank you for purchasing the book. I hope you learn more about Linux and how you can protect the information in your files and folders.

Chapter One: Using Linux on Virtual Machines

Have you wanted to use Linux but did not want to use it on your system? Your system may have trouble if you use dual-booting, and the best thing to do is to use Linux on a virtual machine. It is easy for you to use Linux on a virtual machine if you use Windows. The procedure is straightforward. In this chapter, we will look at installing and using Linux on a virtual machine, a VMware Workstation specifically.

If you want to use a virtual machine, you need to find a PC, which allows you to use virtualization. You may have tried to install Linux on your system using a CD, but you may not be sure about dual booting. You should install the Linux operating system on your PC but using a virtual machine.

Virtual machines are environments that replicate the conditions of the hardware on your device. The environment mirrors everything in your personal computer and is limited only by the system's different components. This means you cannot expect to have a four-core CPU on a processor which only has two cores. You can achieve virtualization on multiple systems, and the result of this will be superior on computers that have CPUs that support visualization.

You can use different virtual machines to install the Linux operating system on your computer. VMware is one of the leading manufacturers of virtual machines and applications. In this chapter, we will look at how you can install Linux OS in Windows using a workstation player designed by VMware.

Installing a Workstation Player

If you want the workstation player, you need to download the latest version from the VMware website. They constantly upgrade their workstation player application and tool. For this example, we will use the VMware workstation 15 player, and this file is 150 MB in size. The latest versions can be heavier, so make sure you have good Internet connectivity.

These workstation players are available for home, non-commercial, and personal use and are free. Non-profit organizations and students can use this version since they do not have to shell out any money on installing the operating system. A VMware workstation player performs all the functions a standard virtual machine must. You can also use VMware products since each product offers a wide range of visualization solutions that you can use for any business. If you want to learn more about their products, you can read about them on their website. After you download the VMware workstation player, click on the installer and follow the installation wizard steps to set up your virtual workstation. It is recommended that you download the Enhanced Keyboard Driver during the installation since you may not need it now but will need it later. Complete the installation and reboot your system when the wizard prompts you.

Choose the Correct Distro

You should read about the different Linux distributions available to you and choose the one that works best for you. Some Linux distributions work best on virtual machines, while others cannot work on them. All 64-bit and 32-bit versions of Linux work well on virtual machines. You cannot run Linux distros, such as Raspberry Pi and other ARM architecture Linux distributions on virtual machines. If you want to use an ARM Linux environment on your Windows machine, you should try QEMU. If you do not know which distro you need to choose, choose any from the list below:

Linux Distros

Since there are many options available, you may find it hard to choose the right Linux distro for your system. How do you know that is the best one you should use for your system? What if you want to game using Linux distros? Do you want to use a pretty distro that uses the same structure as macOS?

In this section, we will look at the different Linux distros lists available for you. These distros have been used actively by various individuals over the last few years. It is best to download a Linux distro that you

can use safely on your system. You should also check if the distro you use is updated regularly using security patches.

Business Linux Distros

Red Hat Enterprise Linux

This distro is like Fedora, but it is used commercially. This distro was designed for enterprise customers. You can use any of the different addons and variants. If you want to be an administrator, you need to be certified.

SUSE Linux Enterprise

This Linux distro version is designed for an enterprise and can be used by businesses. It is for this reason this variant is easy for one to use with different office programs. You can run this distro on various devices, and it can be used even on critical systems. Many versions of this distro are also available on the Linux website.

Gaming Linux Distros

SparkyLinux Game Over Edition

SparkyLinux has various versions, but this version which focuses on gaming, is the most used. This gaming version comes with various pre-installed games, an LXDE desktop, PlayOnLinux, Steam, and Wine. There are numerous premium and free games available on this distro which you can use easily.

SteamOS

Many gamers have started using Linux as their operating system since it comes with a Steam client. It is easier to install the SteamOS version of Linux if you are a gamer. One of the best Linux distros you can use for gaming is SteamOS, and this is optimized to perform well in any game and comes with in-built sound drivers, proprietary graphics, and a Steam client.

General-Purpose Linux Distros

Ubuntu

This is a Debian-based operating system, and it uses GNOME as the desktop environment. You cannot update this environment since it is used as the default. This Linux distro has regular patch updates, and it improves with every new release. The latest versions of this OS are designed for hybrids, desktops, and laptops. Therefore, if you are moving from Windows to macOS, you need to use the Ubuntu OS.

openSUSE

This distro is a general OS built by Linux for various projects, but it is primarily used for openSUSE projects. This distro is used both by beginners and by experienced Linux users. This distro comes with an administration program called YaST which controls and monitors the installation, package management, and other functions.

Fedora

This Linux distro was developed by IBM-owned Red Hat and uses a default GNOME desktop environment. You can switch to LXDE, XForms Common Environment (Xfce), Cinnamon, KDE and MATE, and other desktop environments. Some variations of Fedora, like Fedora spins, can be used by people who have specific requirements.

Debian

Debian is an old Linux distro and is the best version compared to other Linux distros. This also comes with a default GNOME desktop environment, but it can also be used in the FreeBSD kernel. Developers are working on making this compatible with other kernels like the Hurd. Some Linux distros, such as Raspbian and Ubuntu, are based on Debian.

Slackware Linux

This is another distro that has been built specifically for simplicity and security. It is a distro that is Unix-like and is used for server and file management since it has web, FTP, and email servers available for use. If you have never tried managing a server or using a Unix server, you can use this server as a live disc. You can also use this as a virtual machine to learn how to use Linux distros better.

Mageia

This Linux distro was developed by a non-profit fork community and had various features that a major desktop environment should have. The default desktop used by this distro is GNOME and KDE.

SparkyLinux

This version of Linux evolved when the developers were testing the Debian version of Linux. This edition of Linux has a customized lightweight LXDE desktop. You can also use this with other customized desktops.

Gentoo Linux

You can use this distros version on any desktop. It is compatible with multiple requirements, and its performance and versatility make it one of the best versions of Linux OS. Gentoo Linux has Portage, that is an advanced package management system. Since Gentoo can be used on different systems, you gain complete access to your system and control it the way you need to. It does, however, become a problem for a newcomer.

CentOS

Community Enterprise Operating System or CentOS is a distro built by the Red Hat community and is a rebuild of the Red Hat Linux Enterprise. This is a free version of the distro. If you do not want to

work with different Linux distros, you can use the Red Hat enterprise at work and the CentOS at home.

Lightweight Linux Distros

Linux lite

The Linux lite distros are based on the Ubuntu LTS releases and have a very minimal footprint. It uses a simple and clean Xfce desktop. This distro also uses a simple Windows-style Start menu which makes any Windows user feel at home. This distro has a small resource footprint, which means you can use it on a PC with 512 MB RAM and 700 MHz CPU. It is for this reason this version is called light. You can use this version on an old computer or on your laptop if you want to maximize battery life.

Lubuntu

This is another lightweight version of Linux based on Ubuntu, and it is perfect to use on laptops or desktops. It uses a lightweight desktop environment and has in-built lightweight applications which are designed for speed and energy-efficiency. You can use this OS on old mobile devices, computers, and netbooks. It does not need high-speed RAM and has few system requirements. If you want to purchase the best operating system to maintain your device's battery life, you should definitely pick this.

Xubuntu

This derivative of the Ubuntu distros uses an Xfce desktop which means it is lightweight and elegant. You can use it on different notebooks and laptops. If you have devices with low specs, you can use this distro on them. Since it is light, it does not need many system resources. It is for this reason you can use it on old devices, as well.

Puppy Linux

Puppy Linux uses a small distribution that you can run using RAM. This means this version is great for older laptops or computers, and you can use this distro even on computers or laptops without hard drives. Most companies and individuals use this tool to remove malware.

Manjaro Linux

This Linux distro is an easy-to-use, fast and lightweight distribution which mirrors the Arch Linux distro. This version uses the benefits of Arch Linux and is more accessible and user-friendly. It is for this reason a beginner can also work with Manjaro Linux. The default desktop used is Xfce, but you can switch to other options depending on what you are comfortable using.

Arch Linux

This version of Linux is a distribution developed with user experience in mind. The Arch Linux distribution is aimed at keeping things simple and easy. It is updated regularly through patches. Arch has Pacman, a custom-made package manager used in Linux, making it easy for users to build, share and modify packages. This distro is recommended if you are a beginner, since it requires some hands-on experience with the operating system.

NuTyX

Do you want to customize the system you currently use? If yes, you should use this distro. NuTyX allows you to ship bloatware-free and barebones across the OS. You can also customize the OS using the concept of collection. You have a choice for everything you want to use. For example, you may find a selection of window managers or desktop environments, and you can choose to use the one that works best for you. Using these choices, you can develop a user-determined operating system that has multiple possibilities. You can use this as a focused home theater or a versatile desktop.

Bodhi

This is an Ubuntu-based distribution operating system, and it comes with a beautiful and lightweight Enlightenment desktop. Bodhi can be customized, and it comes with applications and themes. You can use these to expand on the basic operating system you may have downloaded.

Multimedia Linux Distros

Fedora Design Suite

You can save time on installing artistic applications and tools by using Fedora, a spin-off of the Fedora design suite. This design suite comes with GIMP and Inkscape. It also comes with different applications and tools which can be used for art and illustration. This is a distro focused on DTP.

Ubuntu Studio

The Ubuntu studio was released in 2007 and is the default choice used by Linux users. If you are creative, you can use this distro to work on your talents. This distro also comes with an Xfce desktop environment and has low kernel latency. Therefore, everything about this distro is geared towards the production of media. You can use different distros for this as well, but Ubuntu studio is the best for photographers, music producers, designers, and other users.

Linux Distros for Beginners

Endless OS

If you have just started using Linux, you may want to keep everything simple. The best Linux distros to use for this is the endless OS. Families often use this since it comes with multiple applications. It is best to use this OS if you do not have an Internet connection at home. You can also use this if you are unsure about which application you need to use on your Linux OS. This is not an ideal approach for you if you are an experienced user. If you are new

to using open-source operating systems, you can use this OS to obtain more information about working with Linux.

Linux Mint

Linux Mint is a modern and elegant distro that is powerful and easy to use. This distro is based on Ubuntu and is reliable. It was developed with the idea of a software manager in mind. This distro is one of the top-rated Linux operating systems since 2011. Many macOS and Windows refugees choose to use this as their new virtual desktop. Linux Mint also comes with various desktop options. You can use the Cinnamon desktop, that is the default for Linux Mint. Alternatively, you can use KDE, Xfce, or MATE. You can also use a Debian and Linux Mint combination if you are a beginner.

Deepin

Deepin is another Ubuntu-based distro, and it comes with a stylish DDE or Deepin Desktop Environment. This distro is great for new Linux users. It is simple and intuitive and features a variety of system settings panel displays. Deepin is inspired and developed based on macOS. This distro also has a software center that is easy to use. It has tools that are far superior when compared to other Linux distros. For this reason, Deepin is a great operating system to use if you are switching from macOS.

Pop!_OS

This is another Ubuntu-based operating system that was manufactured based on Linux hardware manufacturer system 76. It uses a GNOME desktop as the default environment and has a theme that you can change. The colors vary depending on the brand identity of System 76. This distro also comes with its own application and installation browser, making it easier for you to install the required Linux applications. Some applications may not match the theme, but this is an easy-to-use distro for a beginner.

Zorin OS

If you are new to Linux, you can use Zorin OS since it is designed specifically for beginners. This distro can ease the transition from using other operating systems to Linux. This operating system is based on Ubuntu and has several applications, which are like Windows applications. This makes it easy for you to use Zorin OS since you know how to work with the applications. You can also configure the desktop on the Zorin OS distro to resemble Linux, Windows, or macOS.

Elementary OS

Another Ubuntu-based distro is the Elementary OS which has differentiated it from other distros greatly since 2013. One of the most common features of this distro is the use of simple and beautiful default applications and tools. These applications also maintain the operating system's aesthetic appeal, such as using the Epiphany web browser and Mail for email.

Elementary OS also has different features you can use to improve the function of various operating system functions. You can use different productivity apps, as well. If you want to change the desktop layout so it matches that of a macOS, you can use the Elementary OS.

RoboLinux

It is difficult for you to switch from Windows to Linux and vice versa because not all applications and tools used are compatible. Various distros in Linux have found a workaround for this issue. The RoboLinux distro, unlike other distros, has a better or easy solution. It allows you to set up a Windows virtual machine easily on your device. You can set up Windows XP and later versions easily on RoboLinux. This prevents dual booting. You can access all your Windows applications anytime you need to.

Kubuntu

There are different variations or derivatives developed on the Ubuntu operating system. Another popular Ubuntu option is Kubuntu, and this distro uses a KDE desktop as the default environment. If you look at the system beneath the environment, it is the same as Ubuntu and has the same releases as Ubuntu.

Raspberry Pi Linux Distros

Raspberry Pi is an extremely common and popular Linux machine, but the other distros mentioned in this list will not work since Pi uses an ARM processor instead of AMD or Intel 32-bit or 64-bit CPUs. It is for this reason the Raspberry Pi Foundation worked on developing specialist distros. Some of them are Pi-friendly versions of existing Linux operating systems, and these are covered in the sections below.

Raspbian Stretch

For Raspbian Pi, the default operating system used is the Debian-based Raspbian Stretch. The Raspberry Pi Foundation developed the latter. Raspbian Stretch is an ARM Linux distro and has multiple programming tools and applications. A beginner can use these tools to learn more about coding on Linux. Raspbian also has LXDE-based PIXEL environments, making this distro the best option, especially if you are using Raspberry Pi.

Kano OS

Kano OS is like Raspbian, but it focuses more on coding. The operating system is aimed at helping children learn more about how to code. The system comes with an interactive user interface, and this gives your children the tools he needs to code without too much fuss.

DietPi

Do you work on projects where you need to use barebones operating systems? If yes, you should choose DietPi. This is a very

light Debian-based operating system and can be used on all models of Raspberry Pi. You can also use it on single-board computers if you have one. Raspbian Stretch Lite is an option that most Pi users choose, especially if they use applications with a small footprint from the selected operating system. The difference between DietPi and other Raspbian Pi operating systems is the amount of space you need to run the OS on your system. DietPi only needs 1 GB storage, while others need 2 GB or more.

Linux Distros for Security and Recovery

Qubes 3.2

I am sure you know Linux is a very secure operating system, and it is better than Windows, too. The most secure Linux distros are Qubes. The current version is 3.2, and this is a better upgrade when compared to the earlier versions of Qubes. Edward Snowden stated that Qubes is a reasonably secure operating system, and this testimonial is enough for you to use this distro in your virtual machine. If you are a security-conscious user, you need to choose Qubes. This distro is known for freedom, security, and various privacy features. It also comes with sandboxes that allow you to separate the application and hardware when you perform different functions.

Kali Linux

Kali Linux was earlier known as BackTrack. It is a penetration testing Linux distro that is used often by the online security community. This is a Debian-based distro which makes it easier for you to perform various forensic tasks.

Parted Magic

This Linux distro is used to manage disk space on your system. You can partition the hard disk and copy the information across different servers as the OS's primary applications. Parted Magic makes it easier for you to secure erasing and recovery of data.

GParted

GParted is a single-purpose distribution operating system that makes it easier for you to partition hard drives. You can do this easily using a graphical interface. A Linux user is familiar with using standard versions of various distribution operating systems. This is a dedicated and standalone operating system, but it can also be run using a CD. If you want to manage the disk space on your system without booting your computer or the operating system, you can use GParted.

Tails

Tails is a Linux distribution operating system that revolves wholly around the idea of security and privacy. This is an operating system that you can use through a USB stick, SD card, or DVD. You can use this operating system anywhere without worrying about leaving a trace. You route everything you perform on the system through a different router (called the Onion Router or TOR) to maintain anonymity. You can also use different cryptographic tools to protect all the information you send or receive from prying eyes.

Bruce Schneier, a famous American cryptographer, loves using Tails, and this is a big endorsement.

You are looking for a new way to use a secure and portable tool. But how do you know that is the best Linux distro for you to use? There are so many operating systems you can choose from, but you need to choose the one that does what you want it to. Since there are Linux distros for different purposes, you can choose which works best for you. If you want to carry a distro with you on a USB stick, you need to round up the best portable Linux distros.

