**Linux Basics – 1**

Source: Linux Basics for Hackers

**Why use Linux:**

* Open source, can be changed and manipulated.
* Allows better understanding of OS.
* Granular control, allows far greater control over system than e.g Windows.
* Used in 2/3 of web servers.
* iOS = Unix, Android = Linux. 80% of mobile devices run Unix/Linux. Windows = 7%.

I’m using a Raspberry Pi 5 (4GB) running Kali Linux 2024.1, (Kali GNU/Linux Rolling).

<https://www.kali.org/docs/virtualization/install-virtualbox-host/>

**Some Basic Terminology:**

**Binaries** This term refers to files that can be executed, similar to executables in Windows. Binaries generally reside in the */usr/bin* or *usr/sbin* directory and include utilities such as ps, cat, ls, and ifconfig (we’ll touch on all of four of these in this chapter) as well as applica- tions such as the wireless hacking tool aircrack-ng and the intrusion detection system (IDS) Snort.

**Case sensitivity** Unlike Windows, the Linux filesystem is case sensi- tive. This means that *Desktop* is different from *desktop*, which is different from *DeskTop*. Each of these would represent a different file or directory name. Many people coming from a Windows environment can find this frustrating. If you get the error message “file or directory not found” and you are sure the file or directory exists, you probably need to check your case.

**Directory** This is the same as a folder in Windows. A directory pro- vides a way of organizing files, usually in a hierarchical manner.

**Home** Each user has their own */home* directory, and this is generally where files you create will be saved by default.

**Kali** Kali Linux is a distribution of Linux specifically designed for penetration testing. It has hundreds of tools preinstalled, saving you the hours it would take to download and install them yourself. I will be using the latest version of Kali at the time of this writing: Kali 2018.2, first released in April 2018.

**root** Like nearly every operating system, Linux has an administrator or superuser account, designed for use by a trusted person who can do nearly anything on the system. This would include such things as recon- figuring the system, adding users, and changing passwords. In Linux, that account is called *root*. As a hacker or pentester, you will often use the root account to give yourself control over the system. In fact, many hacker tools require that you use the root account.

**Script** This is a series of commands run in an interpretive environ- ment that converts each line to source code. Many hacking tools are simply scripts. Scripts can be run with the bash interpreter or any of the other scripting language interpreters, such as Python, Perl, or Ruby. Python is currently the most popular interpreter among hackers.

**Shell** This is an environment and interpreter for running commands in Linux. The most widely used shell is bash, which stands for *Bourne- again shell*, but other popular shells include the C shell and Z shell. I will be using the bash shell exclusively in this book.

**Terminal** This is a command line interface (CLI).

**Linux Filesystem**

Linux doesn’t have a physical drive (such as the *C:* drive) at the base of the filesystem but uses a logical filesystem instead. At the very top of the file- system structure is */*, which is often referred to as the *root* of the filesystem,

A diagram of a computer system

Description automatically generated

***/root*** The home directory of the all-powerful root user  
***/etc*** Generally contains the Linux configuration files—files that con-

trol when and how programs start up ***/home*** The user’s home directory

***/mnt*** Where other filesystems are attached or mounted to the filesystem

***/media*** Where CDs and USB devices are usually attached or mounted to the filesystem

***/bin*** Where application *binaries* (the equivalent of executables in Microsoft Windows or applications in macOS) reside

***/lib*** Where you’ll find *libraries* (shared programs that are similar to Windows DLLs)

**Commands:**

* Use one dash for letter arguments, two dashes for words. E.g <filename> -h vs <filename> --help

Root Privileges

Print working Directory pwd

Check User whoami

Create File touch <filename>

CPU Info lscpu

List contents long ls -l

Help file <filename> --help

**Finding Stuff**

Locates occurences of word locate <word>

Finds binary files whereis <>

Finds binary file in PATH which <>

Most powerful search is ‘find’ which starts at a given location and looks for all occurrences within directories contained at given location.

kali >**find /[1]-type f [**2]-**name apache2**[3]

First I state the directory in which to start the search, in this case / [1]. Then I specify which type of file to search for, in this case f for an ordi- nary file [2]. Last, I give the name of the file I’m searching for, in this case apache2 [3].