CONTENT

S.No	DATE	TITLE	PAGE	SIGNATURE
01	21.12.2023	INSTALL VIRTUVAL BOX (KALI LINUX)		
02	03.01.2024	GENERAE A SECURE PASSWORD USING KEEPASS		
03	11.01.2024	CHANGE THE WIRELESS DEVICE MODE AS MONITOR MODE		
04	11.01.2024	FIND THE KNOWN AND OPEN VULNERABILITIES OF SYSTEM USING METASPOIT		
05	24.01.2024	IDENTIFY THE MULTIPLE VULNERABILITIES OF WEB SERVER USING NIKTO TOOL		
06	12.02.2024	IDENTIFY THE OPEN PORTS IN THE NETWORK USING N-MAP TOOLS		
07	20.02.2024	LIST ALLTHE NETWORK AROUNDUS AND DISPLAY THE INFORMATION ABOUT THE NETWORKS		
08	28.02.2024	SNIFF AND CAPTURE THE PACKET SENT OVER HTTP REQUESTS		
09	14.03.2024	FIND THE OWNERS OF THE INTERNET USING WHOIS LOOKUP TOOL		
10	14.03.2024	FIND THE SUBDOMAINS OF WEBPAGE USING KNOCK TOOL		

EX: NO: 01 **INSTALL VIRTUAL BOX**

DATE: 21.12.2023 **(KALI LINUX)**

AIM:

To install virtual box (kali linux) software from www.google.com

ALGORITHM:

Step1: Install the Operating System Kali_x64

Machine Folder: D:\Virtual\VirtualBox (Try not to use a system partition C: to store VMs).

Type: Linux

Version: Debian (64-bit)

Step2: Launch VirtualBox Manager and click the new icon.

Step3: Choose the memory to allocate to the virtual machine and click next. The default setting for Linux is 1024 MB.

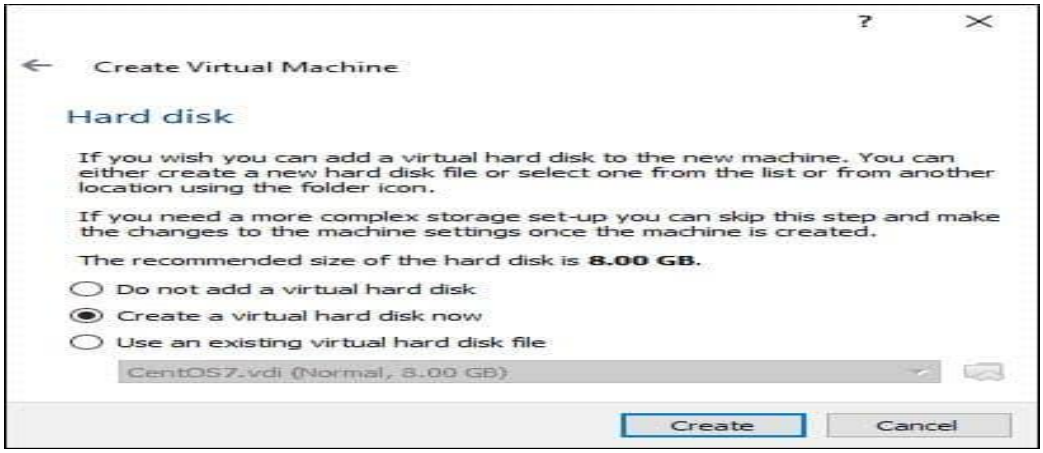
Step4: The default option is to create a virtual hard disk for the new VM. Click Create to continue.

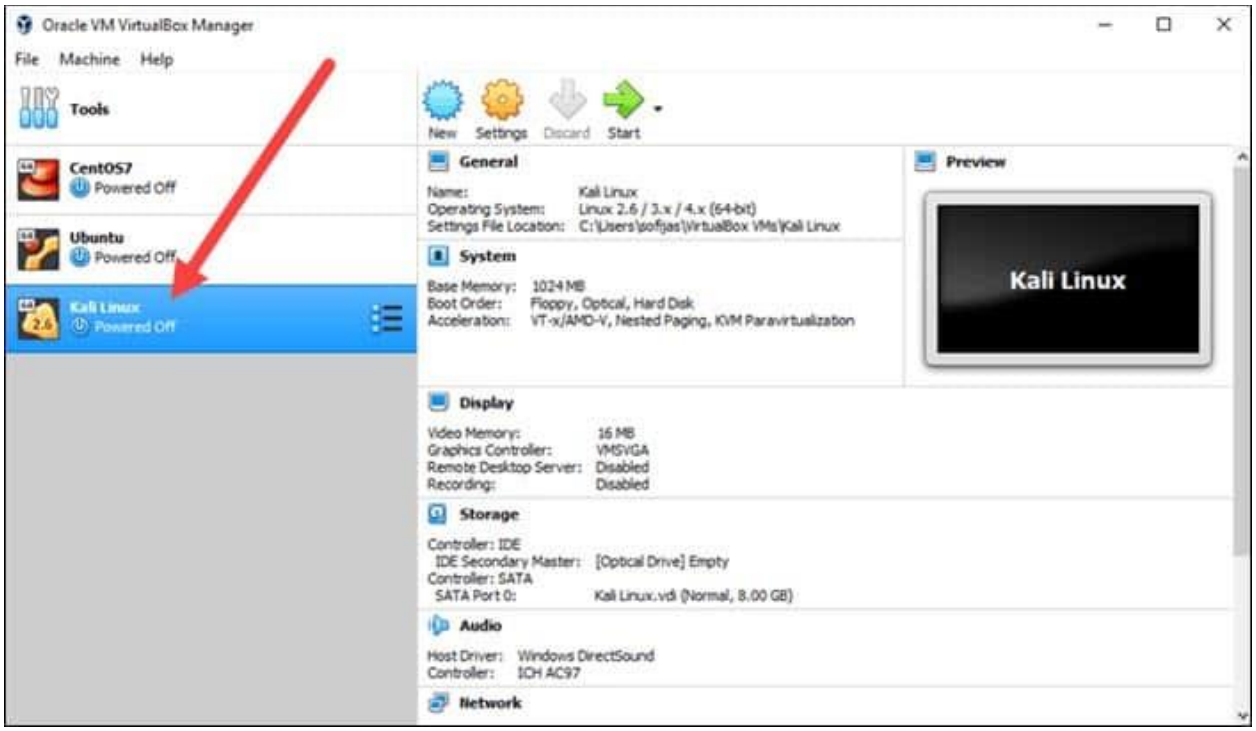
Alternatively, you can use an existing virtual hard disk file or decide not to add one at all.

Step5: Hard disk files type stick to the default file type for the new virtual hard disk, VDI (VirtualBox Disk Image). Click next to continue.

