**Chapter 1:-**

**The Terminal**:

The first step in using Kali is to open the terminal, which is the command line interface we’ll use in this book. In Kali Linux, you’ll find the icon for the terminal at the bottom of the desktop. Double-click this icon to open the terminal or press CTRL ­ALT ­T.

**The Linux File-system:**

/**root:** The home directory of the all-powerful root user

/**etc :** c Generally contains the Linux configuration files—files that control when and how

Programs start up

/**home**: The user’s home directory

/**mnt:** Where other file systems are attached or mounted to the file system

**/bin:** Where application binaries (the equivalent of executable in Microsoft Windows) reside

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

**BASIC COMMANDS IN LINUX :**

**PWD :** Enter pwd in your terminal to see where you are:

Kali >pwd

/root

**whoami :** command to see which user you’re logged in as:

kali >whoami

root

**cd :** For example, here’s how to change to the /etc. directory used to store configuration files:

kali >cd/etc

root@kali:/etc#

**ls :** To see the contents of a directory (the files and subdirectories), we can use the ls(list) command

**man & --help** — To know more about a command and how to use it, use the **man** command. It shows the manual pages of the command. For example, “**man cd**” shows the manual pages of the **cd** command. Typing in the command name and the argument helps it show which ways the command can be used (e.g., **cd –help**).

**. cp** — Use the **cp** command to copy files through the command line. It takes two arguments: The first is the location of the file to be copied, the second is where to copy.

**locate** — The **locate** command is used to locate a file in a Linux system

**whereis :** If you’re looking for a binary file, you can use the where is command to locate it

**cat:** Use the **cat** command to display the contents of a file. It is usually used to easily view programs.

**mkdir & rmdir** — Use the **mkdir** command when you need to create a folder or a directory. For example, if you want to make a directory called “DIY”, then you can type **“mkdir DIY**”. Remember, as told before, if you want to create a directory named “DIY Hacking”, then you can type “mkdir **DIY\ Hacking**”. Use **rmdir** to delete a directory. But **rmdir** can only be used to delete an empty directory. To delete a directory containing files, use **rm**.

**touch** — The **touch** command is used to create a file. It can be anything, from an empty txt file to an empty zip file. For example, “**touch new.txt**”.

**mv :** The mv command can be used to move a file or directory to a new location or simply to give an existing file a new name. To rename newfile to newfile2,

**Chapter 2:-**

**VIEWING FILES:**

the most basic text display command is probably cat, but it has Playlists History Topics Tutorials Offers & Deals Highlights Settings Support Sign Out its limitations. Use catto display the Snort config file (snort.conf) found in/etc/snort (see Listing 2­1).

kali >cat/etc/snort/snort.conf

**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

kali >head/etc/snort/snort.conf

If you want to see more or fewer than the default 10 lines, enter the quantity you want with the dash (-) switch after the call to head and before the filename. For example, if you want to see the first 20 lines of the file, you would enter the command shown at the top

kali >head-20/etc/snort/snort.conf

**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

As with the head command, you can tell tail how many lines to display by entering a dash (-) and then the number of lines between the command and the filename

kali >tail-20/etc/snort/snort.conf

**Numbering the Lines:**

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

**FILTERING TEXT WITH GREP:**

The command grep is probably the most widely used text manipulation command. It lets you filter the content of a file for display. If, for instance, you want to see all lines that include the word output in your snort.conf file

kali >cat/etc/snort/snort.conf|grepoutput

**USING SED TO FIND AND REPLACE:**

The sed command lets you search for occurrences of a word or a text pattern and then perform some action on it. The name of the command is a contraction of stream editor, because it follows the same concept as a stream editor

**VIEWING FILES WITH MORE AND LESS:**

**Controlling the Display with more:-**

The more command displays a page of a file at a time and lets you page down through it using the ENTER key. It’s the utility that the man pages use, so let’s look at it first. Open snort.conf with the more command

kali >more/etc/snort/snort.conf

**Displaying and Filtering with less:-**

The less command is very similar to more, but with additional functionality—hence, the common Linux aficionado quip, “Less is more.” With less, you can not only scroll through a file at your leisure, but you can also filter it for terms

kali >less/etc/snort/snort.conf

Chapter3:-

**ANALYZING NETWORKS WITH IFCONFIG:**

The ifconfig command is one of the most basic tools for examining and interacting with active network interfaces. You can use it to query your active network connections by simply entering ifconfig in the terminal.

kali >ifconfig

the command ifconfig shows some useful information about the active network interfaces on the system.

