Introduction

What is Linux operating system and how it ties in with ethical hacking. We will explore the Linux distributions that have been designed with hacking in mind and see how hackers can leverage their inherent strengths to become ethical hackers. We will also discuss some essential skills that ethical hackers will be required to master for Linux OS.

Why is Linux good for ethical hackers?

The concept of Linux for ethical hackers focuses on the use of the Linux operating system for the sole purpose of ethical hacking. There are a couple of skills that hackers must equip themselves with as they approach hacking using Linux, because a good number of devices that they will be hacking into will be Linux devices and a large percentage of tools in existence today are Linux-based.

There are a number of reasons that hackers will need to use Linux. We'll look at some of these next.

Why do hackers use Linux?

In order to familiarize yourself with the full range of ethical hacking tools, it is important to be conversant with the Linux OS. As the systems engineer suggest: "In Linux you need to understand from the basics to the advanced, learn the console commands and how to navigate and do everything from your console, also shell programming (not a must, but always preferable), know what a kernel is and how it works, understand the Linux file systems, how to network on Linux."

Hackers will want to utilize Linux for hacking for a wide number of reasons. These include the following:

Linux is open-source

The ability to manipulate Linux source code to your liking is one of the reasons why security enthusiasts opt for this over Windows. This is especially worth remembering today, where privacy concerns with major corporations is a concern.

Linux is transparent

We are able to understand the inner workings of Linux because we have access to its entire code. We can manipulate how each component of the operating system works. This is something that operating systems such as Windows don't allow for.

Linux offers granular control

Linux allows us to quickly and easily program certain aspects of the OS, using scripting languages such as BASH or even Python. Windows, on the other hand, hinders you from

accessing certain parts of the OS.

Most hacking tools are built for Linux

A good percentage of hacking tools are written for Linux. This is because using scripting languages such as BASH and lightweight languages such as Python makes it easy to write minimal code that accomplishes a lot. Today, over 90% of hacking tools available are written for Linux.

The future is in Linux

As technology advances, embedded systems are relying on the Linux kernel due to its efficiency and light weight. More and more devices are getting connected to the internet by the day, and people are embracing the Internet of Things. These devices rely on Linux and require being secured on the internet.

The reasons above have attracted most of the security industry to rely on Linux for ethical hacking. So now that we know why Linux is the most favored, why don't we see how we can be able to run it on our own?

How can one run Linux for ethical hacking?

Linux can be installed and run from your computer or within a virtual machine environment such as VirtualBox. There are a few ethical hacking Linux distributions that you can choose to run. The most common include:

1. Kali Linux: This is the most popular hacking OS. It is Debian-based and is maintained by Offensive Security. It includes numerous hacking tools, making it the most desirable hacking OS

2. Black Arch: This is an Arch Linux-based hacking OS with over 2,300 hacking tools incorporated within it. Even though it has more tools than Kali, it is a relatively new project and thus less popular at the moment. This also means that it is less stable compared to Kali

3. Parrot OS: This is another Debian-based hacking OS. It has hacking tools for a wide variety of security projects, from pentesting to digital forensics

4. Santoku Linux: Santoku Linux is a mobile security-based Linux distribution, with tools specific to mobile security

5. BackBox Linux: This is a Debian-based Linux distribution that focuses on being incredibly lightweight

   Of the distributions above, the most commonly used one is Kali Linux. This is what we shall be using in this article. You can access the Kali documentation here to learn more about it, and there's a detailed guide on how to install Kali Linux on VirtualBox here.

   It is advisable that you first begin by installing Kali Linux on VirtualBox and learning how to

use it there before you are confident enough to make it your daily driver. As engineer Sylvain Leroux advises on It's FOSS: "Some commands may be potentially harmful to your home network. In addition, by not understanding the implications of what you are doing, you may put yourself in a difficult situation by using those tools at your work, school or on public networks. And in that case, ignorance will not be an excuse."

What are some basic commands in Linux?

There are some basic commands that you should be conversant with as you grow in your understanding of Linux. Since we are discussing Kali Linux in this article, we shall focus on the Debian-based packages and commands. We decided to distinguish between the different commands and place them according to the categories discussed below.

1. **Managing the file system**: The Linux file system includes files and folders that comprise the system. You can navigate this file system using the Linux terminal as opposed to the GUI. Managing the system through the terminal allows you to quickly and powerfully interact with the system. The following are some of the commands that could be used within this category:

- **pwd:** This command shows you where you are currently working from within the system
- **ls**: This command shows you the contents of the current directory
- **whereis**: This command can be used to locate installed binaries within the system
- **locate**: This command is used to find files within the system
- **find**: This command allows you to find files within the system in a more granular manner
- **rm**: This command allows you to rename or remove files and directories within the system
- **cp**: This command allows you to copy files and directories from one location to another within the system

2. **Managing files within the system:** It is possible to manage input and output from files within the Linux system. The following commands and programs can be used:

- **cat**: This command outputs the contents of a file. It can also be used to feed the contents of a file into another file by combining it with the > operator
- **head**: This command outputs the contents of a file from the beginning, giving output to the first 10 lines only
- **tail**: This command outputs the contents of a file from the bottom, giving output of the last 10 lines of the file
- **grep**: This command can be used to filter the contents of a file to match a particular regex
- **nano**: This program can be used to edit file contents. It is one of the available text editors

operating from the Linux terminal

- **vi**: This program can be used to edit file contents. It is one of the available text editors operating from the Linux terminal

3. **Adding and removing software**: The Linux OS allows you to manage software using the terminal. This is in contrast to the Windows OS, which relies on installation binary packages. Even though there are also installation packages in Linux, the following are the main ways that software can be managed:

- **APT package manager**: The APT package manager uses the program **apt-get** to install, remove, reconfigure and fix broken packages within the Linux system

- **Aptitude package manager**: The aptitude package manager uses the program **aptitude** to manage (install and remove) software

- **DPKG package manager**: This software manager uses the program **dpkg** to manage software packages within the Linux system

4. **Managing the network**: Managing the network is an important skill that can involve multiple tools and programs which beginners in ethical hacking should master. Some of these commands are listed below:

- **ifconfig** and **iwconfig**: These commands can be used to bring up or take down the network interfaces — ifconfig for the Ethernet interface and iwconfig for the wireless interface

- **tcpdump**: This command can be used to analyze network traffic for various purposes and to capture network traffic into a file that can later on be thoroughly analyzed for specific traffic

5. **Controlling file and directory permissions**: One of the most important skills for hackers is to be able to control access to files and directories. This can be a deep topic, so we have decided to include this introductory piece on Linux file and directory permissions. The following commands can be used to manage permissions within Linux:

- **chown**: This command can be used to change the ownership of files and directories from one user to another

- **chgrp**: This command is used to change the ownership of files and directories from one group to another

- **chmod**: This command can be used to change the general permissions of a file or directory

It is also important for beginner hackers to understand how to manage running processes, manage user environment variables, manage and discover wireless networks, go anonymous using proxies, VPNs and TOR, write basic scripts and understand the Linux logging system. However, these are skills that beginners will have to cumulatively acquire as they advance their understanding of Linux.