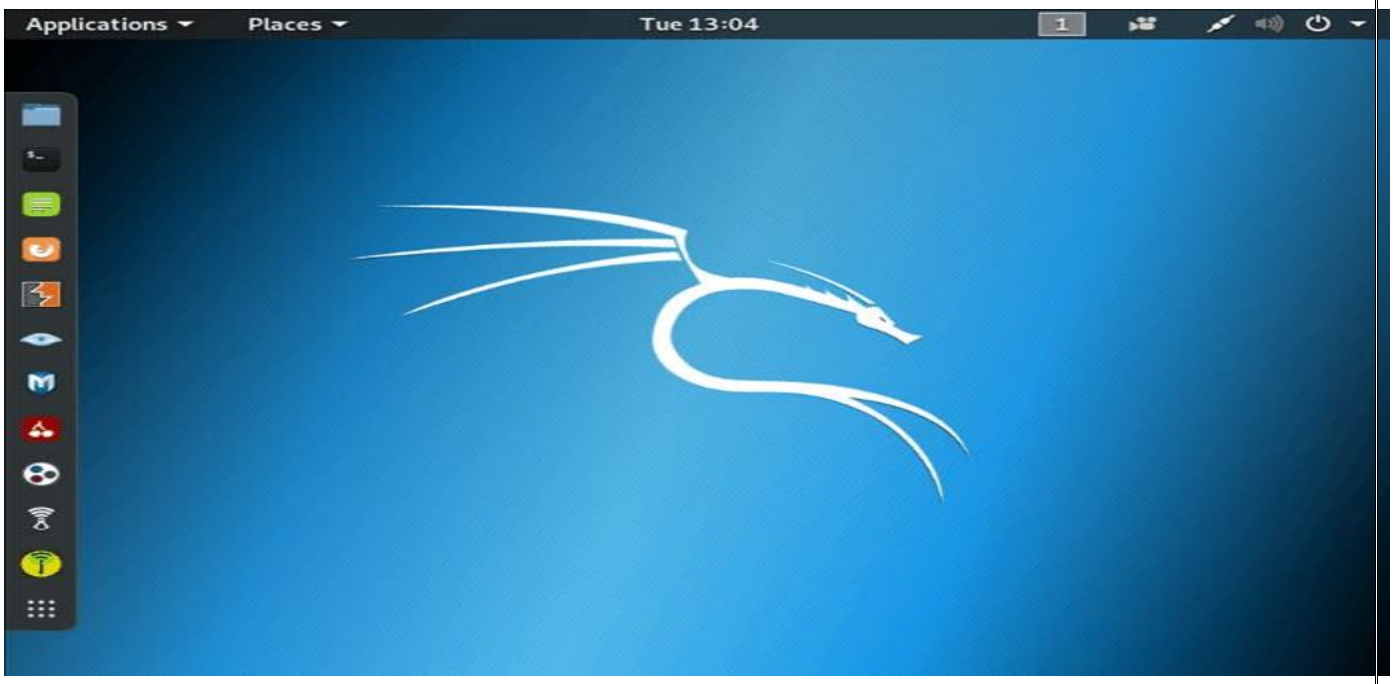
Step6: Storage on a physical hard disk. Decide between Dynamically allocated and fixed size. The first choice allows the new hard disk to grow and fill up space dedicated to it. The second, fixed size uses the maximum capacity from the start. Click Next.

Step7: Specify the name and where you want to store the virtual hard disk. Choose the amount of file data the VM is allowed to store on the hard disk. Clicks create to finish.


Create Virtual Machine
Hard disk
If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select one from the list or from another location using the folder icon.
If you need a more complex storage set-up you can skip this step and make the changes to the machine settings once the machine is created.
The recommended size of the hard disk is 8.00 GB.
Do not add a virtual hard disk
Create a virtual hard disk now
Use an existing virtual hard disk file
CentOS7.vdi (Normal, 8.00 GB)
Create
Cancel


Oracle VM VirtualBox Manager
File
Machine
Help
Tools
CentOS7
Powered Off
Ubuntu
Powered Off
Kali Linux
Powered Off
New
Settings
Discard
Start
General
Name: Kali Linux
Operating System: Linux 2.6 / 3.x / 4.x (64-bit)
Settings File Location: C:\Users\sofjas\VirtualBox VMs\Kali Linux
System
Base Memory: 1024 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, KVM Paravirtualization
Preview
Kali Linux
Display
Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled
Storage
Controller: IDE
IDE Secondary Master: [Optical Drive] Empty
Controller: SATA
SATA Port 0: Kali Linux.vdi (Normal, 8.00 GB)
Audio
Host Driver: Windows DirectSound
Controller: ICH AC97
Network

FINAL REPORT:



Result:

Virtual box (kali linux) was installed successfully.

EX: NO: 02 **GENERATE A SECURE PASSWORD USING**

DATE: 03.01.2024 **KEEPASS**

AIM:

To generate a secure password using keepass.

ALGORITHM:

Step1: Install keepass using apt-get[-] sudo apt-get update.

Step2: After updating it, install Keepass using the command Install Keepass2.

Step3: A database screen is open. Create a New file [Database].

Step4: Add entry (ctrl+I) or Keepass3 command to enter the details of the entry, . Including your username and password by creating new file.

Step5: Keepass will automatically generate a password for you inside the password field. Click on three button to reveal what the password look like.

Step6: Open password generator fix a master password by Generating using character set.