Setting Up the Virtual Machine

While the ISO for your Linux distros is downloading, you should spend time configuring your virtual machine settings. To do this, you

need to launch the workstation player. Follow the steps given below to create a virtual machine:

Step One : When the installation wizard opens, select the option to create new virtual machines
Step Two : Choose the default option, that is the Installer disc image file (ISO). It is best to do it this way to prevent anything wrong from happening during the installation
Step Three : If you cannot find the ISO file, look for it using the browse option
Step Four : Select 'guest OS' and move to the next step of your installation
Step Five : You need to select Linux as the type of guest operating system
Step Six : Select the version of the OS from the list
Step Seven : Click on the next option to move to the next step, and key in the name of the virtual machine
Step Eight : Confirm the location where the OS files need to be saved and let the installation wizard complete the process

Once the operating system is selected, and the installation wizard is configured, you need to build your virtual machine. Follow the steps given below to do this:

Step One : Choose the maximum disk size from the option to select the specific disk capacity. You can stick to the default if you want to
Step Two : You can also choose to split the virtual disk into multiple segments. It is recommended to do this since you can move the virtual machine easily onto your new system
Step Three : Once you are happy with the details, you should confirm them and move onto the next step
Step Four : Click finish to install your virtual machine

The Linux virtual machine will now be a part of your VMware Workstation player.

Customizing Virtual Hardware

When you download the virtual machine, you can customize it before you install Linux. You may need to do this for the following reasons:

1. The Linux distros you are using may need a specific type of OS
2. There may be some components missing in your operating system

You can fix this easily by accessing the settings on your virtual machine. This is where you can work with the virtual machine's hardware and tweak the settings in ways that are beyond the HDD. You can make changes to the network adapter configuration, memory, processors, and more.

You need to look at the processor screen before anything else. You will find a reference to the virtualization engine. This will work automatically when you install the virtual machine in your system. If you want to troubleshoot your processor when there are issues, you need to set the AMD-V or Intel VT-x.

The memory screen on your virtual desktop settings will help you address memory performances. Your virtual machine will have the details of the RAM you need to use. It will tell you about the settings you need to maintain on your physical and virtual machines. It is recommended for you to stick to these settings. If you reduce the memory size below or higher than the recommended size, you may either create a problem or slow your system. This will mean your system cannot function the way it should.

You then need to spend time on the display settings. You can stick to the default settings if you want, but you can play around with the 3D toggle acceleration if there is an issue. You can set up different monitors differently depending on what you would like to use them for. It is important to note that some modes you set up will clash with the different desktops you use.

If you are happy with the changes, confirm them and click on the play button to start your virtual machine.

Download and Install Tools

Now that you have downloaded your virtual machine, you should reboot it. You will be asked to look at different VMware tools you can download and install at this stage. All you need to do is to agree to what the wizard says and let the tools install on your virtual machine. These tools will improve your virtual machine's performance, enabling you to share folders between the guest and host machines, the virtual and physical machine, respectively.

Installing Linux on VMware

When you launch your virtual machine, the ISO boots directly into your live environment, this version of Linux is only temporary and will not reside in your system memory or boot media when you turn off the device. If you want to use the environment the way it should be used, you should use the virtual machine's install option.

At this point, the installation wizard will continue to install the operating system on the actual machine. You need to follow the installation wizard steps, create an account, and set the other options when you are prompted to do this. When the installation is complete, you can use the Linux virtual machine and use the guest operating system. The process is this simple.

Running Linux on a Virtual Machine

Now that you have the virtual machine launched on your system, you can run the distros you want to use on the virtual machine using the Play button on your system. If you are looking for software to install, you can choose the preinstalled applications which come as part of your Linux distros. You can also choose to download different apps if you want to.

If you want to access the Linux terminal through your system, you can do this without a VMware workstation.

Installing a Linux Distro on a Windows Virtual Machine

The easiest way to access Linux on your system is through a virtual machine if you use a Windows operating system. The workstation player from VMware has the best tools to help you do this. You can install Linux easily on your VMware workstation. Let us quickly go through the steps again:

Step One : You need to download the VMware workstation player. It is recommended that you download the latest version
Step Two : Install the workstation player and reboot windows
Step Three : Configure and create the virtual machine
Step Four : Install the Linux distros of your choice on your machine
Step Five : Reboot the virtual machine and use the operating system

The process is this simple, and you do not have to stick to one operating system alone. You can choose from the list of Linux distros mentioned above, and you can install all of them on your workstation player.

Chapter Two: Securing User Accounts on Linux

Don't Login Using a Root Account

The root user on your Linux operating system is like the administrator user on Windows. There are situations where you may want to log in to the administrator account on Windows. You should never log in to Linux using the root account or user. Microsoft has worked on improving the security practices followed on Windows using user access control (UAC). Linux does not have any such tools readily available, so you should avoid using the root user.

Using Sudo Accounts

Users need to avoid using the root account to access the operating system. Ubuntu gives sudo access to different users. Ubuntu locks the root account, so any user cannot log in to the root account without going out of his way to enable the root account and obtain the password.

Earlier versions of Linux distributions allowed users to access the root account through the graphical login screen. They can get to the root desktop. Many applications may not run as root applications, while others may throw errors. If you are moving from using Windows to Linux, you may want to log in to the operating system using root. You may think this is no different from using an administrator account on Windows. This is a terrible thing to do since it endangers your system.

When you use sudo accounts on Ubuntu, you get root privileges. If you use su, you only access the root shell to run the command you may need to use before you come out of the root shell. Through sudo, you can enforce the right security practices in your system. These accesses also ensure that you run the command as a root user without exiting the root shell. You can access and run an application as a root user only when you are in the root shell.

Reducing the Damage

When you access the operating system using your personal account, the system will ensure you that none of the programs you run write on the other programs or systems on your hard drive. The programs you run using your personal account only make changes to your home folder. You cannot modify any system file without gaining access to the root account. This is an easy way to maintain the security of your computer.

Let us assume you use Google Chrome as your default web browsing application. If there is a vulnerability in chrome, and you run the operating system using a root account, you will leave your system open to malware and other web pages. Malware can be pushed into your system through different web pages, and it can be used to read various files on your system, including those stored on personal folders. They can also compromise different system functions. If you are logged into your system using a limited user account, the malicious web page can still send malware, but it cannot read the source files on the operating system or replace any commands. The malware will only damage the information on your account folder. This can lead to problems, but it is better than having your entire system compromised.

Using a limited access account will protect your system against buggy and malicious applications. For instance, you may have an application that has a bug that deletes the files it can access. So, when you run it, the application removes all files from your account folder. This is definitely not good for you, but you can restore the files easily if you have a backup. If the application can access the root account, it can delete every file on your hard drive. This means you need to reinstall the full operating system again on your computer.

Fine-Grained Permissions

Older distributions of Linux used the root account to run various administration programs on your system. Modern distribution systems use tools, like PolicyKit, to differentiate the access or

functions that different user accounts on Linux can perform. You can determine the permissions which can be defined in the application, too.

For instance, if you have a software management application on your operating system, you can use PolicyKit to ensure the application can only install and update your software whenever necessary. The application would only run in your operating system based on permissions you have set. Only the part of the different programs in the operating system which use this software will have elevated or higher permissions. Only this part can install and manage software in your operating system.

The program you are using will not have root access which means it cannot create a security hole or vulnerability in the application or system. You can also use PolicyKit to ensure only some users have the authority to make changes to the system administration. You can also ensure these users do not have access to the root account and cannot make any changes to the operating system. This allows you to control who can perform activities on your system without any hassle.

You can log in to the graphical desktop using your root account in Linux. You can also delete every file on your hard drive or write random information or noise into your hard drive when your system is running. This will obliterate and ruin your file system. This is a terrible idea. You may know what you are doing, but your system is not designed to let you run the applications and tools using the root account. If you use the root account, you will bypass security, leaving your operating system open to any hacks.

Managing User Account Security

You need to maintain control over the user accounts if you want to secure the operating system. This section will look at how you can perform certain user account management functions and tasks. We will also look at how you can implement security measures.

Adding New Users

As mentioned earlier, you should avoid using a root account to perform any functions, especially any regular operations. If you have deployed the operating system on a new server or virtual machine, you will only have a root account on the server. This means you need to create new accounts for everybody who will access the operating system. If it is only you, create a username. To do this, run the command in the shell: *adduser <username>* .

You also need to create a password and enter other key information about the user, and you can do this using the user creation procedure. On Red Hat and CentOS variants, you need to unlock the account to create a password. Do this using the following command: *passwd <username>* .

If you want to use the account you have created to manage the system and other files, you need to give it sudo privileges. If you are using an Ubuntu-based Linux OS, you can do this using the following command: *adduser <username> sudo* . When you add sudo permissions to various users on a CentOS variant, you need to use a different command: *gpasswd -a <username> wheel* . A Debian user does not have to add any sudo privileges since those may have been given to the account as a default setting. If these privileges are not provided, use the command: *apt-get install sudo* . After you do this, you can use the above commands to add the account to the sudo user list. It is important to note the changes to the privilege user groups will only change when you log in after the setting has been updated.

If a user is given sudo permissions, he can perform the operations a root account is allowed to perform. Since the operations are performed in a root shell, you do not compromise on security. If you need to add more users to the server, give them sudo access. Do not give them root access since it is dangerous to share the password with every user. It is also recommended for you to use a sudo account over a root account.

Disable Root Login

Once you set up your account on Linux, you need to disable remote access for the root account. You must do this if you want to prevent any security breaches. The configuration file has the OpenSSH server settings, and you can open it using a text editor on Ubuntu or Debian using the following command: *sudo nano /etc/ssh/sshd_config* . If you use Red Hat or CentOS variants, you can use the following command: *sudo vi /etc/ssh/sshd_config* . You can also search for different authentication settings and options and change the permission to log in to the root account. You can do this by changing the setting to no using the command: *PermitRootLogin no* .

Save the file with the commands. Once you make the updates, restart the server. If you use cloud servers and CentOS, you can use the command: *sudo systemctl restart sshd* . On systems where you use Ubuntu, call the configuration file and restart the system using the following command: *sudo service ssh restart* . The same command will work on Debian, as well.

Password Policies in Linux

If you allow users to access the server remotely, you need to enforce and implement password policies using a module in Linux called PAM. You can invoke this using *pam_cracklib.so* . You can use this module to check the passwords entered by users against any dictionary words. This prevents the use of weak passwords. The module also allows you to define any new password requirements, such as complexity and length. On Debian and Ubuntu systems, you can install this module using the command: *\sudo apt-get install libpam-cracklib* .

Red Hat and CentOS variants come with this module installed. Once you have the distros installed, you need to open and edit the configuration file. If you use Debian or Ubuntu, open the file in a text editor. You can do this using the following command: *sudo nano /etc/pam.d/common-password* . The file will be stored with a new

name on CentOS. Use the command *sudo vi /etc/pam.d/system-auth* to access the file.

When you install the module on Debian or Ubuntu, the password is configured on the server, and the checks are performed. Therefore, you need to find a setting corresponding to this and change it, so it looks like the following: *password required pam_cracklib.so retry=3 minlen=8 difok=3 dcredit=1 ucredit=1 lcredit=1* . If you use CentOS, you may need to add the entire line above directly to the configuration file, but this is dependent on the version you are using.

Let us look at the parameters and see what they mean:

1. **Retry:** This parameter defines the number of times the user can enter an incorrect password
2. **Minlen:** This parameter defines the minimum length every password should have
3. **Difok:** This parameter is used to check the number of characters reused in the current password when compared to a previous password
4. **Dcredit:** This indicates the numerals you need to have in your password
5. **Ucredit:** This defines the number of uppercase characters
6. **Lcredit:** This defines the number of lowercase characters

You can update these settings and save the updated settings. You need to understand that the policies will apply to every user on the server except for administrator users. The latter is responsible for maintaining the strength of root passwords.

Restrict SSH Access

You can use the OpenSSH server to limit the number of connections to the server based on the group users is categorized into. This is a useful technique to have up your sleeve, especially if you have many users and you have some who should not access your server remotely. You can also do this to add more security to your server. For example, when you run a web service, you may not want

everybody to access that service using the same server. To do this, you need to create new user groups. Use an apt name for the group. In the following command, we will create a group of users called sshusers: *sudo groupadd sshusers* .

If you want to be a part of this group, add your username against the group's name using the command: *sudo gpasswd -a <username> sshusers* . If you want to check who has been added to the group, you can use the command: *groups <username>* . The output of this command will show you the different groups of which the username is a part. You can also include another user group in the list for the same user. The list will also have a username that is the same as the name of the user.

The output of the above command is: *user: user sudo sshusers* .

Once this is done, you can specify the group you want to use for OpenSSH. To do this, you need to open the configuration file using an editor. If you have nano installed in your system, you can use the command: *sudo nano /etc/ssh/sshd_config* . Otherwise, you can use the command *sudo vi /etc/ssh/sshd_config* . At the end of your configuration file, you need to add the following line: *AllowGroups sshusers* .

Ensure the configuration option you have chosen is not commented out using the hashtag sign in front of it. Save the file down and exit the editor. Now, restart the SSH server and use this command if you use Debian or Ubuntu servers: *sudo service ssh restart* . With Red Hat and CentOS variants, you can do the same using this command: *sudo systemctl restart sshd* .

Using the new configuration, a user who does not belong to a specific group can be denied access to the server over SSH. Their passwords may be entered correctly, but they will not be given access. This reduces the chance of people hacking the server through brute force attacks. This method is the easiest way to protect the Linux server you are using.

Understanding Account Privileges

As a Linux security professional or system administrator, you need to manage the system users and their activities. You also need to limit the activities a user can perform on the system using different tools. It is important to remember that a user can make mistakes. These can be anything, including assigning an administrator's privileges to a user who is new to Linux, running an application or script on the system using root privileges, or leaving vulnerabilities in your system that allow a hacker to access it. Since you are responsible, you need to do everything in your power to ensure users do not perform any activity on the system that they should not. You may not even want to clean up the mess.

Your main goal should be to control what a user can and cannot do when he accesses the Linux server. A user on a Linux system needs an account to access the system. Users can access these accounts directly when they perform any activity on the operating system, data, or application. Every system requires specific accounts so that it can function properly. It also needs applications that will need an account for them to access the server.

You can manage the privileges assigned to users in multiple ways and using different tools. The best way to manage users' access and privileges is using the privileged access management tools since these allow you to manage the activity centrally.

In this section, we will look at nine important practices you need to bear in mind when it comes to managing accounts and privileges on Linux. It is important to bear in mind that these are not the only ways to protect accounts. Newer methods are emerging regularly, and you can learn more about them depending on the type of system you maintain.

Manage Linux User Accounts

It is easy to create an account on Linux, and we have seen the commands you can use to do this in the previous section. It

becomes difficult to remove or disable an account that you no longer need. If you do not remove these accounts, they continue to be active, which can cause further issues. Every Linux system needs an account that users can use to access the server to perform any activity on the operating system or on the data stored. The system will need accounts for it to function properly. Applications also require accounts that can be used to connect it to the server.

Most people assume that account management only revolves around managing user accounts. They do not worry about the functional, system, or application accounts. This leaves a lot of gaps in your risk management for the server.

Reducing Privileges

When it comes to privileged accounts, you need to restrict these users' access and rights to ensure they only have the authority to perform the required activities and nothing more. It is important to ensure users only do what they are required to do. If you give a user more access than he needs, it will be difficult for you to control what a user can do. You need to consider the following when you assign privileges:

1. Do system administrators need to use the root account?
2. Does a system administrator need to run commands which only the root account can run?
3. Does a database administrator need to access the root account?

Managing Passwords

You may have implemented and enforced a password policy and the parameters one needs to adhere to when they set their policy. Having said that, the goal should be to reduce the number of passwords used in the system. There are places and times where you need to use passwords still. If you use passwords on the system, you must find a way to manage them.

The following need to be kept in mind when it comes to managing passwords on the system:

1. Ensure passwords are frequently changed
2. Prevent the use of old passwords
3. Assess the complexity of the passwords used in the system

These are the basics when it comes to managing passwords. You need to expand this to all passwords on the server, including the root, user, functional, service accounts, and application passwords.

