**P1**.**KALI INSTALLATION.**

:-To install Kali Linux −

1.First, we will download the Virtual box and install it.

2.Later, we will download and install Kali Linux.

**1.install Virtual box.**

Step 2 − Click Next.

Step 3 − The next page will give you options to choose the location where you want to install the application. In this case, let us leave it as default and click Next.

Step 4 − Click Next and the following Custom Setup screenshot pops up. Select the features you want to be installed and click Next.

Step 5 − Click Yes to proceed with the installation.

Step 6 − The Ready to Install screen pops up. Click Install.

Step 7 − Click the Finish button.

**2.install kali linux.**

Step 1 − Download the Kali Linux package from its official website: <https://www.kali.org/downloads/>

Step 2 − Click VirtualBox → New as shown in the following screenshot.

Step 3 − Choose the right virtual hard disk file and click Open.

Step 4− The following screenshot pops up. Click the Create button.

Step 5 − Start Kali OS. The default username is root and the password is toor.

**3.Update the kali linux.**

Step 1 − Go to Application → Terminal. Then, type “apt-get update” and the update will take place as shown in the following screenshot.

Step 2 − Now to upgrade the tools, type “apt-get upgrade” and the new packages will be downloaded.

Page 9 of 132

Step 3 − It will ask if you want to continue. Type “Y” and “Enter”.

Step 4 − To upgrade to a newer version of Operating System, type “apt-get distupgrade”.

**4.Laboratory Setup.**

In this section, we will set up another testing machine to perform the tests with the help of tools of Kali Linux.

Step 1 − Download Metasploitable, which is a Linux machine. It can be downloaded from the official webpage of

Rapid7: <https://information.rapid7.com/metasploitabledownload.html?LS=1631875&CS=web>

https://information.rapid7.com/metasploitabledownload.html?LS=1631875&CS=web

Step 2 − Register by supplying your details. After filling the above form, we can download the software.

Step 3 − Click VirtualBox → New.

Step 4 − Click “Use an existing virtual hard disk file”. Browse the file where you have downloaded Metasploitable and click Open.

Step 5 − A screen to create a virtual machine pops up. Click “Create”.

The default username is msfadmin and the password is msfadmin.

**P2.A. EXPLORING THE COMMAND LINE ARGUMENT.**

**1.Positional Parameters:-**Command-line arguments are passed in the positional way.

# Nano falename.txt

# chmod +x filename.txt

# bash filename.txt WELCOME TO KALI

**2.TOTAL ARGUMENTS ($#).**

**#** bush filename.txt

**#** bush filename.txt WELCOME TO KALI LINUX.

**B. COMPARING TWO FILES**

# cat filename1.txt

# cat filename2.txt

# namo filename1.txt

# namo filename2.txt

# diff filename1.txt filename2.txt

(# diff -w filename1.txt filename2.txt

# diff -q filename1.txt filename2.txt

# diff -c filename1.txt filename2.txt

# diff -u filename1.txt filename2.txt)

**C. Managing Processes**

# ps(show the running process)

# sleep 30 (create ps)

# ps (check PS)

# kill -9 177 (kill PS)

# ps (to check PS is killed )

# pstree (show the running process tree)

# top(show the system performance like taskmanager in window)

# ps -aux(obtaining information about running processes)

# ps -afx

**P3 :- USING NETCAT SOCAT**

1. To start with netcat we just check the help section of netcat by using following command:

#nc -h

**2.TCP scan the target machin**

– nc -vnz 192.168.242.299(Ipaddress) 10-400 (enter range of port )

**3.To scan the UDP ports of target machine**

# nc -vzu 192.168.242.299(Ipaddress) 10-400 (enter range of port )

**4.BANNER GRABBING USING NETCAT:-** Banner grabbing is collection of information from the host machine. We also can do it using netcat. We run following command to see information of services running on a specific port.

# nc 192.168.242.299(Ipaddress) 20 (port number)

**TCP DUMP:-**tcpdump is a packet sniffing and packet analyzing tool for a System Administrator to troubleshoot connectivity issues in Linux.