Step7: Click OK on entry

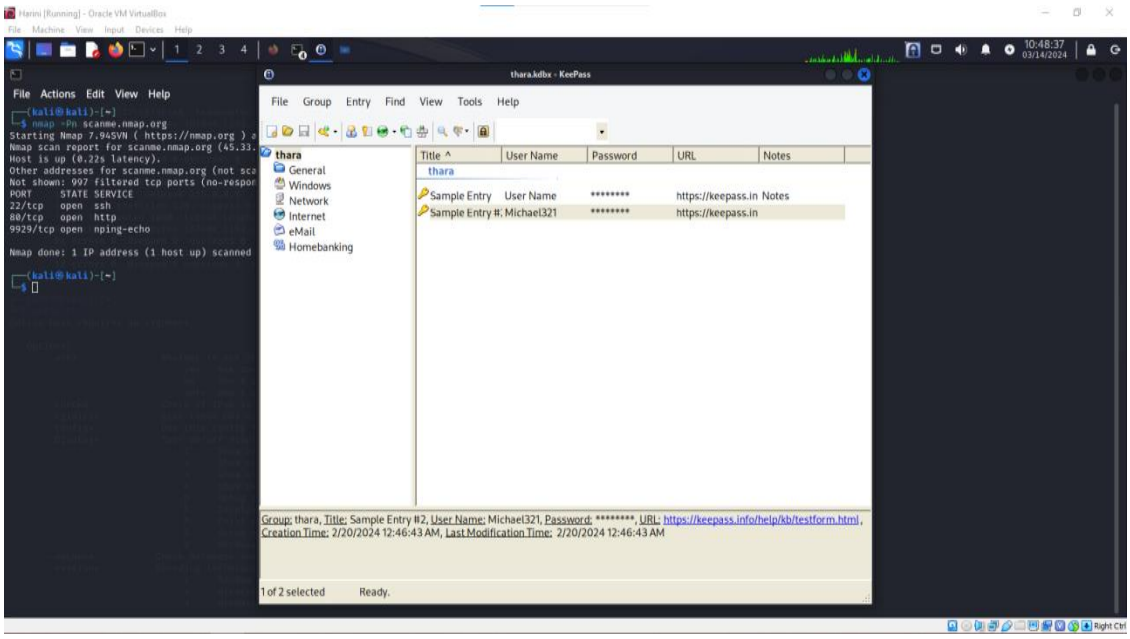
PROGRAM

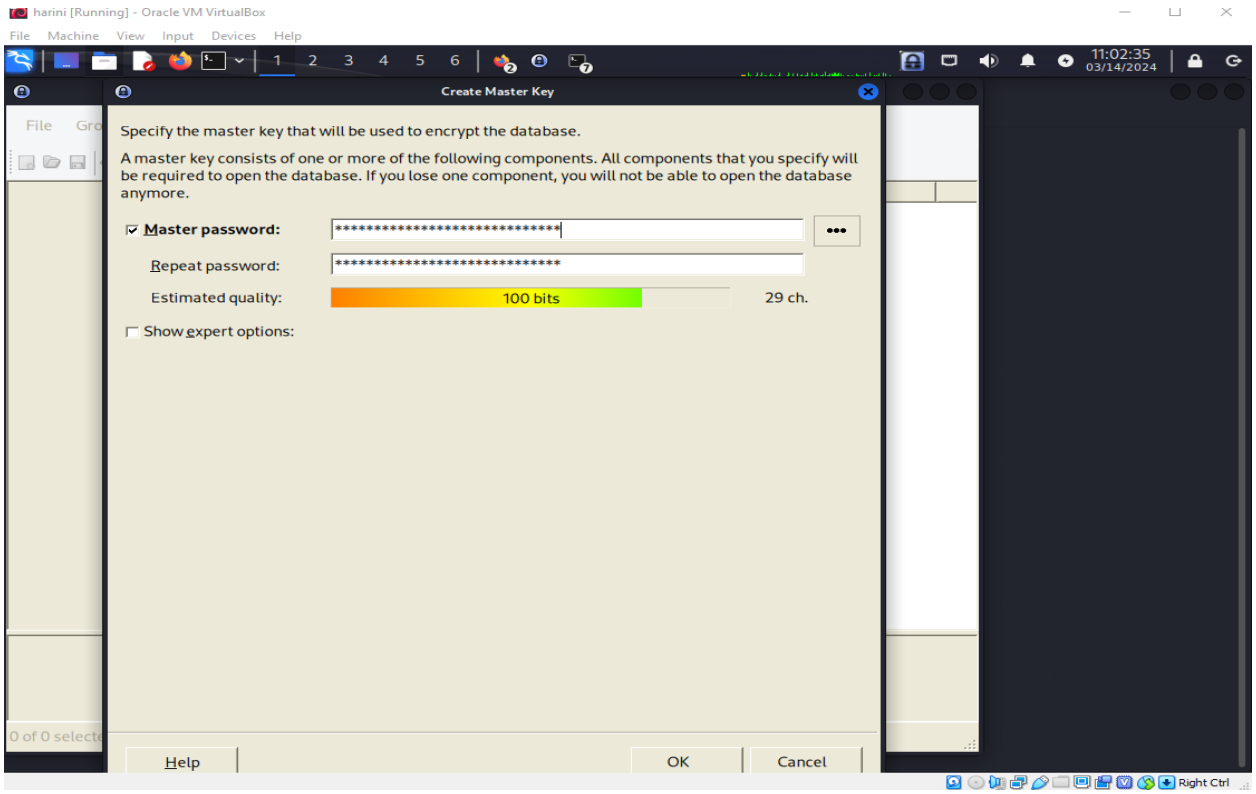
Sudo apt-get update

Sudo apt install keepass2

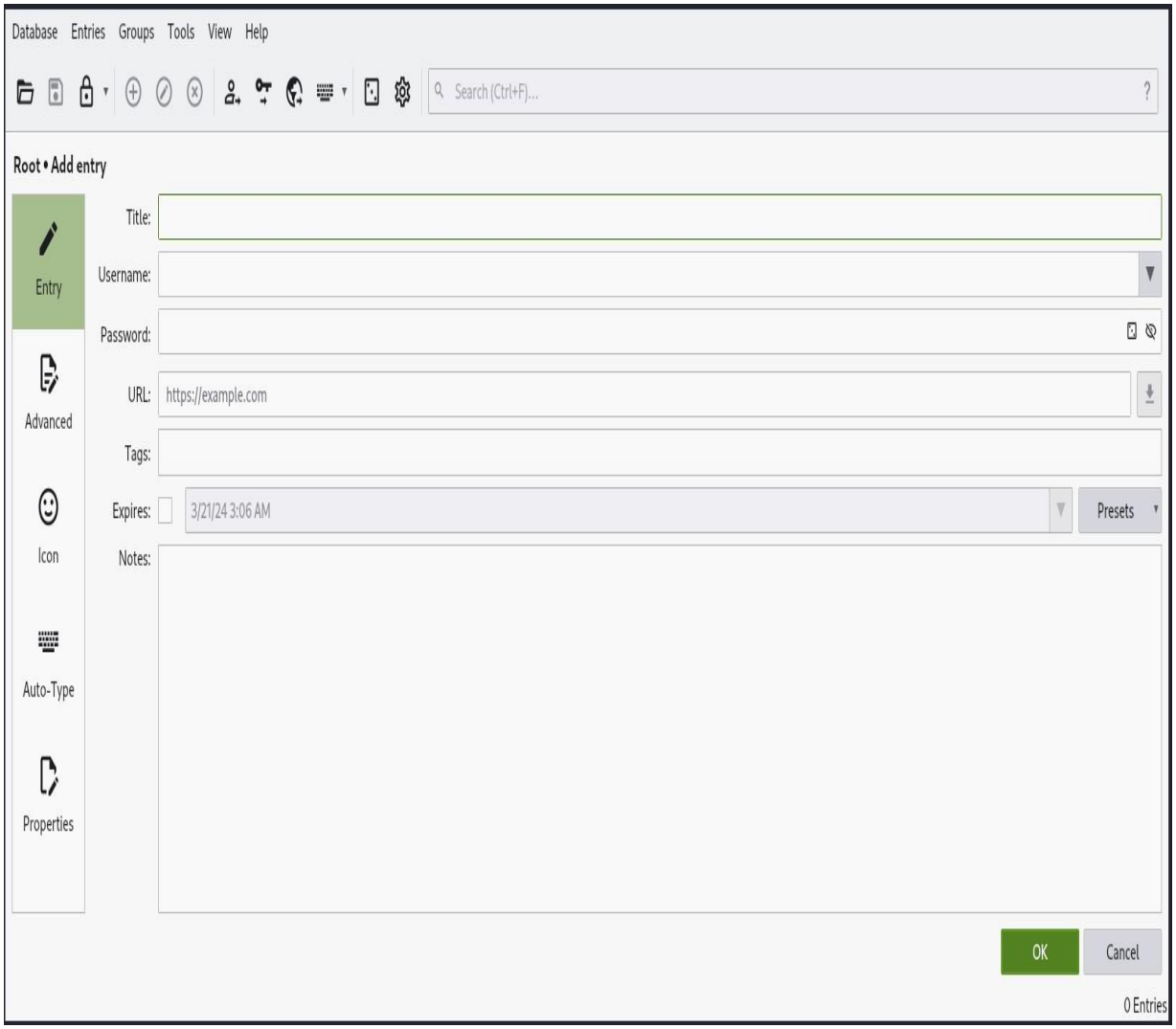
Keepass2

COMMAND OUTPUT:





FINAL REPORT:



RESULT:

Thus a secure password was successfully generated.

EX: NO: 03 **CHANGE THE WIRELESS DEVICE MODE AS**

DATE: 11.01.2024 **MONITOR MODE**

AIM:

To change the wireless device mode as monitor mode.

ALGORITHM:

Step1: To get information on wireless interface using the command sudo airmon-ng.

Before changing the mode, it's good to know the name of your wireless interface. You can use the iwconfig

Step2: If wlan doesn't exists then download compat-wireless-2010-06-28.tar.tz2 from chrome.

Step3: Change to directory - cd Downloads

Step4: After changing a directory copy and paste the filename

cd compat-wireless-2010-06-28

Step5: If we want to kill any process that many interface with using adapter in monitor mode.

Use the command: sudo airmon-ng check.

PROGRAM:

Sudo airmon -ng

Compat-wireless-2010-06-28.tar.tz2(download from chrome)

