**Chapter 1**

**\* Some important terms:**

**1-**Binaries:

This term refers to files that can be executed.

Binaries generally reside in the */usr/bin* or *usr/sbin* directory.

2- Case sensitivity:

Unlike Windows .

Linux is case sensitive. This means that *Desktop* is

different from *desktop ,* which is different from *DeskTop*. Each of these would represent a different file or directory name .

3-Directory :

This is the same as a folder in Windows.

4- Home :

Each user has their own */home* directory, and this is generally where files you

create will be saved by default

5- Kali :

Kali Linux is a distribution of Linux specifically designed for penetration testing.

6- 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.

7- Script :

This is a series of commands run in an interpretive environment that converts

each line to source code.

8- Shell :

This is an environment and interpreter for running commands in Linux.

9-Terminal :

This is a command line interface (CLI).

**The Linux Filesystem**



**The root (/) :**

**of the filesystem is at the top of the tree, and the following are the most**

**important subdirectories to know:**

/root :

The home directory of the allpowerful

root user

/etc :

Generally contains the Linux configuration files—files that control 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)

reside

/lib :

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

**BASIC COMMANDS IN LINUX**

1. Finding Yourself with ( pwd )

The *present working directory* command, pwd, returns

your location within the directory structure.

EX:

kali >pwd

/root

1. Checking Your Login with ( whoami )

you can use the whoami command to see which user you’re logged in

EX :

kali >whoami

root

1. Navigating the Linux Filesystem ( cd )

* To change directories from the terminal, use the *change directory* command, cd
  + kali >cd /etc
  + root@kali:/etc#
* To move up one level in the file structure (toward the root of the file structure, or */*), we use cd followed by double dots (..), as shown here:
* root@kali:/etc# cd ..
* root@kali:/# pwd
* /
* root@kali:/#

you can move up as many levels as you need. Just use the same number of doubledot

pairs as the numberof levels you want to move:

kali >cd .. ..

1. Listing the Contents of a Directory with (ls)

To see the contents of a directory , we can use the (ls)

EX:

kali >ls

kali >ls –la : To show hidden files .

1. Getting Help (--help , -h )

To find information about the command use .

EX:

kali >aircrack-ng --help

kali >nmap –h

1. Referencing Manual Pages with ( man )

In addition to the help switch, most commands and applications have a manual (man) page with more information, such as a description and synopsis of the command or application. You can view a man page by simply typing man before the command .

EX: kali >man nmap

FINDING STUFF

1. Searching with (locate)

Probably the easiest command to use is locate. Followed by a keyword denoting what it is you want to find, this command will go through your entire filesystem and locate every occurrence of that word.

EX:

kali >locate aircrack-ng

1. Finding Binaries with (whereis)

If you’re looking for a binary file, you can use the whereis command to locate it.

**EX:**

kali >whereis aircrack-ng

1. Finding Binaries in the PATH Variable with (which)

It only returns the location of the binaries in the PATH variable in Linux.

EX:

kali >which aircrack-ng

1. Performing More Powerful Searches with (find)

The find command is the most powerful and flexible of the searching utilities.

EX:

kali >find / -type f -name apache2

1. Filtering with (grep)

Very often when using the command line, you’ll want to search for a particular keyword. For this, you can use the grep command as a filter to search for keywords.

1. PS COMMAND

The ps command is used to display information about processes running on the machine.

EX :

kali >ps aux

kali >ps aux | grep apache2 : I can do this by piping the output from ps to grep and searching for a keyword. For instance, to find out whether the apache2 service is running .

MODIFYING FILES AND DIRECTORIES

1. Creating Files (cat)

The cat command followed by a filename will display the contents of that file

EX:

Kali : cat > name\_file : creat new file and show it .

Kali : cat (old file ) : that file creat before

1. File Creation with (touch)

This command creat a new file for writing in it .

EX :

kali >touch newfile

1. Creating a Directory (mkdir )

The command for creating a directory in Linux is mkdir, a contraction of *make directory* To create a directory named *newdirectory*, enter the following command:

EX :

kali >mkdir newdirectory

1. Copying a File(CP)

To copy files, we use the cp command. This creates a duplicate of the file in the new location and leaves the old one in place.

EX :

kali >touch oldfile

kali >cp oldfile /root/newdirectory/newfile

1. Renaming a File (MV)

* This command use to rename :

kali >mv newfile newfile2

* And cat file

1. Removing a File (rm )

To remove a file, you can simply use the rm command, like so:

EX:

kali >rm newfile2

1. Removing a Directory

The command for removing a directory is similar to the rm command for removing files but with dir (for directory) appended, like so:

EX :

kali >rmdir newdirectory : This command don’t remove file because directory not empty .

kali >rm -r newdirector : this remove anyfile .

**Chapter 2**

**VIEWING FILES**

1. Taking the (Head)

If you just want to view the beginning of a file, you can use the head command. By default, this command displays the first 10 lines of a file.

EX :

kali >head /etc/snort/snort.conf

kali >head -20 /etc/snort/snort.conf : This command show first 20 line in /etc/snort/snort.conf

1. Grabbing That (Tail)

The tail command is similar to the head command, but it’s used to view the last lines of a file let’s use it on *snort.conf*:

EX:

kali >tail /etc/snort/snort.conf

kali >tail -20 /etc/snort/snort.conf : same Head

1. Numbering the Lines (nl)

To display a file with line numbers, we use the nl (number lines) command

EX :

kali >nl /etc/snort/snort.conf

1. FILTERING TEXT WITH GREP

EX :

* cat /etc/snort/snort.conf | grep output : Cat show all line in snort.conf and grep searsh in result about “ output “

1. USING SED TO FIND AND REPLACE

* kali >cat /etc/snort/snort.conf | grep mysql
* kali >sed s/mysql/MySQL/g /etc/snort/snort.conf > snort2.conf :

The s command performs the search: you first give the term you are searching for (*mysql*) and then the term you want to replace it with (*MySQL*), separated by a slash (/). The g command tells Linux that you want the replacement performed globally. Then the result is saved to a new file named *snort2.conf*. Now, when you use grep with *snort2.conf* to search for *mysql*, you’ll see that no instances were found, but when you search for *MySQL*, you’ll see two occurrences.