The type of network being used (Ethernet) is listed next, followed by HWaddr and an address; this is the globally unique address stamped on every piece of network hardware—in this case, the network interface card (NIC), usually referred to as the media access control (MAC) address.

The second line contains information on the IP address currently assigned to that network interface (in this case, 192.168.181.131 ➋); the Bcast ➌, or broadcast address, which is the address used to send out information to all IPs on the subnet; and finally the network mask (Mask➍), which is used to determine what part of the IP address is connected to the local network. You’ll also find more technical info in this section of the output

This information from ifconfig enables you to connect to and manipulate your local area network (LAN) settings, an essential skill for hacking.

**CHECKING WIRELESS NETWORK DEVICES WITH IWCONFIG:**

you can use the iwconfig command to gather crucial information for wireless hacking such as the adapter’s IP address

The information you can glean from this command is particularly important when you’re using wireless hacking tools like air crack­ –ng

kali >iwconfig

the only network interface with wireless extensions is wlan0, which is what we would expect. Neither lo nor eth0has any wireless extension

**CHANGING YOUR NETWORK INFORMATION:**

**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. For example, to assign the IP address 192.168.181.115 to interface eth0

kali >ifconfigeth0192.168.181.115

**Changing Your Network Mask and Broadcast Address:**

You can also change your network mask (netmask) and broadcast address with the ifconfig command. For instance, if you want to assign that same eth0interface with a netmask of 255.255.0.0 and a broadcast address of 192.168.1.255

kali >ifconfigeth0192.168.181.115netmask255.255.0.0broadcast 192.168.1.255

**Spoofing Your MAC Address:**

You can also use ifconfig to change your MAC address (or HWaddr). Changing your MAC address to spoof a different MAC address is almost trivial and neutralizes those security measures. Thus, it’s a very useful technique for bypassing network access controls.

kali >ifconfigeth0down

kali >ifconfigeth0hwether00:11:22:33:44:55

kali >ifconfigeth0up

“Now, when you check your settings with ifconfig, you should see that HWaddr has changed to your new spoofed IP address!”

**Assigning New IP Addresses from the DHCP Server:**

, to connect to the internet from a LAN, you must have a DHCP­ assigned IP. Therefore, after setting a static IP address, you must return and get a new DHCP assigned IP address. To do this, you can always reboot your system, but I’ll show you how to retrieve a new DHCP without having to shut your system down and restart it.

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. Different Linux distributions use different DHCP clients, but Kali is built on Debian, which uses dhclient. Therefore, you can assign a new address like this -🡪 kali >dhclienteth0

**MANIPULATING THE DOMAIN NAME SYSTEM :**

Hackers can find a treasure trove of information on a target in its Domain Name System (DNS). DNS is a critical component of the internet, and although it’s designed to translate domain names to IP addresses, a hacker can use it to garner information on the target

**Examining DNS with dig:**

One of the most useful commands for the aspiring hacker is dig, which offers a way to gather DNS information about a target domain. The stored DNS information can be a key piece of early reconnaissance to obtain before attacking. This information could include the IP address of the target’s name server (the server that translates the target’s name to an IP address), the target’s email server, and potentially any subdomains and IP addresses.

kali >dighackers-arise.comns

**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 editor—I’m using Leafpad. Then, on your command line, enter the precise name of your editor followed by the location of the file and the filename. For example,

kali >leafpad/etc/resolv.conf

I would just need to save the file. However, you can also achieve the same result exclusively from the command line by entering the following:

kali >echo"nameserver8.8.8.8">/etc/resolv.conf

the local DNS server in the resolv.conf file and follow it with a public DNS server. The operating system queries each DNS server listed in the order it appears in /etc/resolv.conf, so the system will only refer to the public DNS server if the domain name can’t be found in the local DNS server.

**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, and kind of as with DNS, you can use it to specify your own IP address–domain name mapping. In other words, you can determine which IP address your browser goes to when you enter www.microsoft.com (or any other domain) into the browser, rather than let the DNS server decide. As a hacker, this can be useful for hijacking a TCP connection on your local area network to direct traffic to a malicious web server with a tool such as dnsspoof. From the command line, type in the following command (you can substitute your preferred text editor for leafpad)

kali >leafpad/etc/hosts