cd Downloads

cd Compat-wireless-2010-06-28

sudo make unload

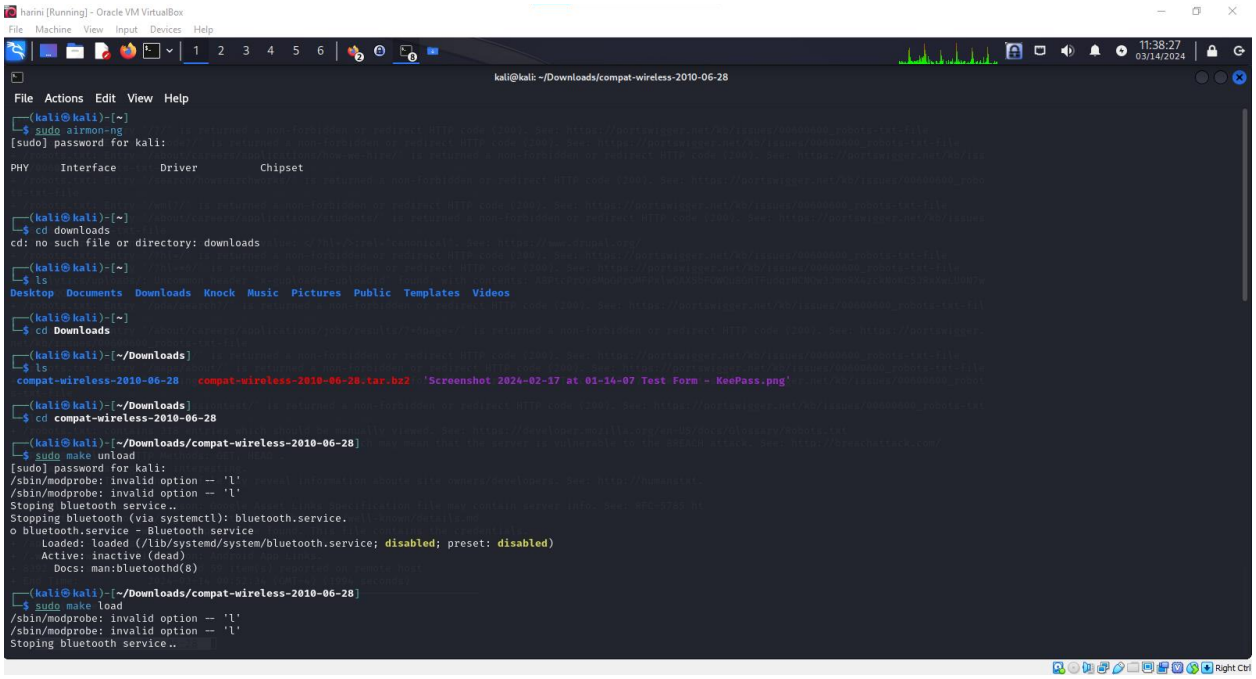
sudo make load

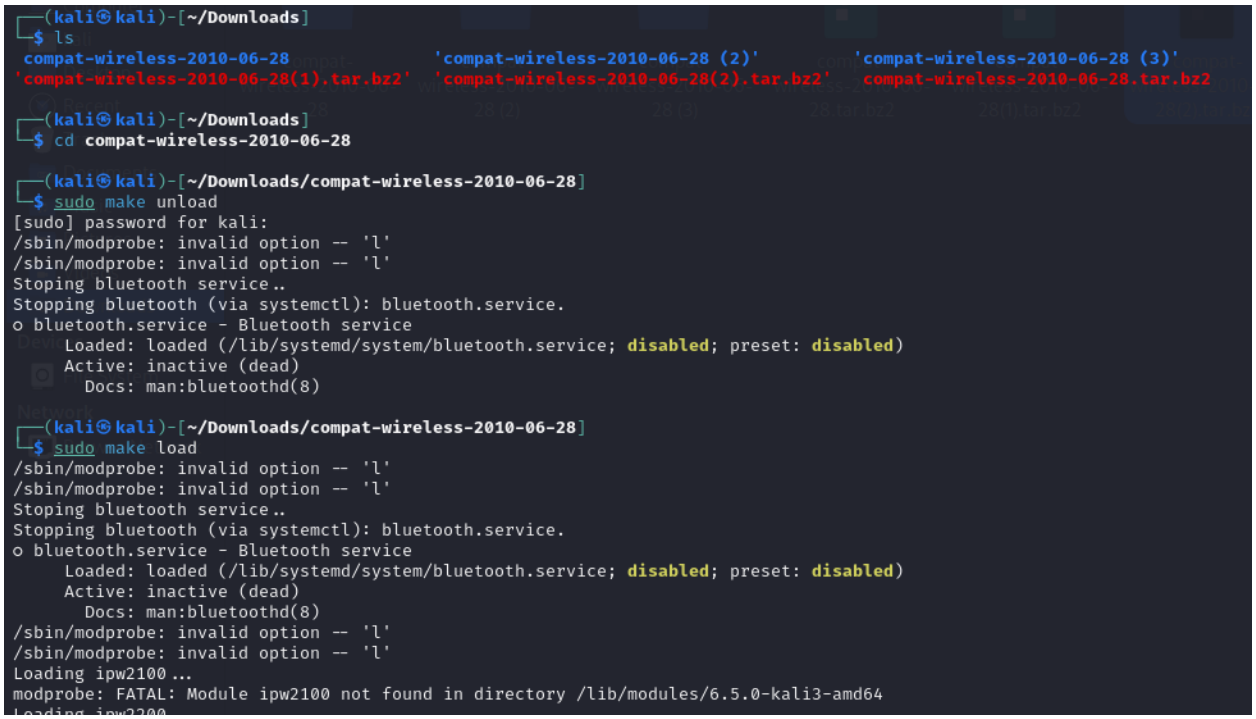
sudo airmon-ng check

sudo airmon-ng kill

sudo airmon –ng start wlan0

COMMAND OUTPUT:





FINAL REPORT:

```
┌──(kali㉿kali)-[~/Downloads/compat-wireless-2010-06-28]
└─$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off

wlan1     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off

hwsim0    no wireless extensions.


┌──(kali㉿kali)-[~/Downloads/compat-wireless-2010-06-28]
└─$ sudo airmon-ng

PHY     Interface       Driver          Chipset

phy0    wlan0           mac80211_hwsim  Software simulator of 802.11 radio(s) for mac80211
phy1    wlan1           mac80211_hwsim  Software simulator of 802.11 radio(s) for mac80211


┌──(kali㉿kali)-[~/Downloads/compat-wireless-2010-06-28]
```

RESULT:

Monitor mode was enabled successfully.

EX:NO:04 **FIND THE KNOWN AND OPEN VULNERABILITIES OF**

DATE: 11.01.2024 **SYSTEM USING METASPLOIT**

AIM:

To find the known and open vulnerabilities of system using metasploit.

ALGORITHM:

Step1: Accessing msfconsole.

Step2: We configure RHOSTS with the IP/IP(s) of our machine(s), and if we want we can modify the scan for certain ports by setting PORTS.

Step3: To set a RHOSTS, PORTS and THREADS for identifying vulnerabilities.

Step4: We can begin enumerating them in order to observe and locate the operating services, as well as their versions.

db_nmap -sV -p 25,80, 22 192.168.56.103

Step5: Auxiliary module execution was successfully completed.

Step6: To display the vulnerabilities of an system was displayed using the command **info –d**

PROGRAM:

msfconsole

auxiliary/scanner/portscan/tcp

show options

set RHOSTS 192.168.56.103

set PORTS 22,25,8,110,21

set THREADS 3

run

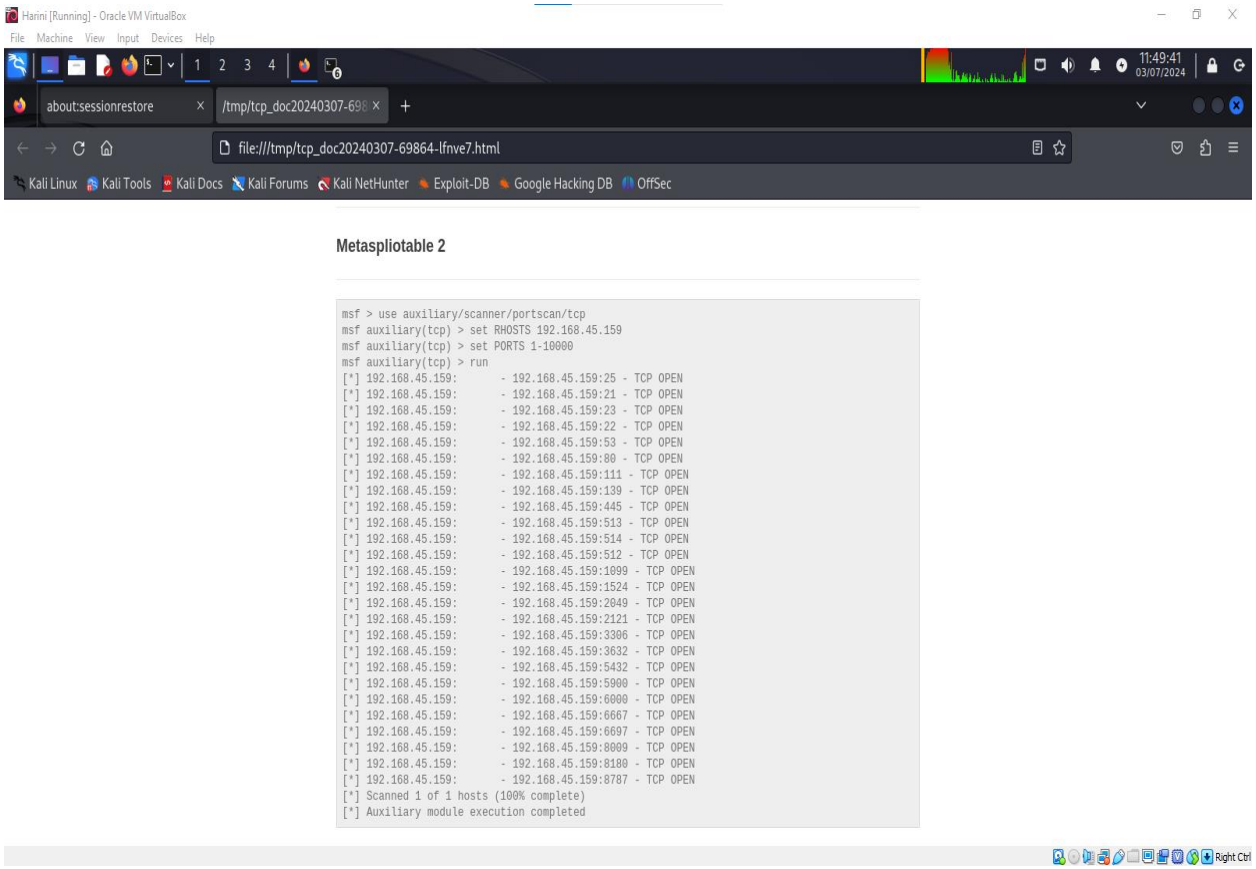
Indo –d

COMMAND OUTPUT:

```
root@kali:~# msfconsole

  METASPLOIT by Rapid7

       =[ metasploit v5.0.60-dev                          ]
+ -- --=[ 1947 exploits - 1089 auxiliary - 333 post       ]
+ -- --=[ 556 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

msf5 > use auxiliary/scanner/portscan/tcp
msf5 auxiliary(scanner/portscan/tcp) > show options

Module options (auxiliary/scanner/portscan/tcp):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   CONCURRENCY 10               yes       The number of concurrent ports to check per host
   DELAY       0                yes       The delay between connections, per thread, in milliseconds
   JITTER      0                yes       The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
   PORTS       1-10000          yes       Ports to scan (e.g. 22-25,80,110-900)
   RHOSTS                       yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   THREADS     1                yes       The number of concurrent threads (max one per host)
   TIMEOUT     1000             yes       The socket connect timeout in milliseconds

msf5 auxiliary(scanner/portscan/tcp) >
```

```
msf6 > use auxiliary/scanner/portscan/tcp
msf6 auxiliary(scanner/portscan/tcp) > show options

Module options (auxiliary/scanner/portscan/tcp):

   Name        Current Setting  Required  Description
   ----        ---------------  --------  -----------
   CONCURRENCY 10               yes       The number of concurrent ports to check per host
   DELAY       0                yes       The delay between connections, per thread, in milliseconds
   JITTER      0                yes       The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.
   PORTS       1-10000          yes       Ports to scan (e.g. 22-25,80,110-900)
   RHOSTS                       yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   THREADS     1                yes       The number of concurrent threads (max one per host)
   TIMEOUT     1000             yes       The socket connect timeout in milliseconds

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/portscan/tcp) > set RHOSTS 192.168.56.103
RHOSTS => 192.168.56.103
msf6 auxiliary(scanner/portscan/tcp) > set PORTS 22,25,0,110,21
PORTS => 22,25,0,110,21
msf6 auxiliary(scanner/portscan/tcp) > set THREADS 3
THREADS => 3
msf6 auxiliary(scanner/portscan/tcp) > run

[*] 192.168.56.103:       - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/portscan/tcp) >
```

FINAL REPORT:



RESULT:

System vulnerabilities are open using Metasploit was executed successfully.

EX: NO: 05 **IDENTIFY THE MULTIPLE VULNERABILITIES OF**

DATE: 24.01.2024 **WEB SERVER USING NIKTO TOOL**

AIM:

To identify the multiple vulnerabilities of an web server using nikto tool.

ALGORITHM:

Step1: Nikto is an open source web server. It also checks for server configuration items such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software.

Step2: Nikto is usually pre-installed on Kali Linux. However, if it's not, you can install it using the following command:

nikto –h <target>

Step3: If the target web server is using HTTPS, you'll need to specify the -ssl option to enable SSL scanning:

nikto –h <target> -ssl

Step4: If the target web server requires authentication, you can provide credentials using the -id option:

nikto –h <target> -id <username>:<password>

Step5: while Nikto is a powerful tool, it's important to use it responsibly and with permission. Scanning web servers without authorization can be illegal and may lead to serious consequences. Always ensure you have the necessary permissions before scanning any web server.

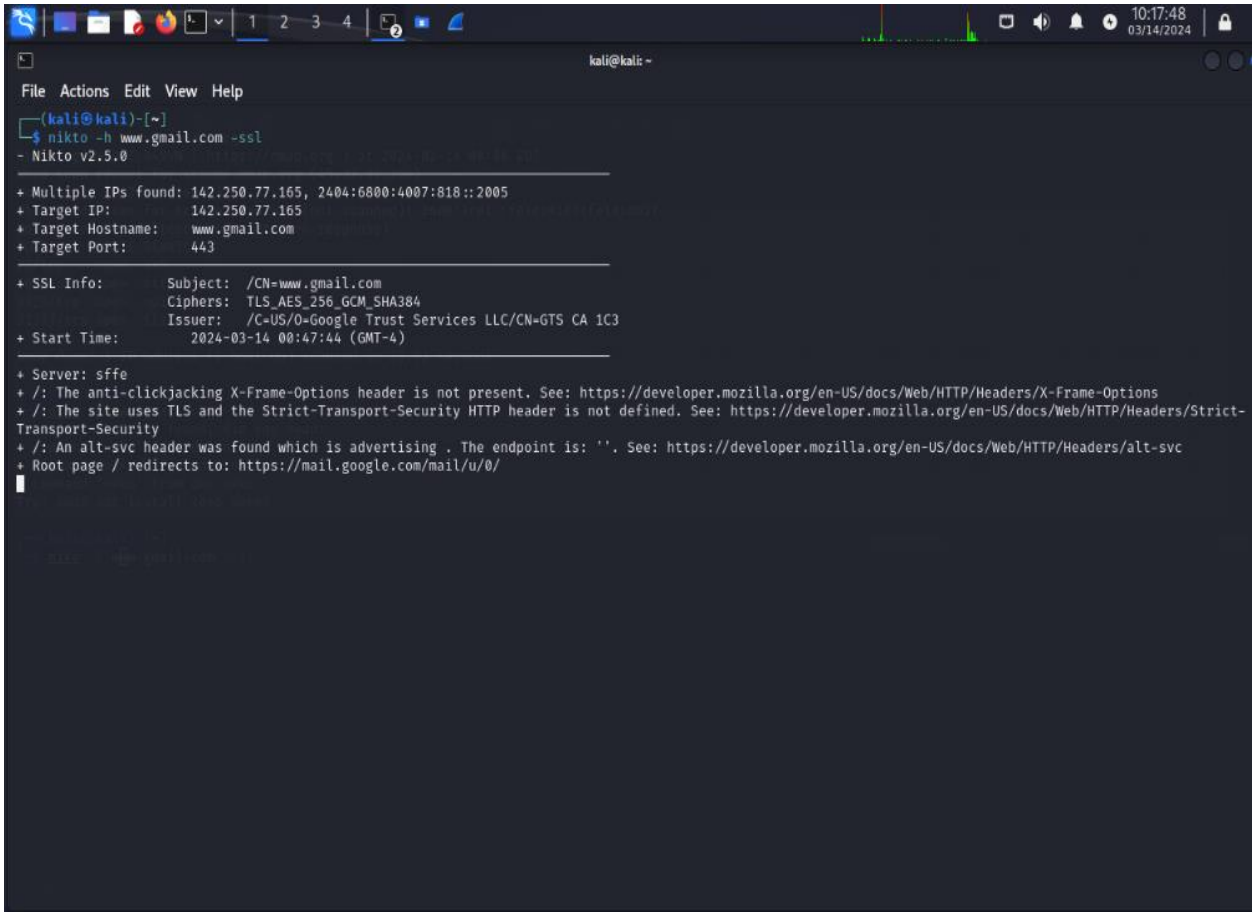
(command:for example: nikto –h www.google.com –ssl)