1. VIEWING FILES WITH (MORE) AND (LESS)

MORE

The more command displays a page of a file at a time and lets you page down through it using the ENTER key

EX :

kali >more /etc/snort/snort.conf

1. Displaying and Filtering with (less)

The less command is very similar to more, but with additional functionality—hence, the common Linux aficionado quip

EX :

kali >less /etc/snort/snort.conf

**Chapter 3**

**ANALYZING AND MANAGING NETWORKS**

This chapter shows you some essential Linux tools for analyzing and managing networks during your network hacking adventures.

1. ANALYZING NETWORKS WITH (IFCONFIG)

You can use it to query your active network connections by simply entering ifconfig in the terminal.

EX :

* kali >ifconfig
* ➊eth0Linkencap:EthernetHWaddr 00:0c:29:ba:82:0f
* ➋inet addr:192.168.181.131 ➌Bcast:192.168.181.255 ➍Mask:255.255.255.0
* *snip*
* ➎lo Linkencap:Local Loopback
* inet addr:127.0.0.1 Mask:255.0.0.0
* *snip*
* ➏wlan0 Link encap:EthernetHWaddr 00:c0:ca:3f:ee:02

1. which is short for Ethernet0
2. Your (IP) The second line contains information on the IP address currently assigned to that network interface
3. the Bcast or broadcast address
4. which is used to determine what part of the IP address is connected to the local network.
5. which is short for *loopback address* and is sometimes called *localhost*.
6. This appears only if you have a wireless interface or adapter .
7. CHECKING WIRELESS NETWORK DEVICES WITH (IWCONFIG)

If you have a wireless adapter, you can use the iwconfig command to gather crucial information for wireless hacking such as the adapter’s IP address, its MAC address what mode it’s in, and more.

EX :

* kali >iwconfig

wlan0 IEEE 802.11bg ESSID:off/any

Mode:Managed Access Point: Not Associated TxPower=

20 dBm

*snip*lo

no wireless extensions

eth0 no wireless extensions

1. CHANGING YOUR NETWORK INFORMATION

Being able to change your IP address and other network information is a useful skill

because it will help you access other networks while appearing as a trusted device on

those networks. For example, in a denialofservice

(DoS) attack, you can spoof your IP

so that that the attack appears to come from another source, thus helping you evade IP capture during forensic analysis. This is a relatively simple task in Linux, and it’s done with the ifconfig command.

1. *Changing Your IP Address*

To change your IP address, enter ifconfig followed by the interface you want to reassign and the new IP address you want assigned to that interface.

EX :

kali >ifconfig eth0 192.168.181.115

1. Changing Your Network Mask and Broadcast Address

You can also change your network mask (netmask) and broadcast address with the ifconfig command. For instance

EX :

kali >ifconfig eth0 192.168.181.115 netmask 255.255.0.0 broadcast

192.168.1.255

6- Spoofing Your MAC Address

You can also use ifconfig to change your MAC address (or HWaddr)

EX :

kali >ifconfig eth0 down

kali >ifconfig eth0 hw ether 00:11:22:33:44:55

kali >ifconfig eth0 up

To spoof your MAC address, simply use the ifconfig command’s down option to take

down the interface (eth0 in this case). Then enter the ifconfig command followed by the

interface name (hw for hardware, ether for Ethernet) and the new spoofed MAC address.

Finally, bring the interface back up with the up option for the change to take place.

1. Assigning New IP Addresses from the DHCP Server

The DHCP server assigns IP addresses to all the systems on the subnet and keeps log files of which IP address is allocated to which machine at any one time. This makes it a great resource for forensic analysts to trace hackers with after an attack. For that reason, it’s useful to understand how the DHCP server works.

EX :

kali >dhclient eth0

To request an IP address from DHCP, simply call the DHCP server with the command

dhclient followed by the interface you want the address assigned to

1. MANIPULATING THE DOMAIN NAME SYSTEM (DNS)

DNS is the service that translates a domain name like hackersarise.com to the appropriate IP address .

TOOL

**dig** : One of the most useful commands for the aspiring hacker

**DNS** include the IP address of the target’s nameserver (the server that translates the target’s

name to an IP address), the target’s email server, and potentially any subdomains and IP addresses.

EX :

kali >dig hackers-arise.com ns :

For instance, enter dig hackers-arise.com and add the ns option (short for name server).

The name server for hackersarise.com is displayed in the ANSWER SECTION

**Dig** can be used to the dig command to get information on email servers connected to a

domain by adding the mx option (mx is short for *mail exchange server*).

EX :

kali >dig hackers-arise.com mx

1. Changing Your DNS Server

In some cases, you may want to use another DNS server. To do so, you’ll edit a plaintext file named */etc/resolv.conf* on the system.

* Open that file in a text edito (nano )
* enter the precise name of your editor (nano) followed and the filename

kali >nano /etc/resolv.conf.

* will open the *resolv.conf* file in the */etc* directory in my specified graphical text editor,
* finally , you can chang your DNS

1. Mapping Your Own IP Addresses

A special file on your system called the *hosts* file also performs domain name– IP address translation. The *hosts* file is located at */etc/hosts* .

To show this file : kali >nano /etc/hosts

**you can add any IP address mapped to any domain you’d like.**