Reduce the Use of Shared Accounts

As an administrator, you should never share an account with another user on the server. Administrators need to have separate accounts for accountability and traceability for all the actions performed by them. You need to track every user's actions. Every Linux system comes with a root account. Applications on your server will have accounts associated with them, and these accounts have their own set of privileges. This limits the access the application can have to the system.

There are times when a data administrator or application administrator needs to perform privileged activities on the operating system, data service, or application. You need to implement and enforce a system where a user can access a different account without logging into the privileged account. This is a sudo command which can be used to access the operating system. You, as an administrator, can extend a user's privilege without allowing them to share accounts. It provides the required accountability and traceability to identify the activities they perform.

Control Access to Accounts

It is important to understand that not every account present in the system needs to be accessed over a network. You must implement and enforce privilege control across the server. It is only when you

do this that nobody logs into incorrect accounts or performs unauthorized activities on your server. It is also important to ensure that every user does not access the server using the SSH configuration. Not every user account on the server needs to access the server from different computers on the network. You do not have to give a user access to the server from anywhere. Users should only access the server to perform the tasks he is assigned.

Maintain Logs

It is important to log everything that happens on your server. You need to log the accesses, changes, patches, privileges, and features of every user on your server. This is not an exhaustive list, and you can look at other aspects of a user's activity, as well. It will take you and your team time to go through the messages and evaluate all the activities performed. This is something you most certainly need to do.

You should report which user has access to perform which activity. You need this information for different regulations. It is important to log all changes to different accounts, changes to entitlements, deletions or additions of users, or any other activity performed by the users. You can only make changes to your servers' rules if you are aware of the activities being performed by the users.

Record and Manage Privileged Activity

It is important to know which user accessed the server, which host was used, where he accessed the server, and how he did it. It is even more important to know the user's privileges and analyze what the user did to the server. You need to collect this data and analyze it to see what activities are being performed on your system.

If you are the administrator, you can manage user rights, activities, and their activities' timings. This is a powerful tool. To understand what a user is doing on the system, you can run commands using privileges not assigned to the users. Some examples of such privileges are database administrators or application administrators.

These users can perform only configuration or maintenance activities. If these users have excessive privileges, it can lead to various problems. You need to manage the administrator access, even if it looks like you cannot trust the administrator. These accounts should be looked at carefully, and the activities should be monitored. This is not because of the people who can use the accounts but because the accounts are a hacker's valuable asset.

Notify or Alert in Case of Suspicious Activity

Once you implement and establish the audit and logging system on Linux, you need to set up an automated notification to alert you of any suspicious activity on any server used in the system. This does not mean you set a signal to report any minor violation, but those which can cause a breach in your servers. Your notification and alerting system must be defined on rules to stop inappropriate behavior. When you log this activity, it will show you that a user is performing a function he should not. You can then use the notification to define rules which will prevent this from happening again. This process will make it easier for you to be proactive instead of reactive. This process is based on the concept of detecting through enforcing. This concept means that you use the same rules to detect and prevent any bad behavior from occurring.

Unify and Centralize

All Linux distros allow you to perform all the actions listed so far natively. For instance, you can use SSH to configure how a user can access the server and where he can access it. You can also use it to define what activities the user can perform using that access. It is easy for you to do this manually if you are working only with one system and a few users. If you have multiple servers, it increases the effort you need to put in to maintain the configuration of the servers. You may also make an error when it comes to manually updating the access and user groups for every user.

It is important to couple privilege management and access control. You will make mistakes if you look at these two domains separately.

In the world of Linux security, you need to couple access and account control as well. To do this, you need to have tools that allow you to manage the access control, account management, and privilege management domains centrally.

Chapter Three: Securing Servers Using Firewalls

As a system administrator, you need to learn how to configure and maintain a firewall for your Linux servers. In this chapter, we will look at how you can manage the server using a firewall-cmd command.

If you have worked on network security before, you know that a firewall is an important part of it. Therefore, it is important for you, as the system administrator, to learn about how a firewall works. It is only when you understand how a firewall works that you can secure the server and make the right choice about which traffic you prefer to allow to enter and exit your server. Firewall is a different name, and some people confuse it with a Tron-style battle which happens at the ends or outside of the network where the game is played. Unlike the Tron-style battle where rogue data packets are released to protect a user's data or techno fortress, a firewall is only a small part of software you can use to control the incoming and incoming traffic in the network.

Ports

You can use firewalls to manage any traffic flowing into and out of the server, and it does this by monitoring the ports used in the network. When it comes to firewalls, the word port does not refer to any physical connection port, such as a VGA, HDMI, or USB. In terms of a firewall, ports are artificial connections or constructs which are created in an operating system. This port is used as a way to connect or create a pathway between various data sources and the operating system to move specific data types. You can name the port using different words, but port is the word used too often. What I am trying to say is that there is nothing new or different about a port. It is only a way to move the data to the right place.

There are different ports used in an operating system, and some are used more often than others. These ports are conventions. If you have worked with HTTP and on coding, you know that the traffic moving via HTTP moves on port 80. Similarly, HTTPS moves on port 443; SSH uses port 22, and FTP uses port 21. When data is moved

from one system to another, a prefix is added to the data set or packets moving through the port. This prefix will determine the port that should be used to move the packets. If the end port accepts the data and information you send through the protocol, it means the data is accepted by the endpoint successfully.

If you do not know how this works, you can learn about it by accessing any URL. Open any browser on your system and use the command *example.com: 80* to send a request to port 80 on your system using an HTTP request through your network using the website. When you do this, you will find yourself on a landing page that is a response. You do not have to enter a port when you try to access a website. All you need to do is enter the URL, and you will reach your website since the network will look at the protocol being called and move the traffic to the respective port. If you want to test how this works, you can run the code using a web browser that is based on a terminal.

```
$ curl --connect-timeout 3 "http://example.com:80" | head -n4

<!doctype html>

<html>

<head>

    <title>Example Domain</title>
```

In the same form, use a different port to reject access to a website. For example, you can add port number 79 (using the notation *example.com:79*) to the above notation. This will push the website to access the incorrect port, which will decline access to the website.

```
$ curl --connect-timeout 3 "http://example.com:79"

curl: (7) Failed to connect: Network is unreachable
```

There is a correlation between protocols and ports on a network, and experts set these conventions. You can easily change these settings if you need to on your computer. When people began to work with computers and networks, they were afraid to change the ports in their network or servers because they believed it could lead to an attack. Now, attacks are sophisticated, and this means the hacker will not learn anything by running a port scanner on the network or web server to determine whether or not there is a change in the ports. A firewall will look at the activity that is performed in the web server on any port.

Using the Firewall-cmd Interface

The operating system you are using will have an infrastructure, in the form of a server and network, in the rack. The objective of this interface is to run the firewall. Alternatively, your modem and router may come installed with a firewall installed in your modem or router. This will act as the primary gateway and path used by any website on the Internet. It is important to remember that firewalls come pre-configured and use a different interface that you can change. In this section, we will look at the different commands you can use through the firewall-cmd interface on your Linux distribution.

You can manage the firewalld daemon on Linux using the firewall-cmd interface. This interface connects the Internet to the Netfilter framework on the Linux kernel. This stack will not be found in modems that have a firewall embedded in them. You can use it on any Linux distribution, which allows you to use the command systemd. If you do not have a firewall that is active on your network, you cannot use the firewall-cmd interface to control anything. Therefore, the first thing you need to do is to check if the interface runs on your system:

$ sudo systemctl enable --now firewalld

Using this command, you can start the firewall daemon on your network and ensure that the daemon will load when you reboot the system.

Bock Everything

When it comes to configuring the firewall used, most experts will ask you to block everything on the firewall. Experts also recommend that once you block everything, you can open the network up to some ports. This means you need to know exactly what your server needs and identify how to do it.

If you work in an organization with its own DNS caching service or DNS, you need to unlock the port before handling the communication in the DNS. If you solely rely on the SSH configuration and use that to change the servers and access them remotely, you cannot block it. You need to know which service runs on the operating system and understand if the service is internal to the organization. You also need to determine if there is any interaction between different services in the server.

When it comes to proprietary software, the server may make calls to external ports, and you may not be aware of these calls. If there are applications that react terribly to any strict firewall on your server, you need to use reverse engineering. You may also need to speak to the application's support line to understand the type of traffic the application is creating. You also need to know why the application behaves the way it does. When it comes to open-source software, this is not a common issue. This is not true for when it comes to complex software stacks. Most media players, for example, will make calls to the Internet. They will need to use the Internet to fetch album art or tracklists. An example of this type of application is Spotify. You need to have your Internet connection on if you want to listen to different music.

The firewall-cmd has presets, and these are zones. These zones have defaults configured in them, which the server can choose from. When you use these zones, you do not have to build the firewall for your server from scratch. A zone will apply to only one section of the network interface, which means if you have two ethernet cables or interfaces on your server, you will have one zone taking care of one ethernet. Therefore, you need to identify the different zones in your

system. If you want to look at all the zones in your system, use the following lines of code:

$ sudo firewall-cmd --get-zones

block dmz drop external home internal public trusted work

If you want to learn more about what is allowed in a specific zone, you can run the following lines of code:

$ sudo firewall-cmd --zone work --list-all

work

   target: default

   icmp-block-inversion: no

   interfaces: ens3

   sources:

   services: cockpit dhcpv6-client ssh

   ports:

   protocols:

   masquerade: no

   forward-ports:

   source-ports:

   icmp-blocks:

   rich rules:

When you use an existing zone in your network interface as the point to build your firewall, you make life easier for yourself. Alternatively,

you can choose to create a firewall from scratch.

Creating a Zone

You need to use the command –new-zone to add a new zone on your web server. Any action you perform using the firewall-cmd command will only persist until you restart the computer. To make anything permanent on your firewall, you need to use the permanent tag to ensure the settings you write are saved. Let us consider an example where you can add a new zone called corp. If you want to make the corp permanent, you need to use the permanent flag and reload the firewall to save the rules. This means your new zone will be active.

$ sudo firewall-cmd - -new-zone corp - -permanent

success

$ sudo firewall-cmd - -reload

Now that you have a new zone in place, you can assign a network interface to this. Before you do this, you need to use the ssh service to access the zone externally. You can also make this a permanent change to your server using the - -permanent flag. This will ensure the changes are maintained even when you reboot the system.

$ sudo firewall-cmd - -zone corp - -add-service ssh - -permanent

You can now use the corp zone since it is active. This will not accept traffic from any port except for SSH. We also have not assigned any network interface to this zone. If you want to activate the corp zone and make it the default zone, you need to use the –change-interface option in the code.

$ firewall-cmd --change-interface ens3 \

  --zone corp --permanent

The interface is under the control of NetworkManager, setting zone to 'corp'.

Success

When you make the corp zone the default zone used in the server, every command you use in the code will be applied to the corp zone. The firewall-cmd command will access the corp zone unless you specify any other zone in the code. You can decide if the corp will be the default zone depending on whether you want it to be the primary zone. If you want to do this, you need to use the following lines of code:

$ sudo firewall-cmd --set-default corp

You can also look at the interfaces and the zones assigned to the interface. To do this, you need to use the following lines:

$ sudo firewall-cmd --get-active-zones``

corp

   interfaces: ens3

work

   interfaces: ens4

Removing or Adding Services

You have now blocked access to the network from every protocol except for SSH. Therefore, you can open the ports used in your network based on the protocol being used. The easy and quick way for you to permit or manage traffic through the firewall is to include predefined networks or services. If you want to look at the list of services that are available on your network, you can use the following lines of code:

$ sudo firewall-cmd --get-services

RH-Satellite-6 amanda-client amqp

amqps apcupsd audit bacula bacula-client

bgp bitcoin bitcoin-rpc bitcoin-testnet ceph

cockpit dhcp dhcpv6 dhcpv6-client distcc dns

[...]

Let us consider a situation where you need to run a web server. To do this, you need to install a web server on the network you want to use. You can use apache2 on Debian or Ubuntu or the httpd package on Fedora or RHEL. In the following example, we will use the httpd service:

$ sudo dnf install httpd

$ sudo systemctl --enable --now httpd

You should now test the web server from your local network and see how it works.

$ curl --silent localhost:80 | grep title

<title>Test Page for the Apache HTTP Server on Red Hat Enterprise Linux</title>

You should then use the network and connect to the web server in your network from any browser, preferably an external one.

$ curl --connect-timeout 3 192.168.122.206

curl: (28) Connection timed out after 3001 milliseconds

Unblocking a Service

If you want to permit the traffic from the HTTP protocol through your network or firewall, you need to include the HTTP service in your

web server.

$ sudo firewall-cmd --add-service http --permanent

$ sudo firewall-cmd –reload

You should test this inclusion using an external browser:

$ curl --silent 192.168.122.206 | grep title

<title>Test Page for the Apache HTTP Server on Red Hat Enterprise Linux</title>

Now, you know how you can include or add a service to your web server. It is, therefore, easy for you to remove one.

$ sudo firewall-cmd --remove-service http --permanent

$ sudo firewall-cmd –reload

Removing and Adding Ports

You may have trouble with finding a predefined service on your system or network. The network or the ports may also assume that the defaults used do not match, and they may reject the access. Instead of adding a service to your firewall, you can add a protocol type or port number using the command *--add-port* . For example, if you want to use a non-standard port for the SSH protocol in your custom zone, you can add the details using the commands below:

$ sudo firewall-cmd --add-port 1622/tcp --permanent

success

$ sudo firewall-cmd --reload

To remove that port, use --remove-port:

$ sudo firewall-cmd --remove-port 1622/tcp --permanent

success

$ sudo firewall-cmd –reload

Walls of Fire

You can do quite a bit using the firewall_cmd command, which is not listed above. You can define ICMP blocking, define the sources which can send data and traffic to your system using the network, or even define the services you want to permit. It is easy for you to learn by experimenting. So, you can install Fedora or Red Hat Enterprise Linux in a GNOME box. This will allow you to play around with traffic and shape it using the firewall-cmd command's different options.

Chapter Four: Securing Your Server

In the previous chapter, we looked at how you can secure the server using a firewall. We also looked at the importance of user accounts and other details. In this chapter, we will look at the different ways to secure a server without using a firewall.

Updating Servers Regularly

If you can access the server as the administrator, you need to update it regularly. To do this, run the following command: *apt-get update && apt-get upgrade* . It is important to ensure while you run the upgrade that you are on a VPS or virtual instance. This can damage the image and the server. So, you need to check if you can do this on your host.

Creating a Secondary User Account

You need to do this to ensure no user logs into the server using the root account. If you want to reduce the probability of unauthorized access on your server, you need to create a user and ensure you give them the relevant privileges to ensure they cannot perform unauthorized activities on the server. We have looked at how you can add new users to the servers. If you want the user to have access to the server with a specified set of privileges, you can give him sudo access.

You need to update these terms in the configuration file. Once you do this, you can save and close the file down. You need to ensure the user can access the server the way he needs to, and you can confirm this by logging into a second terminal on the same server. It is especially important for you to do this. Let us now remove the root users who access the server through SSH. If you want to accomplish this, you need to edit the configuration file: *etc/ssh/sshd_config* . It is important to ensure you are logged into the same server using a different shell before you reload the SSH. This is to ensure you do not log yourself out of the server. Now, open the configuration file

and update the line #PermitRootLogin yes to PermitRootLogin no. You can then restart the service using the following command:

/etc/init.d/sshd restart

Stopping sshd: [OK]

Starting sshd: [OK]

Bear in mind that Linux does not have a default root password when you install the operating system on your server. There is no root login, but you, as an administrator, will have sudo privileges and administrative access.

Setting up SSH Keys

An SSH key on your server allows you to connect securely to the server using an authorized key pair. This is an extra step you need to perform to ensure the server is secure from any unauthorized access. You need to log in to SSH using the root user account and run the following command: *ssh-keygen -t rsa -C "you@example.com"* . Once you click on accept, the default file locations and names will be added to the server along with the file names. You can re-enter the password for your user account and add the public key to the file on your server. Use the following lines of codes to do this:

cd ~/.ssh

cp id_rsa.pub authorized_keys

You should now copy the public key to the SSH directory in the root account that is present on the server. To do this, you can run the following commands:

cd ~/.ssh

scp authorized_keys root@host.servername.com:/root/.ssh/

You can now connect with the server directly.