PROGRAM:

Sudo apt-get install nikto

Nikto –h www.google.com

FINAL REPORT:



```
(kali@kali)-[~]
$ nikto -h www.gmail.com -ssl
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 142.250.77.165, 2404:6800:4007:818::2005
+ Target IP:          142.250.77.165
+ Target Hostname:    www.gmail.com
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=www.gmail.com
                   Ciphers:  TLS_AES_256_GCM_SHA384
                   Issuer:   /C=US/O=Google Trust Services LLC/CN=GTS CA 1C3
+ Start Time:         2024-03-14 00:47:44 (GMT-4)
---------------------------------------------------------------------------
+ Server: sffe
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-
Transport-Security
+ /: An alt-svc header was found which is advertising . The endpoint is: ''. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/alt-svc
+ Root page / redirects to: https://mail.google.com/mail/u/0/
```

RESULT:

Thus the multiple vulnerabilities of an web server was identified using nikto tool successfully.

EX.NO:06 **IDENTIFY THE OPEN PORTS IN NETWORK**

DATE: 12.02.2024 **USING NMAP TOOLS**

AIM:

To identify the open ports i network using nmap tools in Kali Linux.

ALGORITHM:

STEP 1: Nmap is a utility for network exploration. It supports ping scanning (determine host are up), many ports scanning techniques, version detection, service protocols, TCP/IP fingerprinitng. It offers target and port specification.

STEP 2: To install nmap Tool to using this command

Sudo apt install nmap

Size: 4.4 mb

STEP 3: Command for open ports in network.

nmap –pn scanme.nmap.org

[-p<port ranges> is only scan specified ports and overrifes the default]

Website: **nmap.org**

PROGRAM:

```
sudo apt install nmap
nmap –Pn scanme.nmap.org
```

FINAL REPORT:

RESULT:

Thus the program was executed successfully.

EX.NO:07 **LIST ALL THE NETWORK AROUND US AND DISPLAY**

DATE:20.02.2024 **THE INFORMATION ABOUT NETWORKS**

AIM:

To listing the entire network around us with information of the network using Kali Linux.

ALGORITHM:

STEP 1: Use a tool nmap for displaying the information of networks around us. Nmap short for network mapper, it is a powerful open source network scanning tool used for network discovery and security auditing. To install nmap tool with this command

sudo apt –get install nmap.

STEP 2: Next figure out your network address by using **ifconfig.** It display network interfaces on system including ip address and mac address and network related statistics

STEP 3: Use inet addr and mask to figure out network address in CIDR notation.

STEP 4: sudo nmap 10.0.2.15/24

This command displays all the network around us with information of that Network.

STEP 5: Also the command

n.mzp –SA 10.0.2.15/24

The flag –sp used to know the list of connected devices.

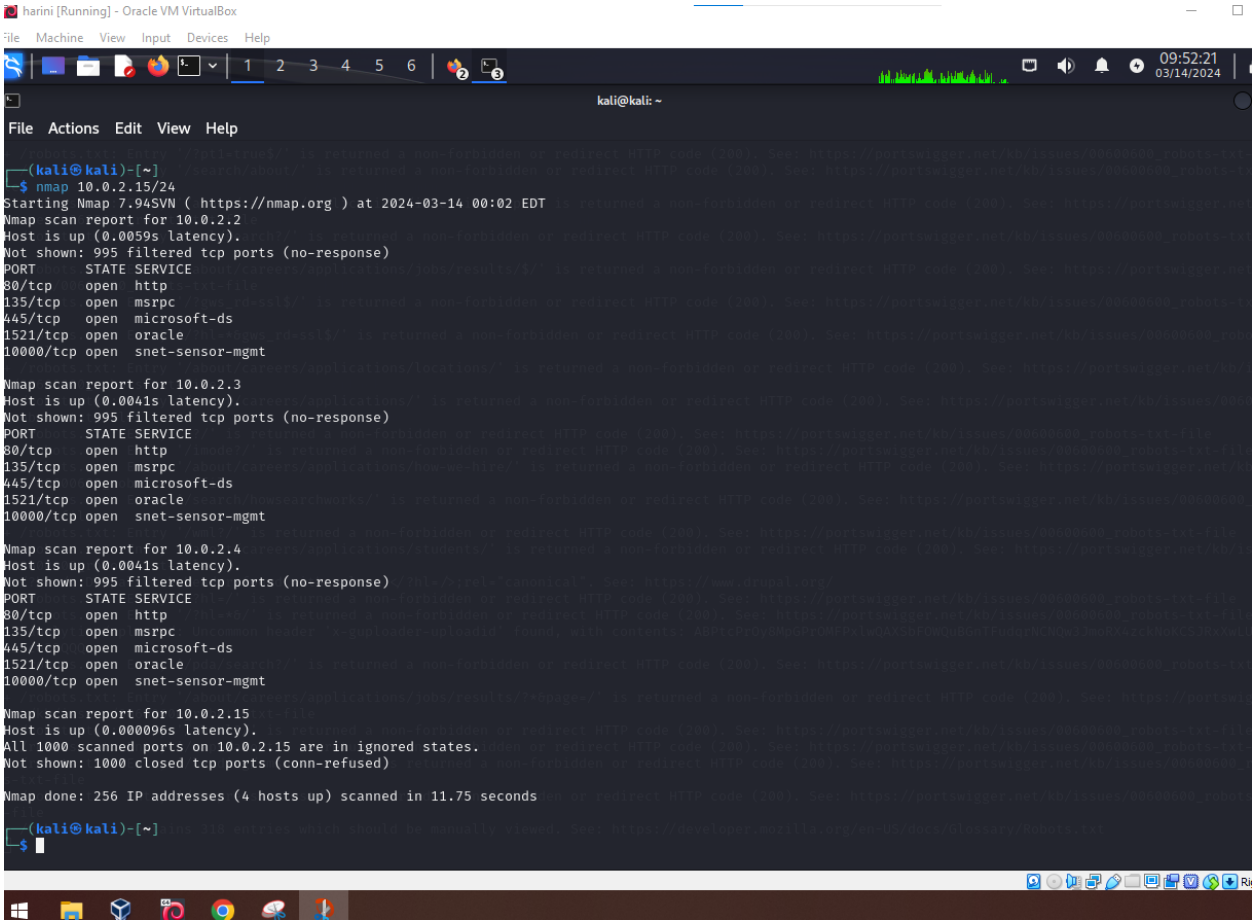
PROGRAM

Sudo apt install nmap

ifconfig

sudo nmap 10.0.2.15/24

FINAL REPORT:



RESULT:

Thus the program was executed successfully.

EX.NO.08 **SNIFF AND CAPTURE THE PACKET**

DATE:28.02.2024 **SENT OVER HTTP REQUESTS**

AIM:

To sniffing and capture the packets sent over HTTP requests.

ALGORITHM:

STEP 1: Wireshark helps diagnose and resolve network issues by capturing and analyzing network packets to identify errors and misconfigurations. To install wireshark package.

Sudo apt –get install wireshark

STEP 2: Launch wireshark: **sudo wireshark**

STEP 3: Choose network Interface to capture packets from (eg.eth0) or wifi interface

(eg. Wlan0).

STEP 4: Click to start the capture Ethernet (eth0).

STEP 5: Filter HTTP traffic -> clear history, clear capche on browser settings. Enter http, in display title bar to showing http packets.

