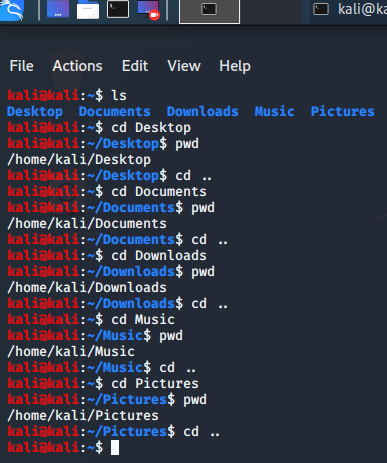
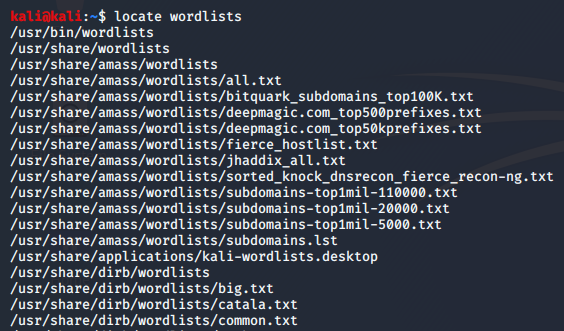
Exercise solution:

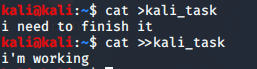
Chapter 1:

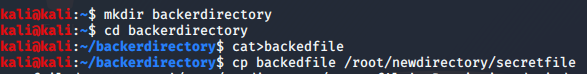
1.



2.

3.

4.

5.

Chapter 2:

1. 
2. Kali>cat /usr/share/wordlists/passwords.lst.txt
3. Kali>more /usr/share/wordlists/passwords.lst.txt
4. Kali>less /usr/share/wordlists/passwords.lst.txt
5. Kali>nl /usr/share/wordlists/passwords.lst.txt
6. Kali>tail -20 /usr/share/wordlists/passwords.lst.txt
7. Kali>cat /usr/share/wordlists/passwords.lst.txt |grep 123

Chapter 3:

1.kali>ifconfig

2.kali>ifconfig eth0 192.168.1.1. (to change my ip)

3.a) kali>ifconfig eth0 down

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

c)kali>ifconfig eth0 up

4.kali>iwconfig

5.kali>dhclient eth0 (to rsest ip address)

6.a) kali >dig hackersarise.com ns (to get name server)

b) kali>dig hackersarise.com mx (to get mail)

7.a) kali>leafpad /etc/resolv.conf

b)kali>echo “nameserver 8.8.8.8 “ >/etc/resolv.conf

chapter 4:

1. kali >apt-get install synaptic (to install synaptic package)

2. kali >apt-get remove synaptic

3.kali>apt-get update

4. kali>apt-get upgrade

5. kali >git clone https: //www.github.com /balle /bluediving.git(I used the book example)

Chapter 5:

1.kali> ls-l /user/sharee/hashcat

2.a)kali>chmod 777 hashcat.hcstat )numercial method)

b)kali>chmod u+w hashcat.hcstat (UGO method)

3.i will search about the answer

4. kali >find / user root -perm -4000

Chapter 6:

1.kali>ps aux (it display prosses for all user)

2.kali>top(display prosses ordered by resource used)

3.kali>kill -9 6996

4. kali >renice +19 6996

5.a) kali >leafpad CATteam

B) kali >at 1:00am wensday

c) at >/root /myscanningscript

chapter 7:

1.kali>set|more

2.kali>echo $HISTSIZE>~valueofHISTSIZE.txt

3.searching for it

4.kali>mynewvariable=”Nabila”

5.kali>echo $mynewvariable

7.kali>PATH-$PATH :/root/nemhackingtool

9.kali>ps1=”world best hacker :”

Chapter 8:

1. #! /bin/bash

echo "Hello world"

2.  #! /bin/bash

 nmap ­sT 192.168.181.0/24 ­p 3306 >/dev/null ­oG MySQLscan

 cat MySQLscan | grep open > MySQLscan2

   cat MySQLscan2(I think it’s constant fot scanner script)

chapter 9:

1.a) #! /bin/bash

echo "linux4hackers1"

b) #! /bin/bash

echo "linux4hackers2"

c) #! /bin/bash

echo "linux4hackers3"

2.kali>tar -cvf l4h linux4hackers1 linux4hackers2 linux4hackers3 (size of l4h is bigger than sum of 3 files)

3.kali>gzip l4h.\*(l4h size is smaller than sum of 3 files)

4.a) kali>bzip2 l4h.\*

b) kali>compress l4h.\*

5. kali >dd if=/dev/sdb of=/root/flashcopy

Chapter 10:

1.a)kali>mount /dev/sdb1/mnt

b) kali>unmount /dev/sdb1/mnt

2.kali>df

3.kali>fsch -p /dev/sdb1

5.kali>lsblk

Chapter 11:

1.kali>locate rsylog

2.kali>leafpad /etc/rsylog.conf

3.i cant understand the question

4. kali >shred -f -n 10 /var/log/auth.log

Chapter 12:

1.kali>service apache2 start

2.kali>leafpad /var/www/html/index.html

<h1>I’m arrive in hacker exiting world<h1>

3. kali >ssh pi @ 192.168.1.10

4.kali>mysql>update user set password=PASSWORD(“backer-arise”) where user =’root’;

Chapter 13:

1. kali >traceroute google.com

2.iam aleardy install Tor browser (it’s faster)

3. kali >proxychains firefox www.quora. Com

\*Another question icannot write it but I will practice them

Chapter 14:

1.kali>ifconfig

2.kali>iwconfig

3.kali>iwlist wlan0 scan

4.kali>nmcli dev wifi (iwlist is better than nmcli because it give me more information tahat might be useful)

5. kali>nmcli dev wifi connect Tedata1 password 1234567

6.kali>hciconfig (scanning for Bluetooth device)

7.kali>l2ping 76:6E:46:63:72:66 -c 4 (l2ping mac address)

Chapter 15:

1.a) kali >uname -a

b) kali>cat /proc/version

2.kali>lsmod (to list the modules )

3. kali >sysctl -w net.ipv4.ip\_ forward =1 (to enable ip forwording)

4.a)kali>leafpad /etc/sysctl.conf

b)i will put # before last line to disable ip forwarding

5.kali>modinfo Bluetooth

Chapter 16:

1.kali>15 00 \*\* 3 /root/mysql (iam not sure about this answer)

2. kali>15 00 3-7 9 3 /root/mysql

4. @noon     user   /usr/share/MySQLsscanner.sh

5. @reboot    user   /usr/share/postgresq (iam not sure about it also)

Chapter 17:

1. #! /usr/bin/python3

   import socket

Ports = [21,22,25,3009]

 for i in range (0,4):

     s = socket.socket()

   Ports = Port[i]

     print ('This Is the Banner for the Port')

     print (Ports)

   s.connect (("192.168.1.101", Port))

     answer = s.recv (1024)

     print (answer)

     s.close ()

then write this

kali > ./HackersArisePortBannerGrab.py

(to see the output of banner port)

3. #! /usr/bin/python3

   import socket

 TCP\_IP = "192.168.181.190"    TCP\_PORT = 6996    BUFFER\_SIZE = 100

 s = socket.socket(socket.AF\_INET, socket.SOCK\_STREAM)

 s.bind((TCP\_IP, TCP\_PORT))

 s.listen (1)

 conn, addr = s.accept()    print ('Connection address: ', addr )

   while 1:

     data=conn.recv(BUFFER\_SIZE)

     if not data:break

 print ("Received data: ", data)

   conn.send(data)

#echo

   conn.close

4. #! /usr/bin/python3

   import ftplib

 server = input(FTP Server: ")

 user = input("username: ")

 Passwordlist = input ("Path to Password List > ")

 try:

     with open(Passwordlist, 'r') as pw:

       for word in pw:

 word = word.strip ('\r').strip('\n')

try:

           ftp = ftplib.FTP(server)

           ftp.login(user, word)

  print (Success! The password is ' + word)

    except:

             print('still trying...')

   except:

     print ('Wordlist error')

(finished.)