Checking and Configuring the Firewall

Run the following commands to check and configure your firewall. You can also do it using the information present in the previous chapter.

root@server:~# ufw app list

Available applications:

OpenSSH

root@server:~# ufw status

Status: active

To Action From

-- ------ ----

22/tcp ALLOW Anywhere

22 ALLOW Anywhere

8080/tcp ALLOW Anywhere

80/tcp ALLOW Anywhere

Anywhere DENY 58.218.92.34

80 DENY 202.54.1.5

22 (v6) ALLOW Anywhere (v6)

22/tcp (v6) ALLOW Anywhere (v6)

8080/tcp (v6) ALLOW Anywhere (v6)

80/tcp (v6) ALLOW Anywhere (v6)

Limiting the Use of Open Ports

When you install Linux on your system, you do not have to worry about any network services listening to and monitoring the data you are passing through the server. When you start the server, you can determine who the administrator and root users should be and determine the various ports and services that can use the server. You need to test the open ports on your server. To do this, run the following lines of code:

root@server:~# /home# netstat -tulpn

Active Internet connections (only servers)

Proto Recv-Q Send-Q Local Address   Foreign Address State PID/Program name

tcp   0 0 0.0.0.0:22   0.0.0.0:* LISTEN   69941/sshd

tcp6   0 0 :::22   :::* LISTEN   69941/ss

Setting Up Live Kernel Patches

You can use the canonical livepatch service to determine when your server needs a security fix, especially when it comes to major kernel securities which do not reboot. As a Linux user, you can take advantage of these services for free up to three zones or nodes. Every machine that is a part of the subscription can find a way to fix security issues and vulnerabilities. You can learn more about these tools on the Linux website.

Hardening the Kernel

There are different built-in protections in a kernel, and you can use these methods to ensure the kernel is not compromised.

Hardening User Space

You need to learn more about how you can harden the user spaces. You can use different hardening tools and applications to do this. A common option is to use a compiler flag when you build a tool or application. This is especially true if you use the kernel to launch the application. You can add additional features to the application or tool if you need to. It is important to remember that these additional features can be added to all applications on the server, not just the operating system's official apps.

Using Secure Boot

When Linux developers launched Ubuntu, they included a secure boot to the operating system. The developers added the secure boot option, enforced it in the bootloader, and switched on the kernel's non-enforcing mode. With this setup, the versions that could not authenticate secure boot failed to boot, and the kernels did not validate the authentication, either.

Setting Up Two-Factor Authentication

If you want to add an additional protection layer to your server, you can set up multi-factor or two-factor authentication on the server. You need to be careful about setting this up, because you can lock yourself if you incorrectly enter the password. To do this, follow the steps below:

Step One

Access the server through SSH and run the following command to use Google as your authentication mechanism.

apt-get install libpam-google-authenticator

Step Two

You should now run the command google-authenticator to create a secret key in your server's home directory.

google-authenticator

Do you want authentication tokens to be time-based (y/n) y

Your new secret key is: 73GRSXVJNUXZWN2T

Your verification code is 389485

Your emergency scratch codes are:

99536578

44768915

90480600

82281337

56945099

Do you want me to update your "/root/.google_authenticator" file (y/n) y

Do you want to disallow multiple uses of the same authentication token? This restricts you to one login about every 30s, but it increases your chances to notice or even prevent man-in-the-middle attacks (y/n) y

By default, tokens are good for 30 seconds and in order to compensate for possible time-skew between the client and the server, we allow an extra token before and after the current time. If you experience problems with poor time synchronization, you can increase the window from its default size of 1:30min to about 4min. Do you want to do so (y/n) y

If the computer that you are logging into isn't hardened against brute-force login attempts, you can enable rate-limiting for the authentication module. By default, this limits attackers to no more

than 3 login attempts every 30s. Do you want to enable rate-limiting (y/n) y

Step Three

You should now edit the configuration file for your SSH port. The file is called '*vim /etc/ssh/sshd_config* ' and you can access it using PAM (pluggable authentication module). You need to run the following command before you save the changes and close the file:

UsePAM yes

ChallengeResponseAuthentication yes

Now, you can restart the server using the command below:

systemctl restart ssh

Step Four

Now that you have the SSH set up, you need to edit another configuration file where the PAM is present. This file is for the SSH daemon. You need to add the following command to the file 'vim /etc/pam.d/sshd': *auth required pam_google_authenticator.so* .

Step Five

You now have to save the file down. Close the file and reboot the server. You will now be authenticated using Google authenticator.

Turning Off Internet Protocols

It is important to identify which Internet protocol (IPv4 or IPv6) you use frequently. For instance, if you do not use the IPv6 protocol frequently, you need to disable it in the configuration file. Add the following lines of code to the configuration file to do this:

vim /etc/sysconfig/network

NETWORKING_IPV6=no

IPV6INIT=no

Understanding the Applications/Tools before Installation

Before you install an application or tool on your server, you need to see if any new software or tools are being added to the server along with the application. This will put your server at risk since it will add a newer opening to the server, leading to a vulnerability.

Removing Unnecessary Startup Processes

Linux has various startup processes which run in the system, and these are called targets. You need to look at the settings and see what you need to change or update before you make the change in the configuration file. You can set up servers to ensure they have only the required packages or servers set. This will reduce the amount of time you spend cleaning up your server space.

Reviewing Activities Regularly

Every file on Linux will be located on the server and the infrastructure. You can access the folder or directory with the backup. In this directory, you will have details of all the files on the server and the different logs and their details. You need to review the logs regularly to ensure no unauthorized activities are being performed on the server. If you want to look at the file, you can run the command: *less file.log* . You can use different commands to go through the logs in the directory.

Start Backing Up

In case of any disaster to the server or a hack, it is important for you to have a backup. A backup is your last line of defense, and it is recommended you follow the backup method 3 − 2 − 1. In this method, you need to do the following:

Step One : Maintain 3 copies of your data – one will be the primary source while the other two will be the backups
Step Two : You need to store the data on at least two storage media, such as tape drives, cloud, local drives, etc.
Step Three : There needs to be one copy of the data stored offsite

It is also important for organizations to account for these backups and ensure they have details of any failed backups. Linux is a mature system, and it is quite secure when compared to other operating systems. The operating system has an unparalleled ability to adapt to and set up different configurations. Therefore, it is one of the best systems to use if you want to have a self-managed and secure system. Linux also offers you to use a dedicated server option, and this is stable and fast.

Only Install the Things You Need

This is an important thing to bear in mind – do not download everything you find. You need to install the packages you want to use. Your server should never be overloaded. This means you should only install those packages, applications, and tools on your server if you need them. If you find any application, server, or package on your system that is not required, you need to remove it. If you have fewer packages on your server, you can avoid patching the code.

Use SELinux

SELinux is an enhancement you need to make to the kernel, and this uses a MAC or Mandator Access Control system to ensure any application or tool is defined based on a set of resources. If you want to install the package, use the following command: *apt-get install selinux-basics selinux-policy-default auditd* .

Once you download the package, you need to load the policy script. This is a modified version of the actual script and is included as part of the SELinux package. You should then move this script to the folder, */usr/share/initramfs-tools/scripts/init-bottom/* , and run the

command written below: *update-initramfs -u* . You can use this to update the SELinux package. Once you do this, you need to run the following command to configure PAM, GRUB, and auto relabel creations: selinux-activate.

You should now reboot the server and ensure the changes you have made have taken effect on your server. It may take your system time for you to label the file systems when you boot the server. The system will reboot for the second time when it has labeled the files accurately. Now, run the command and ensure you have everything set up accurately on your server and system. Performing an audit by yourself will help you find different problems in the installation of SELinux. You can learn more about this using the Debian SELinux documents.

SELinux or Security-Enhanced Linux is a security mechanism provided by Linux developers which can be used in the kernel. SELinux provides three operations:

1. **Disabled** : When you use this mode, you can disable the use of SELinux on your server
2. **Permissive** : If you use this mode, you will only receive a warning or alert when unauthorized activity is performed on the server. It will also log the actions performed by the user
3. **Enforcing** : In this mode, the functions of SELinux are not limited, which means it looks at every aspect of the security of your server

You can manage the modes using the '*/etc/selinux/config* ' file.

Securing the Console Access

It is important to protect a Linux server from end-to-end, which means you need to protect the server's access through a console. You need to disable the use of external devices, such as USB pens, CDs, or DVDs, once you set up the BIOS. You also need to set up the BIOS and use the grub boot loader password to protect the updated settings.

Restricting the Use of Old Passwords

You can ensure users do not use old passwords when they are prompted to update their passwords. Your Linux server will save the old passwords in the file /etc/security/opasswd. You can ensure your server does this using the PAM module. If you are unsure of how to do this, follow the steps given below:

1. If you use CentOS, Fedora or RHEL, you can open the file *etc/pam.d/system-auth* . To do this, run the command: *# vi /etc/pam.d/system-auth*
2. If you use Ubuntu or Debian, you can open the file */etc/pam.d/common-password* using the command *# vi /etc/pam.d/common-password*
3. You need to add the following command to the auth section in your configuration file: *auth   sufficient   pam_unix.so likeauth nullok*

Once you do this, you need to add the following lines to the configuration file to ensure a user does not reuse his last few passwords. You can decide the number of passwords you want the server to store.

password   sufficient   pam_unix.so nullok use_authtok md5 shadow remember=5

This line will indicate to the server that it needs to remember the user's last five passwords. So, if the user enters one of the earlier passwords, he will receive an error from Linux asking him to choose a different password.

Checking Listening Ports

You need to look at the different ports in your server and view them along with the services they provide. To do this, you can run the following command: *netstat -tunlp* . Based on the list you receive, you can determine if there are any ports you need to disable from the system. You can do this using the command chkconfig. You can

then close all the ports in the server which you do not need. To do this, you can run the command: *chkconfig serviceName off* .

Disabling Login through the Root

As mentioned earlier, it is important to ensure that you do not log in to your server using the root account. Therefore, you need to disable the ssh port as the root account on the server's configuration file. Before you do this, let us look at an example where we create a user with sudo privileges, so you can use the ssh port to access the server and perform the necessary tasks. When you log in to the server, you can move from the user to the root account if you need to. Let us first create a new user. To do this, use the following command: *useradd user1* . You can now add a password to this user account using the command: *passwd user1* . Now that you have a user created on the server, you can give it sudo permissions using the following line: *echo 'user1 ALL=(ALL) ALL' >> /etc/sudoers* . You then need to use ssh to access the server using the new user account. This is one way to ensure you log in to the server.

Now, we need to disable the root access to the SSH port. This will mean no user can use SSH to log in to the server using the root account. You need to open the configuration file 'nano /etc/ssh/sshd_conf' to do this. You then need to update the line PermitRootLogin to no in the file. You then need to save this file and close it. Once you restart it, you will see that the settings have been updated.

Before you log out of the server, you should test if you can log in to the server using SSH using a user ID that was created earlier. To do this, you can open another instance in the terminal and log in to the council using SSH. If everything works as it should, you can log out of the server as the root user.

Change Ports

You can also change the default port used by SSH to access the network. You can add a layer of security to ensure your server is

safe. To do this, you need to make updates to the *etc/ssh/sshd_config file* . In this file, you need to replace port number 22 with a number you want to use as the port. Once you save the file down, you can reboot the server. To do this, you need to use the following command: *service sshd restart* . You can then log in to the server using the updated port number with the following command: *ssh username@IP -p 1110* .

Disabling Shortcuts

When you hit the shortcut Ctrl+Alt+Delete, your server will automatically reboot. Therefore, it is best for you to disable this shortcut to prevent someone from rebooting the system by mistake. This action is in the configuration file named *etc/init/control-alt-delete.conf* . All you need to do is to comment out the line '#start on control-alt-delete' in the configuration file.

Logging In Without Passwords

You can log in to your server using SSH. You can let go of passwords if you configure the details in the file. The only thing you need to do is to enter the server by generating a key using SSH. It is important to ensure the user can only enter the server from the machine where he generated the ssh key. Let us see how we can generate an SSH key to access the server: *ssh-keygen - t rsa* . Once you generate the key, you can add the key to the server you want to access using the following command: *cat ~/.ssh/id_rsa.pub* .

If you have more than one user on the server, you can give each user a ssh key to access the server from his system. You can do this using the following command:

cd /home/user1

ls -ll

To ensure that only some users have access to a ssh key for security reasons, you can configure the list of users in a ssh directory. You

can do this using the following commands:

mkdir .ssh

cd /home/admin/.ssh

vim authorized_keys

You can also create a public SSH key and add it to the configuration file before changing the owner. To do this, run the following command: *chown user1 authorized_keys* .

If you do not want to use an SSH key, you need to disable the SSH login. To do this, you need to edit the configuration file using the following lines of command:

Edit /etc/ssh/sshd_config

Passwordauthentication no

PermitRootLogin no

Once you do this, you can ensure only an authorized user can enter the server using the command: *ssh user-name@serverIP -p(port Number)* .

Use fail2ban

If you want to use an application to see where a server is attacked frequently, you can use fail2ban. This application also tells you about any automated attacks that happen on the server. It also works on the firewall and updates it when there is any issue found in the server. Fail2ban changes the configuration in the firewall and will push it to block the IP address either for a specific period or permanently, depending on the type of attack.

Run the following command if you want to install fail2ban on your system: *$ sudo apt install fail2ban -y* . You should then copy the configuration file that is found on your system using the following command: *$ sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local* . If

you do not have the jail.local file, you need to create it and then copy the content from the jail.config file to the jail.local file. You can use the following command:

cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local

Edit /etc/fail2ban/jail.local file

You now need to make the required changes to the file:

[sshd]

enabled = true

port   = ssh (provide the port number if the default port is changed)

protocol = tcp

filter   = sshd

logpath = /var/log/secure

maxretry = 3 (max no. of tries after which the host should be banned)

findtime = 600 (You can use this parameter to set the window that the application will pay attention to when it looks for repetitive incorrect authentication in a few seconds)

bantime   = 600 (time duration for which the host is banned -in seconds)

Before you restart the application, you need to block the IP by setting the bantime parameter to -1. Once you do this, you can restart the application using the following command: *$ sudo service fail2ban restart* .

It is as simple as this. The application will continue to examine the log files on the system and look for any attacks. The application will

also have a list of all IP addresses, which it will prevent from accessing the server. If you want to view this list, use the following command: *$ sudo fail2ban-client status ssh* .

You can also use fail2ban to log in to SSH. You need to ensure the application is updated regularly, so you can access the server using SSH.

Creating a New Privileged Account

You should now create a user account. Bear in mind that you do not log in to the server using the root account. You can also create your own account. As mentioned earlier, you should create a sudo account using which you access the server. Now, log in to the server using the sudo account. We have looked at how you can create new accounts and give it sudo privilege access.

Uploading the SSH Key

When you create a new server, you need an SSH key to access the server. You can use a pre-generated SSH key if you want to or create a new key. To do this, run the following command: *$ ssh-copy-id <username>@ip_address* . You can now avoid the password when you log in to the new server using the SSH key.

Securing SSH

Once you do this, you need to make the following changes:

Step One : Remove the password authentication for the SSH protocol
Step Two : Do not allow users to access the root account remotely
Step Three : You also need to restrict access to IPv6 and IPv4

To do this, you need to make changes to the SSH configuration file. When you open the file, you will find the following lines of code:

PasswordAuthentication yes

PermitRootLogin yes

You need to change it, so the lines look at follows:

PasswordAuthentication no

PermitRootLogin no

You then need to restrict which IP the SSH service uses – either IPv4 or IPv6. You can do this by making changes to the AddressFamily option in the configuration file. If you want to change it, so it uses only IPv4, make the following change:

AddressFamily inet

It is only when you restart the SSH service that your changes will reflect on your server. Bear in mind that you should have two active server connections before you restart the SSH server. When you have an extra connection, you can fix any issue that may arise in case the restart does not go as planned. If you use Ubuntu, you can run the following command: *$ sudo service sshd restart* . If you use any Linux distros which has a Systemd configuration, run the following command: *$ sudo systemctl restart sshd* .