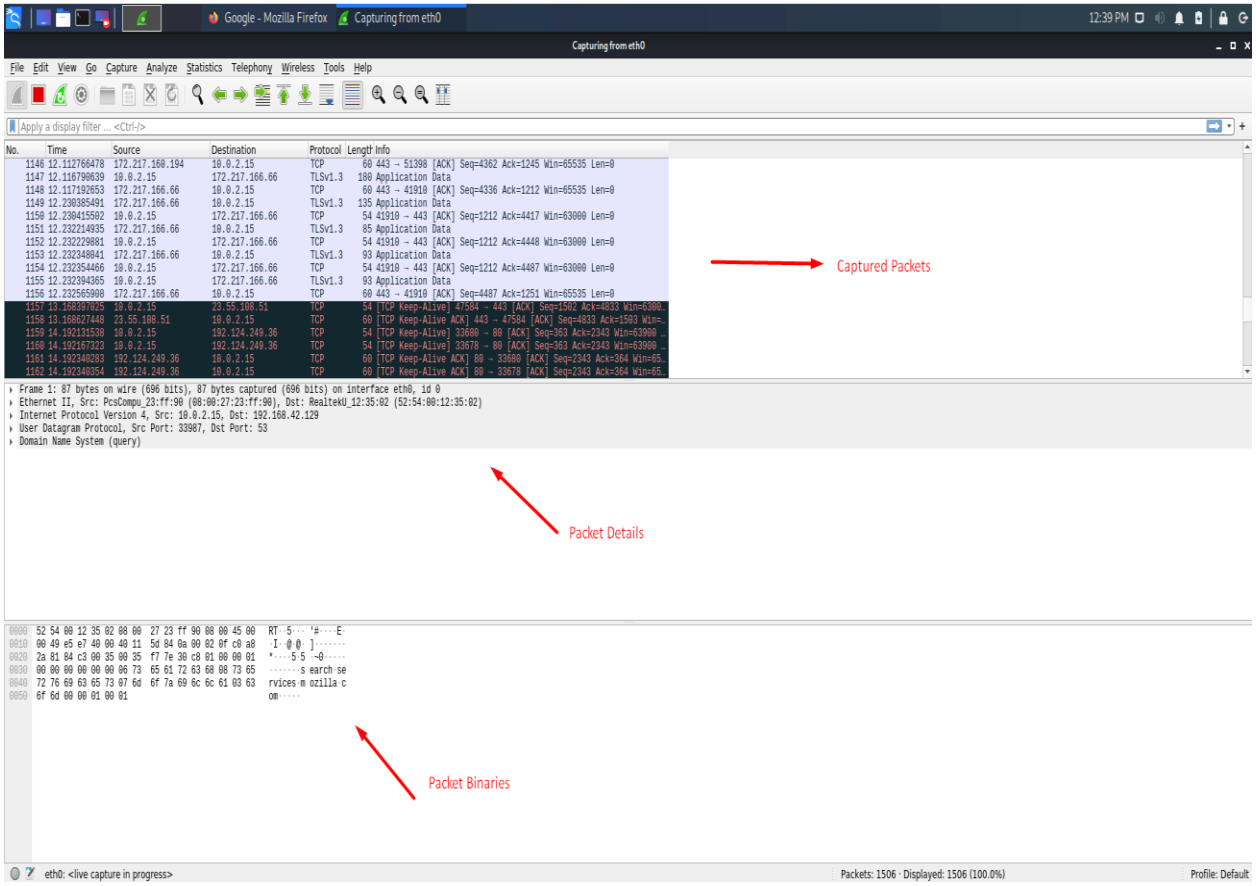
STEP 6: When you are done capturing packets. Click the 'stop' button in wireshark.

PROGRAM:

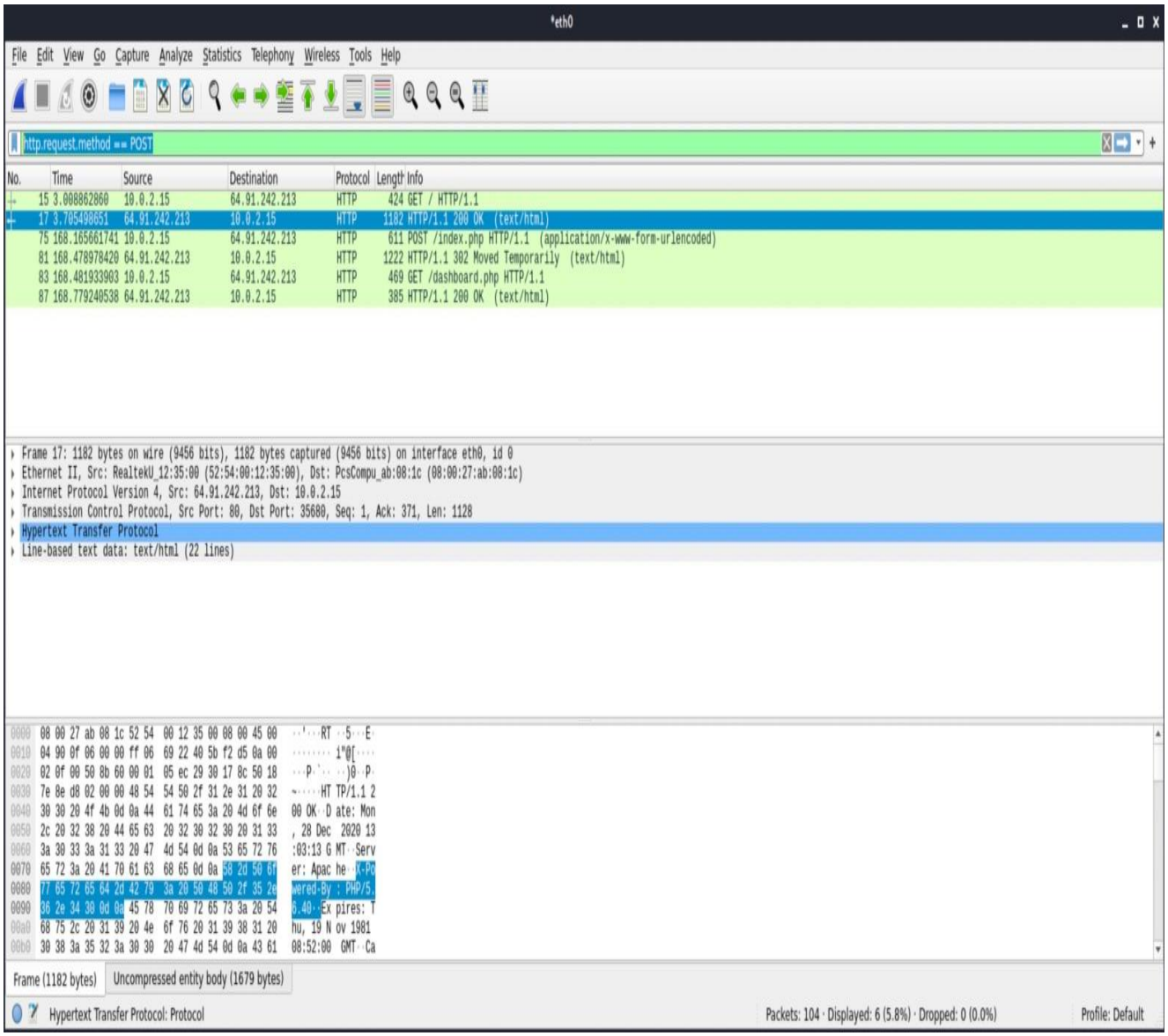
sudo apt-get install wireshark

sudo wireshark

COMMAND OUTPUT:



FINAL REPORT:



RESULT:

Thus the program was executed successfully.

EX.NO.09 **FIND THE OWNERS OF INTERNET RESOURCES**

DATE:14.03.2024 **USING WHOIS LOOK UP TOOL**

AIM:

To find the owners of internet resources using whois tool.