# apt install tcpdump

# ifconfig

**1. CAPTURE PACKETS FROM SPECIFIC INTERFACE**

# tcpdump -i eth0

**2. CAPTURE ONLY SPECIFIC NUMBER OF PACKETS**

**#** tcpdump -c 5 -i eth0

**3. PRINT CAPTURED PACKET IN ASCII FORMAT**

# tcpdump -A -i eth0

**4. DISPLAY AVAILABLE INTERFACES**

# tcpdump -D

**5. CAPTURE IP ADDRESS OF PACKET**

# tcpdump -n -i eth0

**6. CAPTURE ONLY TCP PACKET**

**#** tcpdump -c 5 -i eth0 tcp

**7. CAPTURE PACKET FROM SPECIFIC PORT**

**#** tcpdump -i eth0 port 22

**8. PACKETS FROM DESTINATION IP**

**#** tcpdump -i eth0 dts 8.8.8.8

**9.PACKETS FROM SOURCE IP**

**#** tcpdump -i eth0 src 192.168.242.299(Ipaddress)

**10.FILTERING BY PROTOCOL**

**#** tcpdump -n tcp

**P4:- Passive Information Gathering**

**B. WHOIS ENUMERATION.**

# whois mu.ac.in

**P5: INFORMATION HARVESTING**

**A. USING INFOGA:-**

# git clone open source URL(<https://www.baeldung.com/linux/cat-writing-file>)

# cd Infoga

# ls

# python3 setup.py install

# python infoga.py

**i. Use the Infoga tool to scan shailendradegreecollege.in url on Google.**

**#** python infoga.py --domain shailendradegreecollege.in -- source google -- verbose3

**B. EMAIL HARVESTING USING MSFCONSOLE**

**#** msfd init

# msfconsole -q

**P5: INFORMATION GATHERING FRAMEWORK**

**A.MALTEGO(OSINT TOOL)**

Maltego is the all-in-one tool for link analysis. Maltego offers real-time data mining and information gathering, as well as the representation of this information on a node-based graph, making patterns and multiple order connections between said information easily identifiable.

# sudo apt install maltego

**P6 :ACTIVE INFORMATION GATHERING**

**A.DNS ENUMERATION**

# dnsenum -r [www.nesedu.in](http://www.nesedu.in)

**B.PORT SCANNING**

**1.host**

# nmap 192.168.242.299(Ipaddress)

**2.GET SERVICE AND VERSION**

# nmap -sV 192.168.242.299(Ipaddress)

**3.TCP SYN PORT SCANNING**

# nmap -sS 192.168.242.299(Ipaddress)

**4.SCANNING SPECIFIC PORT**

# nmap -p 1-1000 (portNo) 192.168.242.299(Ipaddress)

**5.SCANNING PORT NUMBER 22,23 and 100 to 150**

# nmap -p 22,23,100-150 192.168.242.299(Ipaddress)

**6.VERBOSE OPTION SCAN**

# nmap -v -A -sV 192.168.242.299(Ipaddress)

**7.NPING :- TCP PROBE FOR SPECIFIC PORT SCANNING**

# nping - -tcp -p 22 - -flags syn - -ttl 2 192.168.242.299(Ipaddress)

**8.PORT SCANNING USING PNSCAN**

# sudo apt install pnscan

# t\_listen -192.168.242.299(Ipaddress)

# pnscan -h

**9.SMB ENUMERATION**

# setenforce 0  
# smbclient -L //192.168.242.299(Ipaddress)/home/riza -U riza  
# service smb restart  
# smbclient -L //192.168.242.298(Ipaddress)/home/riza -U riza

**P7.VULNERABILITY SCANNING**

**1.Nessus**

Step1.Download nessus from browser

Step2.Open Nessus web client. Click on “Click here” link and then Click on Continue.

Step 3: Provide username and password for registering and click on continue.

Step 4: Select managed by security center.

Step 5: Provide username and password for login.

Step 6: Opens the scanner window

**2.Nmap**

Step1. Download nmap from browser and open it

Step 2: Enter the IP address/website name in the target field and click on scan

Step 3: Click on Nmap output, Ports/ host, Topology and host details to see Scanned detail of network.

**P8.WEB APPLICATION ASSESSMENT TOOL**

**A.BURPSUITE**

# burpsuite

**B.DIRB SIMPLE HIDDEN OBJECT SCAN**

# dirb <http://webscantest.com>

# cd/user/share/dirb/word (enter file pathaa)

# ls -i

# dirb <https://wilsoncollege.edu/apache.txt>

# dirb [https://wilsoncollege.edu/jersey.txt](https://wilsoncollege.edu/apache.txt)