Creating a Firewall

In the previous chapter, we looked at how you can install, enable and configure a firewall on your system, so it allows only the network traffic you allow to access the server. You can also use an uncomplicated firewall on your server if you need to, depending on how well you code. If you cannot code, use the uncomplicated firewall. You can install it on your system using the following command: *$ sudo apt install ufw* .

The uncomplicated firewall, by default, will deny any incoming connections and allow everything to go out of the network. This means all the tools and applications on your system or server can connect to the Internet, but if anything external tries to connect to the

server, it will not allow it. You need to ensure you can access HTTPS, HTTP, and SSH protocols on your server using the following commands:

$ sudo ufw allow ssh

$ sudo ufw allow http

$ sudo ufw allow https

After you do this, you should enable the uncomplicated firewall using the following command: *$ sudo ufw enable* . You also need to check which services and applications are allowed and denied by the uncomplicated firewall: *$ sudo ufw status* . If you do not want to use the uncomplicated firewall, you should type the following command: *$ sudo ufw disable* . Alternatively, you can use the firewall interface we discussed in the previous chapter, as well.

Removing Unused Network Services

Every Linux operating system has a server that has applications and servers that work with the network. You need to use most of these applications and servers, but you can get rid of some. Using the command ss, you can see the network services and applications being used on your Linux servers.

$ sudo ss -atpu

The output of this command will differ depending on the distros you are using on your system. The following is an example of the output you may see. The output shows that the Ngnix (ngnix) and SSH (sshd_ services are the only active services. These are listening to every activity on the server and are waiting to connect to another server.

tcp LISTEN 0 128 *:http *:* users:(("nginx",pid=22563,fd=7))

tcp LISTEN 0 128 *:ssh *:* users:(("sshd",pid=685,fd=3))

The process of removing an unused or dormant application or service will be different depending on the type of distros you are using. It also depends on the package manager on the operating system. If you use Ubuntu or Debian, you need to run the following command: *$ sudo apt purge <service_name>* . On CentOS or Red Hat systems, you need to run the command *$ sudo yum remove <service_name>* . If you run the ss -atup one more time, you can determine if the unused or dormant services are no longer running and are uninstalled on your operating system.

In this chapter, we looked at tips you need to keep in mind when it comes to hardening your Linux server without using a firewall. You can add additional security layers to the server depending on how you and your team use the system. Some of these layers include intrusion detection software, access control and management, two-factor authentication, individual application configuration, and more.

Chapter Five: Password Encryption Methods in Linux

Since passwords are the main security mechanism used these days, it is important to ensure that every user on the server or system has a difficult and secure password. Linux distributions come with password programs that ensure a user's password is strong. You can also use other encryption software available in the market if you want to add another layer of protection to the passwords stored in the server. You need to ensure the programs used to protect passwords are updated constantly.

You need to use encryption software since it is necessary now more than ever. There are different methods you can use to encrypt data, and every method has its own characteristics. We will discuss methods in the latter part of the chapter. Since Linux distributions use a one-way password encryption method, no user can learn another user's password. The method used is called Data Encryption Standard (DES).

The passwords, once encrypted, are stored in a file on the server. If you do not use shadow passwords, the passwords are stored in the '*/etc/passwd* ' file. Otherwise, they are stored in the '*/etc/shadow* ' file. When a user logs into the server or network, the password he enters will be encrypted and checked against the file where his password is stored. If the passwords match, the user can enter the system. Otherwise, his access is denied. He is given a number of attempts depending on what has been keyed into the server. The data encryption algorithm or standard works as a two-way algorithm that allows users to encode and decode any message by using the right keys. Most Linux distributions only use a one-way algorithm, which means no user can reverse the encryption to identify the password.

You can use different methods, such as brute force attacks or password injections, to guess a user's password unless the password is strong. Using PAM modules, a user can encrypt his

password using different routines in the module. If you are still unsure of the password being used, you can use "Crack" to assess your password's strength and the passwords of every other user on the system. Experts recommend that users run the "Crack" program on their server as often as possible to identify any insecure passwords. Only when you do this can you determine the strength of the passwords in your system.

Pretty Good Privacy (PGP) and Public-Key Cryptography

If you use public-key cryptography, there will be separate keys used to encrypt and decrypt the information passed through the server. Traditional forms of cryptography use one key to encrypt and decrypt information, and this key should be available to both parties. It is assumed that the key is transferred carefully between the users. The public-key cryptography method uses two different keys to prevent the loss of the key used to decrypt information during the transfer. A public key is available for anybody who performs the encryption. The user, however, must ensure the decryption key used by them is kept private. They should not share this key with anybody over the network.

PGP is another privacy option you can use to protect the data on your system and server. If you choose to use this, ensure you have the version applicable and allowed in your country. There are some export restrictions placed by the US government. Therefore, you cannot use strong encryptions when you transfer any information from outside the country.

S/MIME, SSL and S-HTTP

Most users are unaware of the differences between these forms of encryption and security protocols. They also do not know how they can be used. In this section, we will go through each protocol to know how to use them to secure your network and server.

S/MIME

S/MIME or Secure Multipurpose Internet Mail Extension is a standard encryption protocol. This is used to encrypt all messages passed through the Internet, especially electronic email. S/MIME is an open standard, and this was developed by three programmers - Ron Rivest, Adi Shamir, and Leonard Adleman or RSA. Therefore, you will see it used in Linux quite often.

SSL

SSL or Secure Sockets Layer is an encryption method used often in Linux. It was developed to provide security when moving data across the Internet and was programmed by Netscape. SSL also uses different encryption protocols and ensures the client and server is authenticated. The protocol will operate at the transport layer. It will also create a secure encrypted channel within which the data is passed. This makes it easy for you to encrypt the data passed through the connection. This encryption method is used when you visit a secure website. For example, you may want to access an online document that is secured. To do this, you can use the communicator. On using this method, the SSL will create a secure communication network with the communicator using different encryption software.

S-HTTP

S-HTTP is another Internet protocol that is used to provide security when you pass data through the Internet. This protocol was first designed to provide confidentiality, integrity, and authentication when data is passed across the network. It also supports cryptographic algorithms and the use of multiple key-management systems through the option of negotiating between the different parties communicating over the Internet. This protocol is limited to the use of specific encryption software, and you can implement it to ensure every individual only accesses secure information.

Linux IPSEC Implementation

Along with Cryptographic IP Encapsulation (CIPE) and other forms of data encryption, there are different Internet Protocol Security (IPSEC) methods used in Linux. The Internet Engineering Task Force developed the IPSEC methods and tools to ensure the data passed between IP networks was safe. These methods and tools encrypt the data using different cryptographic programs. You can also use these methods to manage access control, confidentiality, integrity, and authentication.

The Linux FreeS or WAN IPSEC is a free implementation of IPSEC which can be used on almost any system. This service allows you to build a secure tunnel even when you use untrusted networks or connections. The IPSEC gateway machine will encrypt all the information passing through the untrusted network. The machine also decrypts the information at the destination. The IPSEC gateway machine led to the development and use of Virtual Private Networks or VPNs to ensure there is a secure network used by machines, especially if they are connected to the same server or network from different locations and devices.

Secure Telnet (stelnet) and Secure Shell (ssh)

ssh and stelnet are a collection or suite of programs that enable a user to log in to the server or system remotely. These programs use an encrypted connection which allows them to log in safely.

Another suite of programs called openssh is used as a replacement for rcp, rlogin, and rsh. This is a secure alternative to these programs. This suite encrypts the communication or data passed between hosts through public-key cryptography. It also can be used to authenticate users on the server or system. This program can also be used by users to log in to the server remotely. Once they are logged in, users can copy the data between hosts and prevent DNS spoofing, man-in-the-middle, and other hacks. The suite compresses the data passed between users and secures the data passed between the connection.

SSLeay is another SSL protocol that has many features like stelnet. It was developed as part of Netscape's SSL protocol. It can be used on numerous databases and algorithms, including IDEA, DES, and Blowfish.

Pluggable Authentication Modules or PAM

New versions of Red Hat Linux and Debian Linux distributions use a unified authentication mechanism to move data between networks and other logical connections. This is termed as PAM or Pluggable Authentication Modules. These modules allow users to change their authentication methods and requirements as and when they need to. They can also use these modules to encapsulate any local authentication methods used without having to recompile the information or binaries. The following are functions you can perform using PAM:

1. Prevent Denial of Service (DoS) attacks from users by setting resource limits for each user
2. Allow users to log in to the server only from specific devices and places at specific time intervals
3. Use shadow passwords (we will cover this shortly)
4. Use different forms of encryption, including DES, for passwords to ensure they cannot be detected through brute-force attacks

If you have this enabled in your server or network, you can prevent numerous attacks before they occur on your system.

CIPE or Cryptographic IP Encapsulation

The objective of this encryption is to provide a facility that is secure for the server and system. This encryption protects the interconnection between subnetworks across insecure packet networks from traffic analysis, eavesdropping, and faked message injection. Using CIPE, you can encrypt the data at both the server and network levels. All the information moving along the network in

the form of packets is encrypted, and these packets are received and sent by an encryption engine that is next to the network driver.

CIPE does not encrypt the data that is passed through the network or connection. It does not even encrypt the data at the network or socket levels. It will only encrypt the logical connection between networks, sockets, and programs found on different hosts. This is very different from SSH. You can also use CIPE to create new VPNs through tunneling. If you want to avoid making changes to the application software being used, you can use low-level encryption methods. These methods ensure the logical connection between two networks connected in the VPN or Virtual Private Network work transparently.

Using Shadow Passwords

You can use shadow passwords to ensure a user's password is encrypted and the information is maintained in a file that normal users cannot access. New versions of RedHat and Debian Linus use this setting as a default. After encryption, the passwords are stored in a file in the server directory that every user on the server can access. If one were to run a password cracking or guesser program on the file, they could obtain every user's password on the system.

A shadow password will be stored in a different file which can be accessed only be an administrator or privileged users. If you want to use shadow passwords, you need to ensure that every application, tool or utility which needs the password can access the information. You may also need to recompile the list of passwords to support the user's access to the system. Using PAM, you can plug in a shadow module that does not require you to recompile any of the system's passwords.

John the Ripper and Crack

If you use a password program on your server, but you notice that hard-to-guess passwords are not used, then you need to run a password cracking program. This program will help you determine if

the passwords used by you and your users are safe and secure. The idea behind a password cracking program is simple – the program will look at every word in the dictionary and try variations of the same words. It will also encrypt the words and check those words against your password. If the program finds a match, it will know the user's password.

There are numerous password-cracking programs you can use, but people often use "John the Ripper" and "Crack." These programs may take up your CPU's time but give excellent results. Before a hacker uses these programs on your system and server, you need to use them and check if there are any weak passwords. If yes, ask the users to change them immediately to avoid any hacks. You may wonder how the hacker can access the password file on the server when he can only access the server through a hole or vulnerability. Unfortunately, there are holes in the server, and an experienced hacker can find those holes easily.

You can also try other encryption methods used in Linux, such as Transparent Cryptographic File System (TCFS), Cryptographic File system, display security, X11, and SVGA. We will look at them in detail later in the book.

Chapter Six: Tools to Encrypt and Decrypt Password Protected Files

The process of encoding or protecting files to ensure only selected users can access the file is termed encryption. We have been using the concept of encryption even before computers came into existence. When countries were at war, they developed codes to communicate with their spies or soldiers in the warzone. This was one way for them to ensure nobody else could understand the message that was being passed.

Linux distributions come with standard tools used to encrypt and decrypt the information in the system or server. In this chapter, we will look at seven tools you can use to encrypt and decrypt files using a password.

GNU Privacy Guard or GnuPG

GnuPG, often called GPG, is a collection or suite of various cryptographic software and is written in C language. If you want to use this to encrypt and decrypt files, it is best to download the file's latest version. Most Linux distributions released in the last few years will come with this package installed as a default. If you find that it is not installed in your server or system, use the following commands to install it:

$ sudo apt-get install gnupg

yum install gnupg

Across all the examples in this chapter, we will use a file called tecmint.txt file to encrypt and decrypt. This file is on the desktop of the system and will be moved to a different location if required. Before we go ahead, let us look at the content in this file. To do this, run the following command: *$ cat ~/Desktop/Tecmint/tecmint.txt* .

You can now encrypt the tecmint.txt using the tool. When you run the GPC command using the '-c' option. This is a symmetric cipher, and

it will create the encrypted file with the extension '.gpg' against the file tecmint.txt. You can look at the content in the directory to determine which file was encrypted:

$ gpg -c ~/Desktop/Tecmint/tecmint.txt

$ ls -l ~/Desktop/Tecmint

You need to enter the word 'paraphrase' twice if you want to encrypt any file. In the above example, we have used the encryption algorithm CA S T5 to encrypt the file. You can specify a different algorithm if you use a specific one often. If you want to look at the different algorithms available to you, enter the following command: *$ gpg –version* .

To decrypt the file we have encrypted above, you need to use the commands below. Before you do this, you need to remove the original file from the desktop and only leave the encrypted file. We do this since the decryption algorithm will replace the encrypted file with the original file, and you may receive an error if you have the older file on the desktop while you perform the decryption. The commands to run are:

$ rm ~/Desktop/Tecmint/tecmint.txt

$ gpg ~/Desktop/Tecmint/tecmint.txt.gpg

It is important for you to remember the password you use at the time of encryption. You need to use the same password if you want to decrypt the file.

Bcrypt

Bcrypt is a function based on the Blowfish cipher, and the developers tried to ensure that the algorithm used was not as weak as the Blowfish cipher. Most organizations stopped using the Blowfish cipher when they learned that users could attack the algorithm from

anywhere because of a small vulnerability. To install the tool on your system, run the following commands:

$ sudo apt-get install bcrypt

yum install bcrypt

When you encrypt the file, you need to run the following command: *$ bcrypt ~/Desktop/Tecmint/tecmint.txt* . When you run this command, the server will create a new file on your desktop and replace the original file. To decrypt the file, you need to run the command: *$ bcrypt tecmint.txt.bfe* .

Since bcrypt is not very secure when it comes to encryption, it cannot be used on some versions of Debian that do not have their own security layers.

Ccrypt

This tool was developed specifically for Linux and is like the crypt tool used for Unix. Ccrypt is a utility for the encryption and decryption of streams and files. The tool uses a cypher called Rijndael. You can use the following commands to install the tool or application on your system:

$ sudo apt-get install ccrypt

yum install ccrypt

The tool uses the ccencrypt and ccdecrypt to encrypt and decrypt a file, respectively. It is important for you to notice that when you encrypt the file, you need to use the original file tecmint.txt. After encryption, you need to replace the file with the file tecmint.txt.cpt. When you decrypt the file, the original file is found in the folder instead of the encrypted file. You can use the 'ls' command to do this.

Use the following command when you want to encrypt a file: *$ ccencrypt ~/Desktop/Tecmint/tecmint.txt* . Similarly, the command used to decrypt a file is: *$ ccdecrypt ~/Desktop/Tecmint/tecmint.txt.cpt* . You must ensure to enter the same password when you encrypt and decrypt the file.

4-Zip

Users commonly use this tool, and it is the most famous archive format. Since this tool is used often, the files used are called archive files. If you have not installed this application or tool on your system, you can do it using yum or apt.

$ sudo apt-get install zip

yum install zip

You can create an encrypted zip file by grouping multiple files together using the following command: *$ zip --password mypassword tecmint.zip tecmint.txt tecmint1.1txt tecmint2.txt* . Using the above code, you are using mypassword to encrypt the file you want to. The tool will create an archive with the name techmint.zip. There will be two zipped files, namely tecmint1.txt and tecmint2.txt, and you can use the following command to decrypt the file: *$ unzip tecmint.zip* . You need to provide the same password when you encrypt and decrypt the file.

Openssl

Openssl is a cryptographic tool used to encrypt and decrypt files and messages. This is run on the command prompt, and it's easy to use if you are familiar with coding. If you do not have the application installed on your system, you can do this using the following commands:

$ sudo apt-get install openssl

yum install openssl

Let us first look at the commands you need to run to encrypt a file using this tool:

$ openssl enc -aes-256-cbc -in ~/Desktop/Tecmint/tecmint.txt -out ~/Desktop/Tecmint/tecmint.dat.