ALGORITHM :

STEP 1: Whois tool in kali linux is used to query WHOID databeases to retrieve information about domain registrations ip addresses and other related informations it is commonly used for investigated domain ownership and gathering information about network.

STEP 2: Open a terminal window in Kali Linux.Use the 'whois' command followed by the domain name or IP address you want to look up. Replace "example.com" with the domain name or IP address you want to look up.

For Example: **Whois example.com**

STEP 3: Press enter.

STEP 4: The whois database will provide you with information about the domain name

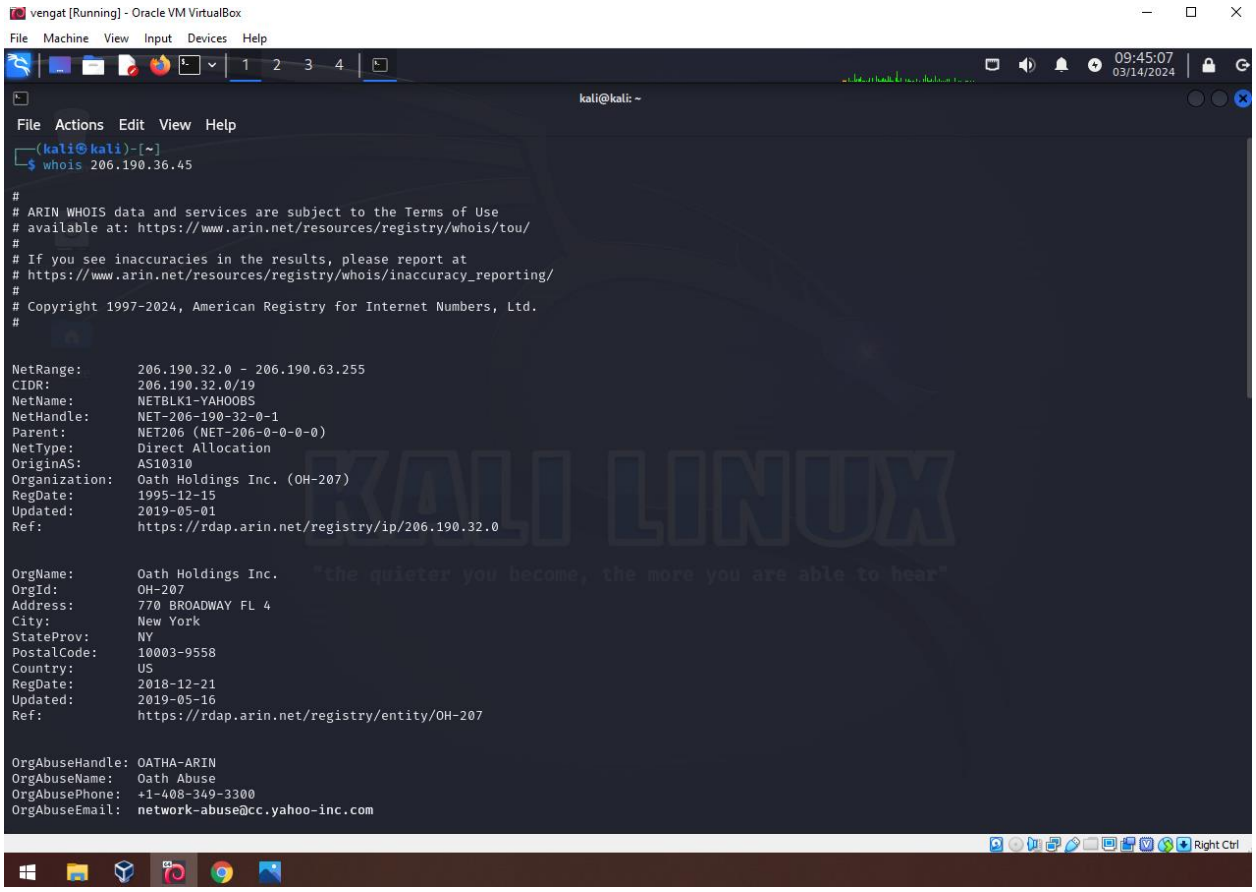
Or IP address, including details such as the registrar, registeration date, expiry

Date, and sometimes contact information of the owner.

PROGRAM:

```
sudo apt update

sudo apt upgrade

whois 206.190.36.45
```

FINAL REPORT:



RESULT:

Thus the program was executed successfully.

EX:NO:10 **FIND THE SUB DOMAINS OF WEBPAGE**

DATE: 14.03.2024 **USING KNOCK TOOL**

AIM:

To find the subdomains of webpage using knock tool.

ALGORITHM:

Step: 1 Knock tool is used for port knocking, a security technique is used to open ports on a fire wall by sending a sequence of connection attempts to predefined ports.

Step:2 To clone the tool from the GitHub repository by using the below command

git clone https://github.com/santiko/KnockPy.git .

Then Change to your preferred directory

cd KnockPy

Step:3 To run the tool and to know its options, type the following command.

python knock.py –h

Step:4 To show version of the tool, enter the command:

python knock.py –v

Step:5 To find out short information about any domain, enter the command

python knock.py -i domain name (which in our case is google.com)

Step: 6 To get the subdomain of a website, type the following command.

python knock.py tesla.com.

PROGRAM:

sudo apt-get install knockpy

git clone https://github.com/santiko/knockpy.git(chrome)

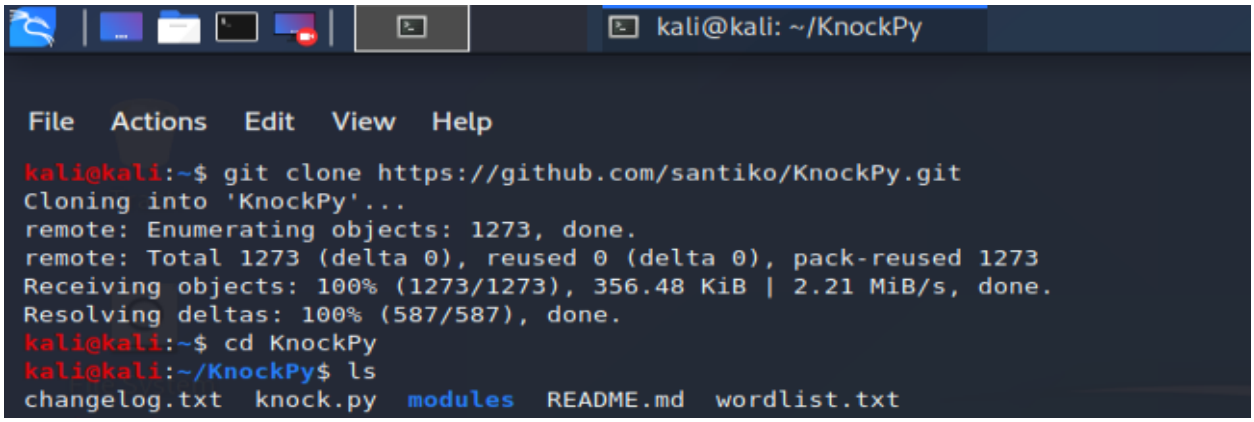
cd knockpy

knockpy google.com

knockpy –d google.com

knockpy –d facebook.com –recon –bruteforce.

COMMAND OUTPUT:



FINAL REPORT:

```
199.66.9.90     warehouse.tesla.com
.txt104.109.3.63        www.tesla.com
104.109.3.63    a104-109-3-63.deploy.static.akamaitechnologies.com
104.109.3.63    www.tesla.com.edgekey.net
104.109.3.63    e1792.dscx.akamaiedge.net
204.74.99.100   xmail.tesla.com

Ip Addr Summary
---------------
23.35.46.196
104.109.3.63
23.64.133.137
13.111.47.195
23.35.44.156
162.159.128.79
13.111.47.196
209.133.79.82
40.100.138.18
8.45.124.215
199.66.9.90
204.74.99.100

Found 48 subdomain(s) in 12 host(s).
kali@kali:~/KnockPy$
```

RESULT:

The sub domain of web page was identified using knock tool successfully.