Ch 2 :

1. Use the ls command from the root (/) directory to explore the directory structure of Linux. Move to each of the directories with the cd command and run pwd to verify where you are in the directory structure.

```
$ls
$cd Downloads ‘or any directory ’
$pwd
```

2. Use the whoami command to verify which user you are logged in as.

```
$whoami
```

3. Use the locate command to find word lists that can be used for password cracking.

```
$locate wordlists | grep password
```

4. Use the cat command to create a new file and then append to that file. Keep in mind that >redirects input to a file and >>appends to a file.

```
$cat >cat_file
mohamed
$cat >>cat_file
ezat
```

5. Create a new directory called hackerdirectory and create a new file in that directory named hackedfile. Now copy that file to your /root directory and rename it secretfile.

```
$mkdir new_folder
$cd new_folder
$touch hackedfile
$cp hackedfile /root/secretfile
```

ch 2

1. Navigate to /usr/share/wordlists/metasploit. This is a directory of multiple wordlists that can be used to brute force passwords in various password-protected devices using Metasploit, the most popular pentesting andhacking framework.

```
$cd /usr/share/wordlists/metasploit
```

2. Use the cat command to view the contents of the file passwords.lst.

```
$cat passwords.lst
```

3. Use the more command to display the file passwords.lst.

```
$more passwords.lst
```

4. Use the less command to view the file passwords.lst.

```
$less passwords.lst
```

5. Now use the nl command to place line numbers on the passwords in passwords.lst. There should be 88,396 passwords.

```
$nl passwords.lst
```

6. Use the tail command to see the last 20 passwords in passwords.lst.

```
$tail -n20 passwords.lst
```

7. Use the cat command to display passwords.lst and pipe it to find all the passwords that contain 123.

```
$cat passwords.lst  |grep 123
```

ch3

1. Find information on your active network interfaces.

```
$ifconfig
```

2. Change the IP address on eth0to 192.168.1.1.

```
$ifconfig eth0 192.168.1.1
```

3. Change your hardware address on eth0.

```
$ifconfigeth0 down
$ifconfigeth0 hw ether 00:00:00:11:11:22
$ifconfigeth0 up
```

4. Check whether you have any available wireless interfaces active.

```
$iwconfig
```

5. Reset your IP address to a DHCP-assigned address.

```
$dhclient eth0
```

6. Find the name server and email server of your favorite website.

```
$dig facebook.com ns
$dig facebook.com ms
```

7. Add Google’s DNS server to your /etc/resolv.conf file so your system refers to that server when it can’t resolve a domain name query with your local DNS server.

```
>Open resolv.conf with leafpad
$leafpad /etc/resolv.conf
>change the name server to 8.8.8.8
$echo"nameserver8.8.8.8">/etc/resolv.conf
```

ch4

1. Install a new software package from the Kali repository.

```
$sudo apt install officelibre ‘any package  ’
```

2. Remove that same software package.

```
$sudo apt remove officlibre
```

3. Update your repository.

```
$sudo apt get update
```

4. Upgrade your software packages.

```
$sudo  apt get upgrade
```

5. Select a new piece of software from github and clone it to your system.

```
$git clone https://github.com/helghareeb/DSA20
```

ch5:

1.Select a directory and run a long listing on it. Note the permissions on the files and directories.

```
$ls -l /anydirectory
```

2.Select a file you don't have permission to execute and give yourself execute permissions using the chmod command.

```
$chmod myusername+x filename
```

3. Choose another file and change its ownership using chown.

```
$chown username /userfile
```

4. Use the find command to find all files with the SGID bit set.

```
$find / -root -perm -400
```

ch6

1. Run the ps command with the aux options on your system and note which process is first and which is last.

```
$ps aux
```