In the above command we used various options/keywords to encrypt the file. Let us look at what these terms mean:

1. Enc: encryption
2. -out: This is the path where the file will be decrypted
3. -in: This is the location where your encrypted file will be stored
4. -aes-256-cbc: This is the algorithm used to encrypt and decrypt the files

Now, let us look at how you can decrypt files using this tool. Run the following command in the command prompt:

$ openssl enc -aes-256-cbc -d -in ~/Desktop/Tecmint/tecmint.dat > ~/Desktop/Tecmint/tecmint1.txt

7-Zip

This is an open-source tool that is written in C++, and it can be used to compress and uncompress most information stored in files. If you do not have this tool on your system yet, you can either install it using the yum or apt commands as follows:

$ sudo apt-get install p7zip-full

yum install p7zip-full

Once you do this, you need to compress the file into a zip folder using the tool and encrypt it using a password. Run the following command to encrypt the file: *$ 7za a -tzip -p -mem=AES256 tecmint.zip tecmint.txt tecmint1.txt* . If you want to decrypt the file, you need to run the command: *$ 7za e tecmint.zip* .

Bear in mind that you need to provide the same password when you encrypt and decrypt the files.

Nautilus Encryption Utility

So far, we have looked at tools that are based on commands. The Nautilus Encryption Utility is a graphic user interface tool. You can encrypt and decrypt files in the graphical interface.

Encryption

You need to follow the steps below if you want to encrypt the files using a Nautilus encryption utility.

Step One : Select the file you need to encrypt
Step Two : The next thing to do is encrypt the file into a zip folder and choose the location you want to save it to. You also need to choose the password you want to use to encrypt the file
Step Three : Once you do this, you will note that the encrypted file has been created in the location

Decryption

Step One : Open the zip file created in the user interface. You will see a lock icon present next to the file's name. This icon indicates that you need to enter a password before you can view the contents in the file
Step Two : If you have entered the right password, the file will open for you

This is not an exhaustive list of tools you can use to protect files using encryption.

Chapter Seven: Using Tools to Encrypt Files on Linux

In this chapter, we will look at the different tools you can use to encrypt and mount various files and folders onto your partition.

Tomb

This is an open-source and free tool that can be used to encrypt data easily. You can also use it to back files on your Linux system easily. It consists of simple programs and shell scripts that you can use to implement in-built encryption tools on your systems, such as LUKS and cryptsetup. This tool aims to improve the safety of your data to ensure you encrypt the data without losing any data. It uses well-tested methods and standards. It is easy to implement. The tool comes with the right practices and methods to store data and mount encrypted data onto a file or partition.

Cryptmount

Cryptmount is an open-source and free tool that was created specifically for Linux operating systems. This tool allows you to mount any encrypted file in the partition created without using administrator or root privileges. The tool uses a devmapper mechanism or process, which offers numerous advantages. It also helps you improve the functionality of the kernel. It also supports the movement and partition of swaps for privileged users. It also supports the use of the crypto-swap mechanism when the system boots. You can also store multiple encrypted systems and files onto one disk.

CryFS

CryFS is an open-source and free cloud-based encryption application that allows you to encrypt and store files anywhere on the cloud. It is extremely easy for you to set up, and you can run it in the background. It works with all the popular cloud services, including iCloud, Dropbox, and OneDrive. The tool ensures there is no data

anywhere but in your system and on the cloud. This data includes metadata, file content, and directory structure.

GnuPG

GNU Privacy Cloud, GnuPG or GPG is a free and open-source tool you can use to encrypt files on the server. It comes with a collection of cryptographic tools and you can use this tool as a replacement for Symantec's PGP cryptographic software. This tool or application is compliant with the various standards and tracks specific to the RFC 4889 and OpenPGP. We have looked at how this can be used in the previous chapter.

VeraCrypt

This is an open-source, free and multi-platform tool which can be used to provide any user with the option to encrypt the files whenever they need to. You can use the tool to encrypt selected partitions or an entire device using different methods of authentication. VeraCrypt allows users to:

Step One : Create disks, encrypt them and mount them onto the shell
Step Two : Ensure the files appear like they are real
Step Three : Pipeline
Step Four : Parallelize the drives and storage units into different partitions

EncFS

This is another open-source and free tool that is used on Windows and Mac to mount EncFS folders. You can also use it to edit, create, export, and change the encrypt EncFS folders' password. If you wish to use this tool, you need to download the latest version. It is also compatible with Linux.

7-zip

This is a free and popular tool and is open-source to an extent. You may have to pay to use some functionalities in the tool. It is a multi-source platform and uses a file archiving mechanism to compress files or directories into containers. These containers are termed as archives. 7-zip is a popular utility tool used because of the compression ratio using the forms LZMA and LZMA2 with the 7z format. It also comes with a plugin for a FAR manager and can be integrated with Windows. Some other features of 7-zip are AES-256 encryption.

Dm-crypt

Dm-crypt is another tool used to encrypt the files and folders stored at the disk level. It does this by encrypting portable containers, disks and partitions. This tool was developed to address reliability and vulnerability issues found in the tool cryptoloop. It can also be used to back up large volumes of data of different forms.

eCryptfs

eCryptfs is an open-source and free collection of software and tools you can use to encrypt data on disks used in Linux. This tool works like the GnuPG tool, and it implements a POSIX-compliant layer of encryption on the files and systems. This is a part of the Linux kernel and comes installed with most Linux distros. Every version after the Linux 2.6.19 version comes with this tool. eCryptfs is easy for beginners to use since it helps you encrypt partitions and directories without worrying about the file system.

Cryptsetup

Cryptosetup is a tool or application used to enable users to encrypt various files using a DMCrypt, a kernel module with an emphasis on the Linux Unified Key Setup (LUKS) design. This key has become a standard encryption technique used in the Linux hard drive because it is compatible with every distro available on Linux. This design also ensures that data can be migrated or transported through the

network smoothly by securing the information through passwords and other encryption methods.

Chapter Eight: Using Cryptsetup to Setup Encrypted Filesystems and Swap Space

A Linux Foundation Certified Engineer or LFCE is trained and has the knowledge to handle Linux network services. He will be trained to install, troubleshoot and manage network services in these systems. He also deals with the maintenance, design, and implementation of the architecture used in Linux systems. If you are a certified LFCE, you can do everything out there to manage the data and files stored in the system or network.

The objective of encryption is to ensure you have only trusted people accessing your information, especially sensitive data. This is the best way to protect the data from being used by hackers in case of any data leak. You can also use this method to protect the data from being stolen or lost from your hard disk or machine.

In simple words, the objective of encryption is for you to use a lock to access the information on your system or server. This is done to ensure the information only is available when you run the system. You can ensure any unauthorized users cannot unlock the system. This means if a person tries to look at the content on the disk, he will not find any information on the files.

In this chapter, we will look at how you can use the dm-crypt to set up an encrypted file system in your server. The term dm-crypt is short for device-mapper and cryptographic. This is the standard tool used for encrypting data in the kernel. It is important to note that the dm-crypt tool can only be used at a block-level. You can use it to encrypt the entire device, loop device, or partition.

Using a Drive, Loop Device, or Partition for Encryption

Before you perform encryption on your drive, you need to backup all the files on the drive, partition, or loop device before you wipe the data in the chosen space. It is important for you to do this before you

proceed further. You also need to wipe the data from the device used, and to do this, we will use the dd command. You can also perform these actions using different tools, such as shred. We will now create a partition on the device, /dev/sdb1, using the command # dd if=/dev/urandom of=/dev/sdb bs=4096.

Testing the Encryption

Before we see how we can use cryptsetup to encrypt files, we need to ensure the kernel is compiled of the encryption you use. To do this, you can write the following command: # grep -i config_dm_crypt /boot/config-$(uname -r). You need to ensure the kernel module dm-crypt is set up correctly to ensure the files and systems can be encrypted in the server and network.

Installing cryptsetup

Cryptsetup is a tool used to create, configure, access and manage any encrypted files on the server or network. You can do this using dm-crypt. Run the following commands to install the tool on your system:

aptitude update && aptitude install cryptsetup   [On Ubuntu]

yum update && yum install cryptsetup   [On CentOS]

zypper refresh && zypper install cryptsetup   [On openSUSE]

Setting the Encrypted Partition

The cryptsetup using Linux Unified Key Setup (LUKS) as the default operating mode, so this means you can stick to it. You can set the partition along with the passphrase using the command: # cryptsetup -y luksFormat /dev/sdb1

In the above command, you can run the cryptsetup using some of the default parameters. If you do not know what these parameters are, you can list them using the command: # cryptsetup –version. Using the list of parameters on your screen, you can determine if you want to change the key, cipher, or hash parameters. If you want to change them, you need to add the symbol '-' before the parameter and add a flag to it. You can then change the parameter which you take from the file /proc/crypto. You then need to open the partition you have created for LUKS. You will be asked to enter the passphrase you used previously. If your authentication passes, you will see that the partition is encrypted in the server or system. This will be present inside /dev/mapper using the following name: # cryptsetup luksOpen /dev/sdb1 my_encrypted_partition.

We will now save the partition using the format ext4. To do this, run the following command: # mkfs.ext4 /dev/mapper/my_encrypted_partition. This will allow you to create a mount point in your partition, which will help you mount the partition encrypted in the partition. You can also use the commands below to determine if the mount operation is successful:

mkdir /mnt/enc

mount /dev/mapper/my_encrypted_partition /mnt/enc

mount | grep partition

If you are done reading from or writing to the file system you have encrypted, you need to unmount it using the following command: # umount /mnt/enc. Once you do this, you can close the LUKS partition using the following command: # cryptesetup luksClose my_encrypted_partition.

Testing Encryption

Now that you have encrypted the file, you need to check if the partition or swap you have encrypted is safe.

Step One : The first thing you need to do is enter the LUKS partition you have created. To do this, run the command: # cryptsetup luksOpen /dev/sdb1 my_encrypted_partition

Step Two : Now, enter the passphrase you entered to encrypt the file

Step Three : The next thing to do is to mount the partition using the following command: # mount /dev/mapper/my_encrypted_partition /mnt/enc

Step Four : You need to create a dummy file in the mount point using the command: # echo "This is Part 3 of a 12-article series about the LFCE certification" > /mnt/enc/testfile.txt

Step Five : You also need to verify if you can access and use the files you have created in the mount point using the command: # cat /mnt/enc/testfile.txt

Step Six : To unmount the system, you need to enter the command: # umount /mnt/enc

Step Seven : Now that this is done, you can close the partition using the command: # cryptsetup luksClose my_encrypted_partition

Step Eight : When you try to mount the file in the regular file system, it will indicate an error. If it does, you have done the right thing to encrypt the partition

Adding Additional Layers of Security

You can also encrypt the swap space in the server to add another layer of security. When you enter a passphrase on your server to encrypt the partition in the server, it will be stored in the RAM when you switch your system on. If any hacker wants to use this key, he can easily decrypt this information in the data. It is especially easy to do this when it comes to a laptop since the partitions of a RAM are maintained, even during their hibernation sessions, in the swap layers or sections of the memory.

If you want to avoid leaving a copy of the accessible to a hacker, you need to encrypt this swap layer or partition using the process mentioned below:

Step One : Create a partition or separation in the RAM, which will be used as the swap. You need to maintain the right size and use the encryption mechanism mentioned earlier. You can name this section as swap if you need to

Step Two : Once you set this partition, you need to activate the swap using the following commands:

    # mkswap /dev/mapper/swap

    # swapon /dev/mapper/swap

Step Three : You should now change the entry of the swap in the file: /etc/fstab. To do this, use the following command: /dev/mapper/swap

none   swap   sw   0 0

Step Four : The last thing you need to do is to save the file down and reboot the server. To do this, run the following command: swap   /dev/sdd1   /dev/urandom swap

When you reboot the system, you can verify if the swap space is active or not using the following command: # cryptsetup status swap.

Chapter Nine: Using Access Control Lists in Linux

Now that you know how to encrypt and protect your files and data using a password, let us understand how you can control access to the servers in Linux.

Introduction to Access Control Lists (ACL)

An ACL is one that provides flexible and additional permissions for your files and directories. It is designed so you can work with the different file permissions in Linux. ACL also allows you to identify the permissions you need to set for each user or a group of users. You can also use it to protect any disc resource.

Uses of ACL

Consider a situation where you have a user who is not a part of any user group on the server or network. This user needs to access files and make changes to them, so you will need to give him access using commands. This is where the concept of Access Control Lists comes into the picture. Using ACLs, you can grant flexible permissions to specific users in the system. If you are an administrator, you can use an ACL to define the fine-grained access rights for directories and files. You can use the keywords setfacl and getfacl to set up an ACL and view the ACL on your server or system. For instance, if you run the following command: getfacl test/declarations.h, you will receive the output below:

file: test/declarations.h

owner: mandeep

group: mandeep

user::rw-

group::rw-

other::r—

List of Commands to Set Up ACLs

In this section, we will look at the different commands you can use to set up ACLs in your system.

Adding Permissions to Users

You can do this using the following command:

setfacl -m "u:user:permissions" /path/to/file

Adding Permissions to Groups

To do this, run the command: setfacl -m "g:group:permissions" /path/to/file

Allowing Files and Directories to Inherit ACL Entries

You can use the following command to allow a file or directory to inherit the properties or privileges found in an ACL from the directory it is a part of: setfacl -dm "entry" /path/to/dir.

Removing a Specific Entry in the ACL

To do this, you can run the command: setfacl -x "entry" /path/to/file

Removing Entries in ACL

There may be times when you might want to remove the entries in the ACL. To do this, you need to run the command: setfacl -b path/to/file. For instance, you can use the following to remove the declarations against the user Mandeep: setfacl -m u:mandeep:rwx test/declarations.h

Modifying the ACL

Adding Permissions for Users

To do this, you need to enter either the username or ID of the user who you want to add to the list. Use the following command to do this: # setfacl -m "u:user:permissions".

Adding Permissions to Groups

This is similar to what was done in the previous section. You can use the group name and ID to add permissions. Use the following command to do this: # setfacl -m "g:group:permissions"

Allow Files or Directories to Inherit the ACL Entries

You can use commands to let the files and directories obtain the properties from the directory where the files and directories are present. To do this, you need to use the command: # setfacl -dm "entry".

For example, when you run the command setfacl -m u:mandeep:r-x test/declarations.h, the output will be the one in the image below.
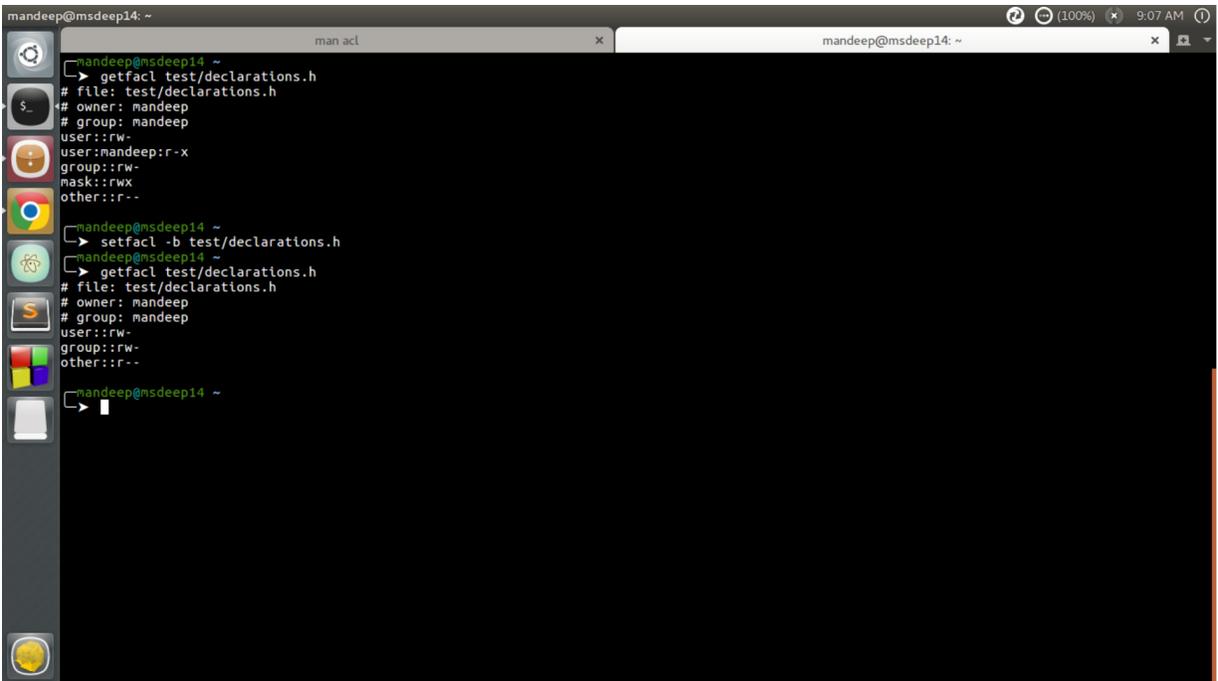
Viewing ACL

You can use the following command to view the permissions written in ACL: # getfacl filename. The differences between the getfacl and setfacl commands are quite obvious. So, pay attention to them. We have used an extra line against the username Mandeep, and this is in the image above. You can use the above command to change the permissions in the ACL from rwx to r-x.

Removing ACL

If you want to remove any commands you set in the ACL, use the setfacl command with the option '-b.' Consider the example below:

Now, compare the output when you run the getfacl command before and after you use the setfacl commands with the option '-b.' You will see there is no entry in the list with the name mandeep in the second output. You can also look for any extra permissions which were set through the ACL using the command 'ls.'
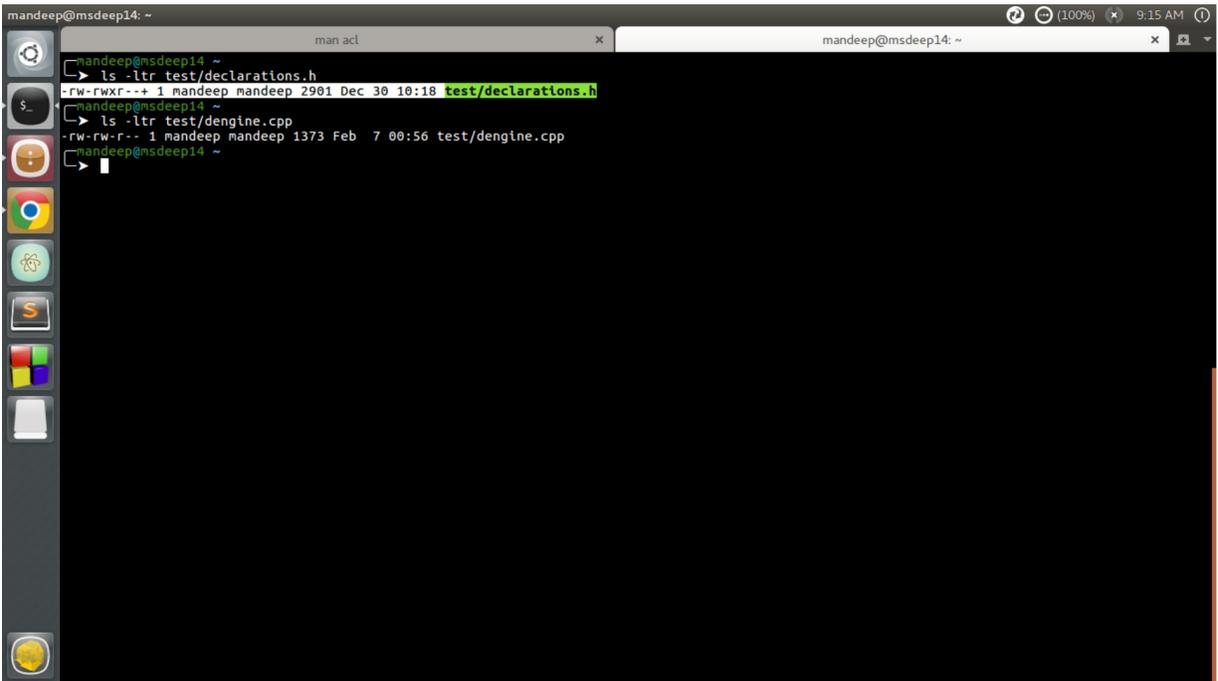
When you look at the first command in the above image, there is a plus sign immediately at the end of the ACL's permissions. This is an indication that there are some extra permissions that you can set in the ACL, and you can do this using the getfacl command.

Using Default ACLs

The default ACL uses a specific permission type that is assigned to the directory where you are making changes directly to the directory. This makes it easier for you to use the ACLs which come with your Linux. Let us see how you can use it. We are now going to create a directory or file and assign the default ACL to the file or directory using the option '-d' using the following command: $ mkdir test && setfacl -d -m u:dummy:rw test.

You now have an idea of what you can do to maintain security in your systems and server. The next two chapters shed light on how you can perform penetration testing and scanning to find any vulnerabilities in your server and network.

Chapter Ten: Downloading and Installing Kali Linux

If you want to perform an analysis of your system's security, you need to use the Kali Linux distro. This is a powerful tool you can use to assess the vulnerabilities in the system. In this chapter, we will look at how you can download and install the Kali Linux distro in your system and use various penetration testing tools which are built into the operating system. These tools will help any system administrator while conducting penetration tests in the various stages of the penetration testing lifecycle.

We have covered the details of how to install an operating system onto your system using a virtual machine, but let us look at what you should do when you install the operating system directly onto your system. For those of you who have never installed an operating system ever, there is nothing to worry about, as this chapter will guide you with a detailed installation of the Kali Linux operating system. From the information in this chapter, you will learn how to install Kali Linux and where you can download the installation media from.

Kali Linux is a tool that you can use to check the system for any vulnerabilities. This operating system installs quickly on permanent media like a hard disk but can also be installed on a USB stick and live booted from it whenever required. This is a very convenient and portable tool in the toolkit of a system administrator. If you can access the local machine while you work as a system administrator, you can leverage the Kali Linux live disk to boot it into a locally available physical machine inside the target organization's infrastructure. There are over 400 tools and applications available in the Kali Linux operating system.

Downloading Kali Linux

Kali Linux is a distribution of the Linux operating system, and we discussed the same in the first chapter. This operating system is

available for free, and you can download the ISO image file from the official website. You may need to use a different system to download the ISO and then burn it onto a DVD or USB to ensure you install it onto your system. You can download the image from the following URL: https://www.kali.org/downloads/

If you need material to learn more about the configurations, advanced operations, and other special cases, you can find this information on the official Kali Linux website at

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

It is recommended that you register on the Kali Linux website to access the community where you can discuss your issues and learn more about how to overcome them.

Before you download the image file from the website, you need to ensure you select the right architecture. Your system architecture is 32-bit or 64-bit, and you need to choose the image which works for your system. Once you complete the download, you can use the image burning software to copy the Kali Linux installation media onto a DVD or USB stick.

In this chapter, we will look at how you can install Kali Linux using a USB drive and Hard disk using Live boots.

Hard Disk Installation

Once you start with the installation process, you need to place the DVD in the drive and plug the USB stick to install the media used to load the operating system. Depending on what you want to use, you should set up the boot priority in your computer's BIOS settings, so this installation drives through the right media.

Booting Kali Linux for the First Time

If you have managed to install the Kali Linux exe file from a USB stick or DVD, you will be given options on the screen about any

existing information about the operating system and any other operating system on your hard disk. It will also replace the files with Kali Linux. Other advanced options are using which you can load the operating system on part of your hard disk using your existing operating system. This is beyond the scope of the book. Let us now look at how you can install the operating system.

Setting the Defaults

The next few screens will have the default settings you need to use when you set up the Kali Linux operating system. You can choose various options, such as the language, location, and language for your keyboard. You need to select the settings which you need to apply to the region and device. You also need to click on the next option to proceed with the installation process. You will be given information about the progress of your installation.

Initial Network Setup

A screen will appear on your system, and you can use it to type the hostname. Ensure the word is unique. When you click next, the installation manager will request you to enter the fully qualified domain name. The installation manager will use this domain name to download and install Kali Linux on your network or server. You can skip this step if you need to while you install Kali Linux and run it as a standalone system. If you are unsure about what you need to do, you can leave the option blank and continue.

Password

On this screen, the installation manager will ask you to choose the password for the root account. The root account is a super or privileged account, and it can be used to own the system. The Kali Linux system comes with a default password for the root account, and this is 'toor.' It is recommended for you to change the password to the complexity of your choice. You also need to ensure the password you enter adheres to the following criteria: uppercase, lowercase, number, and symbol. Ensure to set up a complex

password to secure your system from getting accessed by the wrong hands. Once you choose the password, you need to click on continue to move to the next step in the installation process.

System Clock

Another screen prompt will appear on your screen, where you can choose to set the alarm clock. Now, select the time zone and continue with the installation.

Disk Partitioning

There are different methods you can implement when it comes to using partitions when you install Kali Linux using a hard disk. There is a lot of information one needs to know when it comes to disk partitioning. In this chapter, we will only look at the basic process that is called Guided Partitioning. Since we are using a Guided partition mechanism, you need to use the entire disk to install the operating system. Select the option and continue the process of installation.

On the next screen, you will obtain information about all the hard drives which are on your system. You will see only one hard drive in the list and not multiple drives since most systems only come with one hard drive. Choose the hard drive you want to use to install Kali Linux. Now, select Continue. On the next screen, the installer will prompt you to determine how you will use the available hard drive.

I am assuming you are a beginner reading this book and will guide you on how you should do this. You need to select the 'All Files' option and choose one partition. This will keep the process extremely simple. Once you select this, click continue. In the next section, you will be given all the options which you can use as an input. You will be given the details selected to review. If you are happy with the details you have provided, you can continue with the information. There is only going to be one primary partition where all the files and folders will be saved. The secondary partition is called a swap. The latter is used as the virtual memory system where you switch between the RAM and CPU and the files are moved between

these two locations. In simple terms, this is termed as buffer memory.

It is important to ensure all the swap partitions are only on Linux systems. This is the best way to encrypt the swap and protect the information in the swap. The swap needs to be the same size as the RAM that is installed on your system. Once this is done, you can select finish and move onto the next step. Once you are done with the selection, you can confirm the options selected by you. You will also be presented with a prompt to select yes and continue with the installation. You can change the partitioning scheme if you need to, but you can only do this when your operating system is live. This will damage your system. After clicking Continue, you will see a progress bar screen with the, and the installer will begin copying files to your hard disk. The time your system takes to complete the installation process is dependent on the hardware in your system.

Configuring the Packet Manager

When you finish copying the files onto the hard disk, you will receive a prompt that will ask you how you would like to configure the packet manager for your system. This package manager is especially important for your system, and it is used by the Kali Linux system when it needs to update the package repository based on the new updates made to the software. You need to use a network that mirrors the one that Kali Linux is sitting on since this is the only way you will learn about the package sources available for Kali Linux.

You now need to click on yes to continue the process of installation. You will also be prompted with another screen to specify the use of a third-party URL network package. This is again used when your Kali Linux system is part of a corporate system that stores a local repository for Kali Linux packages on its local server. If you do not want to fill in these details, you can leave it blank and continue with the installation process.

Installing the GRUB Loader

When you move onto the next screen, the installer will throw a prompt asking you to choose if you wish to install the GRUB bootloader when you run the Kali Linux system on your computer. The Grand Unified Bootloader, or GRUB, is the main screen that will appear on your screen when the Kali Linux operating system will boot up. The GRUB gives you a menu that you can use to move into the advanced settings before you boot the Kali Linux on your computer. You do not have to do this if you are an advanced user, but you need to install it if you are a beginner. Select Yes and click on Continue.

Completing the Installation

You are now at the end of the installation phase and will find the system's completion screen. Once this is done, you can click on Continue, and your system will automatically reboot. You can remove the installation DVD or use a USB stick if you need to before you reboot your system. At this point, you will see the Kali Linux welcome screen on your system. You need to log in using the root account you had initially set up and finally access Kali Linux.

USB Drive Installation

You can use a USB drive, thumb drive, or stick to install Kali Linux. This is a storage device, and you can plug this into the port of your system. It is recommended for you to use a USB drive with at least 10 GB storage space or more if you want to install Kali Linux on your system. Every new computer system will allow you to boot the Kali Linux operating system from a USB device. You can choose to set the option to boot priority for your USB device from the BIOS settings on your system. We will look at how you can use a USB drive to install Kali Linux on your Windows or Linux machine. You can look at the documentation provided on the Kali Linux website to understand this better.

When you use a USB drive, you need to remember two terms – persistence and non-persistence. The former is the system's ability to retain the modifications or changes you make to the file even after

you reboot the system. The latter refers to the fact that your system will lose its changes when you reboot the system. In this chapter, we will look at the persistent and non-persistent installation of Kali Linux on Linux and Windows operating systems, respectively. This way, you will learn both methods.

Windows Non-Persistent Installation

Before you move with the installation of Kali Linux using a USB drive through your Windows operating system, you need to download the Win32 Disk Imager from the following URL: https://sourceforge.net/projects/win32diskimager/

Once you download the ISO for Kali Linux like you did when you used the hard drive to install it, you can plug your USB drive into the system. Your current operating system will detect this automatically, and it will assign a driver to the file. You then need to launch a Win32 Disk Imager application and then click on the folder to browse through the different files and folders. You need to select the ISO for Kali Linux and download the file and click on the OK button. Select the drive letter you want to assign to the USB drive from the drop-down. You now need to click the write button, so your operating system will write the Kali Linux operating system onto your USB drive.

This process will take time, and this is dependent on your system's hardware. When the installer has completed moving the ISO to the USB drive, you need to restart your computer. Set the option to highest boot priority for the USB drive form the BIOS settings in your system. It is important to understand that each system has its own user interface for the BIOS settings depending on the manufacturer. Therefore, you need to select the boot priority settings carefully. Once you do this, you need to reboot the system and the first thing on your screen will be the Kali Linux boot menu. You can choose the Live option that is the first option when it comes to booting Linux from the USB drive directly.

Linux Persistent Installation

It is important to remember that the size of the memory you have matters, especially if you use a USB drive to install Kali Linux on your system. Depending on the type of operating system you use, you need to create a Kali Linux USB drive. You need to ensure that the GParted application is installed on your device before you work on installing Kali Linux. If you have trouble with installed GParted, you need to read the documentation and see what you should do to get rid of any errors during installation. You can use any of the following commands in the terminal to install this tool:

apt-get install gparted

aptitude install gparted

yum install gparted

Once you have GParted downloaded on your system, you need to download the Kali Linux ISO from the official website and plug the USB drive onto your computer system. You need to use the command below in the Linux terminal if you want to see where the USB drive is present.

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

The file in the USB drive will be saved using the name /dev/sdb1. You must ensure you look at the right file when you install Linux on your system since the file can be different from one system to the next. In the following command, you can remove the numbers at the end to ensure you switch between file names.

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

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

Launch Gparted application using the following command.

gparted /dev/sdb

You should now have one partition in your drive which has the Kali Linux image on it. The next thing to do is create another partition in the drive by right-clicking on the drive and selecting the 'New' option from the menu. This will appear once you select the partition menu available in the Menu bar. The following are the steps you need to follow, and they may vary depending on the machine you use:

- The unallocated space in the drive is greyed out
- You should now select the new option from the partition using the drop-down menu
- You can specify the size of the drive using a graphical slider
- Now, choose the file system and update it to ext4
- Select the add option and click on the drop-down menu. You need to select the option to apply all the operations on your system
- When you see a prompt, click ok, and the settings will update

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

mkdir /mnt/usb

mount /dev/sdb2 /mnt/usb

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

umount /mnt/usb

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

Chapter Eleven: The Penetration Testing Life Cycle

As a system administrator, you need to perform penetration testing in your organization to ensure you have the right security enabled in your network and server. In this chapter, we will look at the different stages used in penetration testing. Using this chapter, you will learn more about system administrators' different tools and the processes they need to follow during each stage. This way, you will understand the five stages of the penetration testing lifecycle and have an idea of the tools used by security professionals while engaging in penetration testing.