2. Run the top command and note the two processes using the greatest amount of your resources.

```
$top
>20870
```

3. Use the kill command to kill the process that uses the most resources.

```
$kill -1 20870
```

4. Use the renice command to reduce the priority of a running process to +19.

```
$renice 19 20873
```

5. Create a script called myscanning(the content is not important) with a text editor and then schedule it to run next Wednesday at 1 AM.

```
$leafpad myscanning
```

```
$at 7:20 2/15/2020
$/myscanning
```

ch7

1. View all of your environment variables with the more command.

```
$set | more
```

2. Use the echo command to view the HOSTNAME variable.

```
$echo $HOSTNAME
```

3. Find a method to change the slash (/) to a backslash (\) in the faux Microsoft cmdPS1example (see Listing 7-2).

4. Create a variable named MYNEWVARIABLE and put your name in it.

```
$MYNEWVARIABLE =”mohamed”
```

5. Use echoto view the contents of MYNEWVARIABLE.

```
$echo $MYNEWVARIABLE
```

6. Export MYNEWVARIABLE so that it’s available in all environments.

```
$export MYNEWVARIABLE
```

7. Use the echo command to view the contents of the PATH variable.

```
$echo $PATH
```

8. Add your home directory to the PATH variable so that any binaries in your home directory can be used in any directory.

```
$PATH=$PATH:/home
```

9. Change your PS1 variable to “World’sGreatestHacker:”.

```
$PS1=”World’sGreatestHacker:”
```

ch8

1. Create your own greeting script similar to our HelloHackersArise script.

```
$#! /bin/bash
$echo "my script"
```

“ save it “ as HelloHackersArise

2. Create a script similar to MySQLscanner.sh but design it to find systems with Microsoft’s SQL Server database at port 1433. Call it MSSQLscanner.

```
$#! /bin/bash
$nmap -sT  192.168.1.1/24 -p 1433>/dev/null -oG MySQLscan
$cat MySQLscan |grep open MSSQLscanner
$cat MSSQLscanner
```

3. Alter that MSSQLscanner script to prompt the user for a starting and ending IP address and the port to search for. Then filter out all the IP addresses where those ports are closed and display only those that are open.

```
#! bin/bash
echo "Enter the starting IP address : "
read FirstIP

echo "Enter the last octet of the last IP address : "
read LastOctetIP

echo "Enter the port number you want to scan for : "
read port

nmap sT $FirstIP$LastOctetIP p $port >/dev/null oG MySQLscan

cat MySQLscan | grep open > MSSQLscanner

cat MSSQLscanner
```

ch9

1. Create three scripts to combine, similar to what we did in Chapter 8. Name them Linux4Hackers1, Linux4Hackers2, and Linux4Hackers3.

Done

2. Create a tarball from these three files. Name the tarball L4H. Note how the size of the sum of the three files changes when they are tarred together.

```
$tar -cvf L4h.tar Linux4Hackers1 Linux4Hackers2 Linux4Hackers3
```

3. Compress the L4H tarball with gzip. Note how the size of the file changes. Investigate how you can control overwriting existing files. Now uncompress the L4H file.

```
$gzip L4H.*
```

4. Repeat Exercise 3 using both bzip2 and compress.

```
$bzip2 L4h.*
$compress L4H.*
```

5. Make a physical, bit-by-bit copy of one of your flash drives using the ddcommand.

```
$dd if=/dev/sdb of=/root/flashcopy
```

ch10

1. Use the mount and umount commands to mount and unmount your flash drive.

```
$mount /dev /sdb1 /directory_name
$umount /dev /sdb1
```

2. Check the amount of disk space free on your primary hard drive.

```
$df
```

3. Check for errors on your flash drive with fsck.

```
$fsck
```

5. Use the lsblk command to determine basic characteristics of your block devices.

```
$lsblk
```

ch11

1. Use the locatecommand to find all the rsyslogfiles.

```
$locate rsyslog
```

2. Open the rsyslog.conf file and change your log rotation to one week.

```
$leafpad /etc/rsyslog.conf
$leafpad /etc/logrotate.conf
```

change the rotation to rotate 1 ‘as weeks ‘

3. Disable logging on your system. Investigate what is logged in the file /var/log/syslog when you disable logging.

```
$service rsyslog stop
```

4. Use the shred command to shred and delete all your kernlog files.

```
$shred -f /var/log /auth.log.*
```

ch12

1. Start your apache2 service through the command line.

```
$service apache2 start
```

2. Using the index.html file, create a simple website announcing your arrival into the exciting world of hacking.

Done

3. Start your SSH service via the command line. Now connect to your Kali system from another system on your LAN.

```
$service ssh start
ssh pi@192.168.1.7
sudo raspi-config
```