The Five Stages of the Penetration Testing Life Cycle

In this section, we will look at the five stages in the penetration testing lifestyle, and the information is broken down easily to help you understand what exactly is expected out of you during each stage.

Stage 1: Reconnaissance

This is the first step in the penetration testing phase. Let us assume you are running a military operation. The officers and analysts are going through the foreign territory map, and others in a different room are looking at the news and trying to see what can be done to take down the enemy. Another group is working on the information they need to collect to ensure the team can move into the enemy territory and make it their own. You need to do this when you work on a penetration test during your ethical hacking process.

If you do not have the expertise to run a penetration test, the organization will hire a team to perform this test. During this phase, you need to discover the information about the target system and also gather information about the system using public and private sources. You can do this easily by looking for information about the

Internet since most information is publicly available. During this stage, you need only to understand what is present in the target's network and server. You do not breach the network and server since you only have to scan and document the information you will need while performing the next few steps.

Stage 2: Scanning

Let us consider that you are on a military mission with a team of people, and there is a hilltop you need to reach. This hilltop is behind your enemy lines, and one of your soldiers is hidden in the bushes. This soldier will come back and give you information about the enemy camp. The objective of this mission is for you to determine the type of activities the enemy is performing. This soldier will also tell you about the different ways you can move into enemy land and the security that is around the camp.

This soldier was told what he needed to do for him to get the information he needed. He was told what he had to look at. This is exactly what you do in the reconnaissance stage. You gather information, and it is this information you use during the scanning stage to determine which server and network you need to scan to find any vulnerabilities. You can use various tools to scan the target network, and Kali Linux comes with in-built options. You need to use the information you collect during this stage during the exploitation phase to determine which areas you need to exploit so that you can extract information.

Stage 3: Exploitation

If you are performing the penetration testing with a team, you need to ensure you move through the network and server easily without being detected. You also need to find a way to enter the server without getting caught. You need to find the right gaps in the server and enter the system and network through the server's open door. You also need to spend time inside the server and see what information you can extract from the system. You need to do this during the exploitation stage. The objective is to ensure you quickly

enter and exit the network and server with the information you need without being detected by anybody. During this stage, you need to exploit the system and find sensitive information about the business. You can do this repeatedly if you need to.

Stage 4: Maintaining Access

When you perform the penetration test, you must ensure you have unlimited access to the servers and network you are using. You need to ensure there is access to all the information you need. As the system administrator, you need to find a way to keep access while you discover how to enter the target system and network. You also need to find a way to exploit the server and see what information you can obtain or access through the network. You also need to find a way to get in and out of the system without getting caught. Therefore, with the information gathered in the exploitation state, they automate a way to keep their access continued to the target system.

Stage 5: Reporting

When you perform penetration testing on your system and server, you need to stand in front of the entire team and the higher-ups to tell them what you learned from the penetration test you performed. You need to explain every step and detail everything you found during the test. You need to expand the details of your findings. At the end of the penetration testing lifecycle, you also need to prepare a report which explains each phase of your penetration test. You need to explain the loopholes discovered, the vulnerabilities exploited and the servers, networks and systems targeted during the test. In some cases, you may need to provide information about the findings. You need to ensure management will look at the different means they can use to protect their servers and networks.

Chapter Twelve: Scanning

In this chapter, you will learn about the second stage of penetration testing, and this is the most important step since you will learn more about how to scan the servers and see what can be done to identify any vulnerabilities. In this stage, you need to take input from the discoveries made during the reconnaissance stage and gather information about the operating system and the users who use the information on that system. When you perform the testing as a system administrator, you can move back to the reconnaissance stage to see if there is any new information you need to obtain about the processes and people.

This stage's objective is for you to scan the information in the network and server and identify the information about the target. You can learn more about your information and network systems. During this stage, you need to focus on obtaining information about live hosts, device types(laptop, desktop, router, mobile, etc.), operating systems, software, public-facing services offered(SMTP, FTP, web applications, etc.). You can use this stage to remove any basic vulnerabilities in the system. These vulnerabilities are easy for one to detect during the scanning stage. You can use different tools in the scanning process, but we will look at the main tool Nmap that is used to perform this process. This stage's objective is for you to gather the information you can pass onto the next step of the ethical hacking process.

Network Traffic

You need to learn more about network traffic and how it works for you to understand the different tools and processes used in this stage. The communication which takes place between two devices over a network can only happen because of network traffic. The most popular modes of network traffic are wireless ethernet and wired ethernet. In this section, we will look at the main aspects of network traffic: firewalls and ports, and see how you can use them to improve your systems' security.

Firewalls and Ports

One of the main reasons why organizations have firewalls is to protect the systems, network, and server used to transfer information. You can protect the internal server and network on your system and server to ensure the communication between external and internal networks is secure. A firewall can is software or hardware which has rules to serve as a gatekeeper to a network. The firewall has access controls defined in them, enabling you to monitor the inbound traffic called outbound and ingress traffic. This is termed egress. The traffic that satisfies these rules ensures the firewall is never dropped or discarded during a hack. This is done by opening and closing ports on the firewall that allow or reject traffic.

We have looked at what ports are and how they are used and adjusted in the Linux operating system earlier in the book.

PING

Ping is an ICMP-based application to which you and every other user in the system or server is exposed to. When you use the ping command, you can send a code 0 and type 8 packet, indicating that the packet was just an echo. Systems that receive this package will instantly respond with a type 0 code 0 packet, an echo reply. A successful ping indicates to the system that the ping was made only on a live network. This means that you are working out of a live host. When you use the ping command, you can use the Windows command prompt. The ping will send the request at least four times by default. If you use this ping in the Linux terminal, the command will continue to run until you interrupt it.

Let us look at a successful and unsuccessful ping command.

If the host being pinged is Live

Ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

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

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

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

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

If the host is unreachable

Ping 192.168.1.200

Pinging 192.168.1.200 with 32 bytes of data:

Reply from 192.168.1.129: Destination host unreachable.

Reply from 192.168.1.129: Destination host unreachable.

Reply from 192.168.1.129: Destination host unreachable.

Reply from 192.168.1.129: Destination host unreachable.

Ping statistics for 192.168.1.200:

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

Traceroute

If you use the traceroute command, you will see that the ICMP ping command is used to determine the number of devices that lie between the system and the network. This is one way for it to initiate the trace on the target system. The traceroute command functions by manipulating the Time To Live value of a network packet, also known as TTL. This term indicates the number of times a packet of data is moved through a network and is broadcasted repeatedly by the host before the packet of data expires.

On Linux-based systems, the command to run a traceroute is traceroute. If you want to run the command on Windows, you can do

it to check the vulnerabilities in the system and network. Let us take an example of a traceroute to google.com

tracert www.google.com

Tracing route to www.google.com [74.125.227.179]

over a maximum of 30 hops:

1 1 ms<1 ms 1 ms 192.168.1.1

2 7 ms 6 ms 6 ms 10.10.1.2

3 7 ms 8 ms 7 ms 10.10.1.45

4 9 ms 8 ms 8 ms 10.10.25.45

5 9 ms 10 ms 9 ms 10.10.85.99

6 11 ms 51 ms 10 ms 10.10.64.2

7 11 ms 10 ms 10 ms 10.10.5.88

8 11 ms 10 ms 11 ms 216.239.46.248

9 12 ms 12 ms 12 ms 72.14.236.98

10 18 ms 18 ms 18 ms 66.249.95.231

11 25 ms 24 ms 24 ms 216.239.48.4

12 48 ms 46 ms 46 ms 72.14.237.213

13 50 ms 50 ms 50 ms 72.14.237.214

14 48 ms 48 ms 48 ms 64.233.174.137

15 47 ms 47 ms 46 ms dfw06s32-in-f19.1e100.net [74.125.227.179]

Trace complete.

You can use different tools on Kali Linux to run these traces, and these tools use the ICMP, TCP, and UDP protocols to scan the target systems and networks. The result of a successful scan will give you information such as operating systems, network hostnames, IP addresses, and services operated on the network. Some scanning tools can also be used to discover any vulnerabilities in the server and network. The details gathered in the scanning stage can be used in the exploitation stage to attack specific targets.

Nmap: The King of Scanners

The Nmap scanning tool is one of the most popular scanning tools used by system administrators since it is the easiest way to help you list down all the active hosts present on the target network. You can also use it to determine operating systems, services, ports, and even user credentials in some cases. This tool uses a combination of options, switches, and commands to find the details and vulnerabilities in your system during the scanning stage of this lifecycle.

Timing Options

We have learned above that the default timing option in the Nmap scan does not specify anything, but you can use the default value or choose from one of the options below. There is a feature in Nmap through which the user can specify the timing option he wants to use. This option can be used to override the default time option used in the tool. You can either choose to expedite the process or slow the process down if you need to.

Using this timing template, you can enable various settings, especially the one where you add a delay between the scanning and parallel processing of the ports. The different timing templates can be explained using the options scan_delay, max_scan_delay, max_parallelism. We can use these options to measure every timing template so that an appropriate timing template is used for scanning a target network.

You can use the can_delay option if you need to set the probes in the target system to a minimum number. You can use the max-scan_delay to define the scanner's maximum time between delays made while scanning the ports and IP addresses in the server and network. If you ask why this is important, it is because certain systems respond to probes only at a specific rate. When you use these options, you will adjust to the different probes and find a way to meet the system's requirements that you are scanning. The max_parallelism option allows Nmap to send scan probes one at a time or in serial or in parallel. Let us look at the different timing options you can use in the Nmap tool.

-T0 Paranoid

When you use this timing option, the scan is performed slowly, and the network links are slow. You may get detected when you run these scans on your Linux network or server. Using this timing option, the scan will work serially and pause every 5 minutes. The max_delay setting is ignored during the scan when you use this timing template since the base scan_delay has a higher value than the default.

-T1 Sneaky

This timing method is used to perform a sneaky scan of the network and server. This is better and slightly faster than the previous timing by maintaining your discretion. This scan also serially scans the target system but reduces the scan_delay to about 15 seconds. The scan_delay is reduced in number, but since the value is higher, Nmap will ignore max_scan_delay.

Target

The target used in an IP address is an important part of the Nmap command string used, and if you end up using an incorrect target, you may end up scanning empty IP systems or spaces. You cannot do this as per the regulations. There are several ways to set a target

for the Nmap scan, and we will look at the two common methods used to do this: IP address range and scan list.

IP Address Range

Using IP Address ranges to define targets in the system is an easy process to define the range or port you want to use. Let us take an example of a class C IP address range for our example. If you use the C IP address, you can run the scan on 254 different hosts. To do this, you can use the command below. Using this, you can scan all the hosts on a particular IP address range belonging to class C.

nmap 10.0.2.1 -255

You can use the Classless inter-domain routing (CIDR) to run the same scan on the server or system's ports. CIDR is a quick way to specify an IP address range, but this is something beyond this book's scope.

nmap 10.0.2.1/24

If the IP address being used is very small, you can use a smaller range to define the target used in the scan. For instance, if you want to scan the IP addresses within the range, you can use the following command: nmap 10.0.2.1 -50

Scan List

You can use text files as inputs when you need to use the Nmap command to scan the list. The file will include the IP addresses which are present in your target server or system. You can choose to use the following IP addresses and store them in the target text file if you need to.

10.0.2.1

10.0.2.15

10.0.2.55

10.0.2.100

The syntax of the above command is as below:

nmap -iL target.txt

Port Selection

The Nmap command structure allows you to determine the ports you want to use by using the -p switch. This will help you determine the port you want to scan. You can either specify a single port or a range of ports depending on what you need to scan.

nmap -sS -p 1-100

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

You can also choose to combine both commands like the example below: nmap -sS -p 1-100, 53, 25, 143, 80

Output Options

The results of a scan you perform on the network and servers will scan the Nmap command results. You can print the information on the terminal window, but it is not always a good idea to do this. As the administrator, you need to save the file down with the output, so you can use it to determine how to remove any vulnerabilities in the system. You can redirect the output from the scan and send it to a file. There are some built-in commands you can use if you prefer, and this allows you to redirect the output and move it onto a file. Let us go with each of these options.

-oN Normal Output

You can use this output option to create a normal text file to ensure the output is stored in the form of a text file. You can use this file to evaluate the output. You can also use it as an input key for other programs: nmap -oN output.txt 10.0.2.111

-oX Extensible Markup Language(XML) Output

Some applications and tools use XML files as their input when they perform a penetration test, and therefore, this option is extremely easy to use. You can also store the output in an XML format using the following command: nmap -oX output.txt 10.0.2.111

-oS Script Kiddie Output

The output files from a script kiddie attack cannot be used when you perform penetration testing, but these are a good way to determine how good the security in your network and server is. You cannot use the output from the following syntax for any industrial use.

nmap -oS output.txt 10.0.2.111

Nmap Scripting Engine

You need to learn how to build a custom script in Nmap if you do not want to use the built-in packages. If you are willing to use the preconfigured penetration tests in Nmap, you can use the following URL: https://nmap.org/nsedoc/ .

For instance, you can use this script to fetch the MAC address and the NetBIOS, each of which is important information you need for the target system. You can use the flag '—script' as per the below example, along with the Nmap command followed by the script name.

nmap --script nbstat.nse 10.0.2.111

As a system administrator, you must ensure you have a script database and update it regularly. It is important for you to update the Nmap script as well every time you perform a new penetration test on your server or network. To do this, use the following command: nmap --script -updatedb

Conclusion

If you are a system administrator or engineer trying to learn more about Linux, then you found the right book. This book included all of the information you needed about Linux and how you can use it on your system or a virtual machine. You learned about the different distribution systems of Linux and how every distro differs from the other.

This book covered the different ways to encrypt and decrypt information. It also provided information about the different methods you can use to secure the server and the files and folders in the network and system. You learned about the different ways to use an access control list to manage how users access the system. It is important to take care of the access users have to the server and network since these individuals play a key role in taking care of the system's information. You learned more about the different ways to manage access control and discovered how you can manage privileges in the system. By the end of the book, you were able to learn to improve your network security, including the different methods you can use to test the system, and how to look for vulnerabilities.

Now it's time to dive in and keep your system up to date and safe!

References

7 Tools to Encrypt/Decrypt and Password Protect Files in Linux . (2015).
Tecmint.com. https://www.tecmint.com/linux-password-protect-files-with-encryption/

16 Ways to Secure a Linux Server . (2019, March 26). Liquid Web.
https://www.liquidweb.com/kb/security-for-your-linux-server/

Access Control Lists(ACL) in Linux - GeeksforGeeks . (2018, May 2).
GeeksforGeeks. https://www.geeksforgeeks.org/access-control-listsacl-linux/

comments, 08 O. 2019 P. H. M. F. 92up 6. (n.d.). *7 steps to securing your Linux server* . Opensource.com. https://opensource.com/article/19/10/linux-server-security

Controlling Unix & Linux Account Privileges: 9 Best Practices | BeyondTrust .
(n.d.). Www.beyondtrust.com. Retrieved from
https://www.beyondtrust.com/blog/entry/controlling-unix-linux-account-privileges-9-best-practices

Hoffman, C. (n.d.). *Why You Shouldn't Log Into Your Linux System As Root* .
How-to Geek. Retrieved from https://www.howtogeek.com/124950/htg-explains-why-you-shouldnt-log-into-your-linux-system-as-root/

How to manage Linux user account security - Tutorial . (n.d.). UpCloud.
Retrieved from https://upcloud.com/community/tutorials/manage-linux-user-account-security/

How to Setup Encrypted Filesystems and Swap Space Using "Cryptsetup" Tool in Linux - Part 3 . (n.d.). Www.tecmint.com. Retrieved from
https://www.tecmint.com/disk-encryption-in-linux/

s, R. (n.d.). *Encryption Methods in Linux | Unixmen* . Retrieved from

https://www.unixmen.com/encryption-methods-linux/

skenlon. (n.d.). *Secure your Linux network with firewall-cmd* . Enable Sysadmin.

Retrieved from https://www.redhat.com/sysadmin/secure-linux-network-

firewall-cmd

The Best Linux Operating Distros . (2019, February 3). MUO.

https://www.makeuseof.com/tag/best-linux-distributions/