4. Start your MySQL database service and change the root user password to hackers-arise. Change to the my sql database.

```
$service mysql start
$sudo mysql -u root -p
>use mysql
>>update user set password = PASSWORD("hackers-arise") where user ='root';
```

5. Start your PostgreSQL database service. Set it up as described in

this chapter to be used by Metasploit.

```
$service postgresql start
$msfconsole
 >msfdbinit
 >supostgres
/root$createusermsf_user-P
/root$createdb--owner=msf_userhackers_arise_db
/root$exit
>db_connectmsf_user:password@127.0.0.1/hackers_arise_db
>db_status
```

ch13

1. Run traceroute to your favorite website. How many hops appear between you and your favorite site?

```
$traceroute google.com
>14
```

2. Download and install the Tor browser. Now, browse anonymously around the web just as you would with any other browser and see if you notice any difference in speed.

…..

3. Try using proxychains with the Firefox browser to navigate to your favorite website.

.

4. Explore commercial VPN services from some of the vendors listed in this chapter. Choose one and test a free trial.

5. Open a free ProtonMail account and send a secure greeting to occupytheweb@protonmail.com.

Ch14

1. Check your network devices with ifconfig. Note any wireless extensions.

```
$ifconfig
```

2. Run iwconfig and note any wireless network adapters.

```
$iwconfig
```

3. Check to see what Wi-Fi APs are in range with iwlist.

```
$iwlist wlan0 scan
```

4. Check to see what Wi-Fi APs are in range with nmcli. Which do you find more useful and intuitive, nmcli or iwlist?

```
$nmcli dev wifi
>nmcli
```

5. Connect to your Wi-Fi AP using nmcli.

```
$nmcli dev wifi connect my_wifi password 12345678
```

6. Bring up your Bluetooth adapter with hciconfigand scan for nearby discoverable Bluetooth devices with hcitool.

```
$hciconfig
$hciconfig hci0 up
$hcitool scan
```

7. Test whether those Bluetooth devices are within reachable distance with l2ping

```
$l2ping 10:f0:05:e9:e9:62
```

ch15

1. Check the version of your kernel.

```
$uname -a
```

2. List the modules in your kernel.

```
$lsmod
```

3. Enable IP forwarding with a sysctl command.

```
$sysctl -w net.ipv4.ip_forward=1
```

4. Edit your /etc/sysctl.conf file to enable IP forwarding. Now, disable IP forwarding.

```
$sysctl -w net.ipv4.ip_forward=0
```

5. Select one kernel module and learn more about it using modinfo

```
$modinfo fat
```

ch16

1. Schedule your MySQLscanner.sh script to run every Wednesday at 3 PM.

```
$leafpad /etc/crontab
add :
00 15 * * 3 user /usr/share/MySQLsscanner.sh
```

2. Schedule your MySQLscanner.sh script to run every 10th day of the month in April, June, and August.

```
$leafpad /etc/crontab
add :
00 00 10 4,6,8  * user /usr/share/MySQLsscanner.sh
```

3. Schedule your MySQLscanner.sh script to run every Tuesday through Thursday at 10 AM.

```
$leafpad /etc/crontab
add :
00 10 * *  2 user /usr/share/MySQLsscanner.sh
```

4. Schedule your MySQLscanner.sh script to run daily at noon using the shortcuts.

```
@midnight user /usr/share/MySQLsscanner.sh
```

5. Update your rc.d script to run PostgreSQL every time your system boots.

```
$update-rc.d PostgreSQL defualts
```

6. Download and install rcconf and add the PostgreSQL and MySQL databases to start at bootup.

```
$sudo apt-get install rcconf
$rcconf
>select mysql from gui form
```

ch17

1. Build the SSH banner-grabbing tool from Listing 17-5 and then edit it to do a banner grab on port 21.

```
**in python script called python.py
#! /usr/bin/python3
s = socker.socket()
port = 21
print('this is the banner for the port')
s.connect (("192.168.1.101",port))
answer = s.recv(1024)
print(answer)
s.close()
$sudo ./python.py
```