

## **CONTENT**

<b>S.No</b>	<b>DATE</b>	<b>TITLE</b>	<b>PAGE</b>	<b>SIGNATURE</b>
01	21.12.2023	INSTALL VIRTUVAL BOX (KALI LINUX)		
02	03.01.2024	GENERA E 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](http://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.

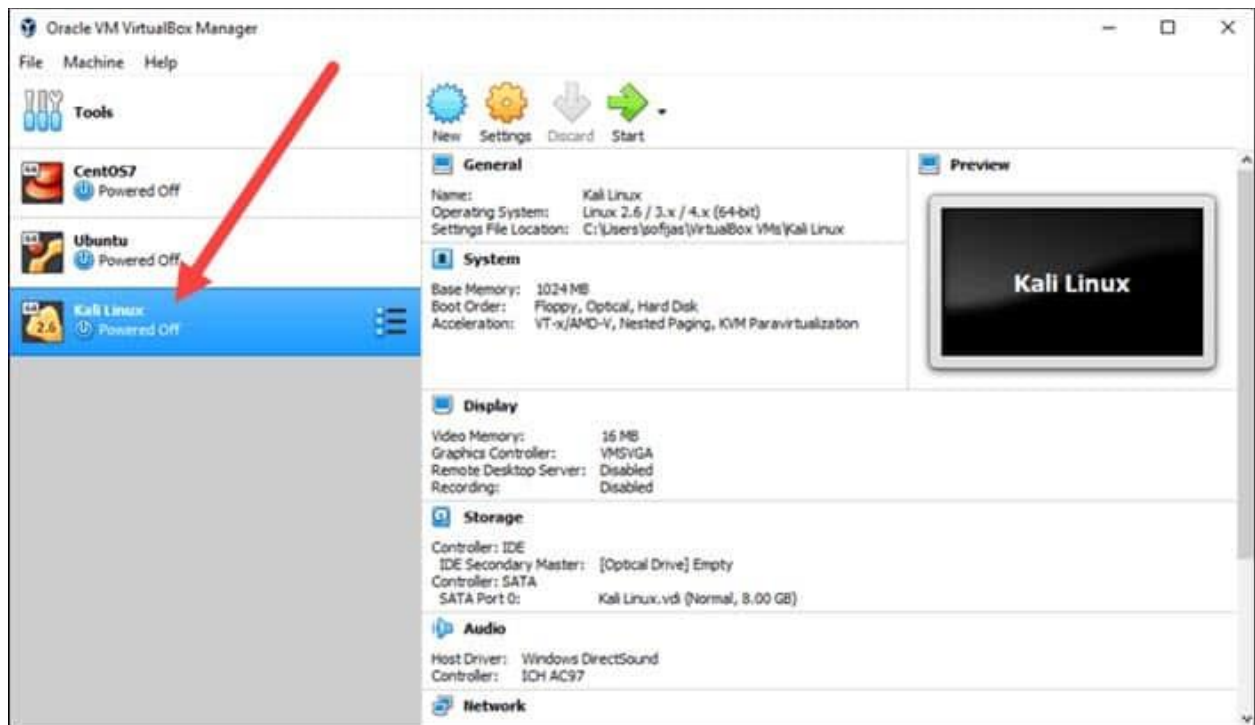
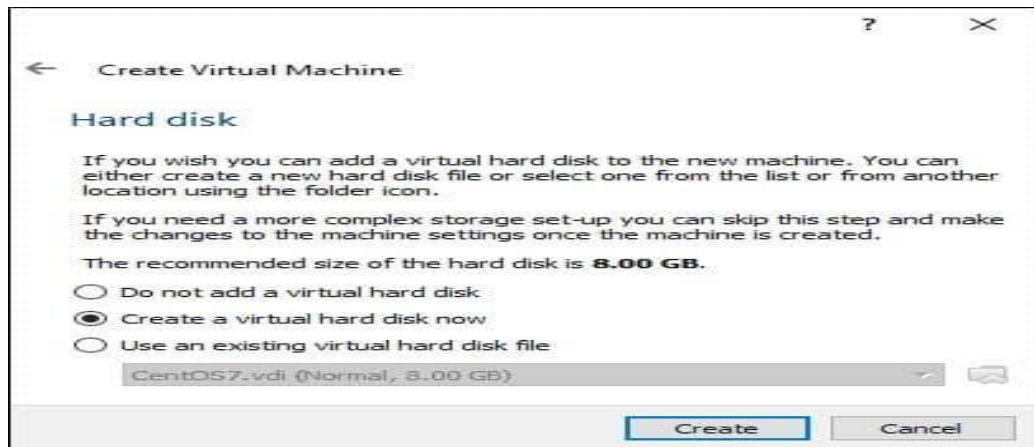
**Step4:** The default option is to create a virtual hard disk for the new VM. Click Create to continue.

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.



## 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

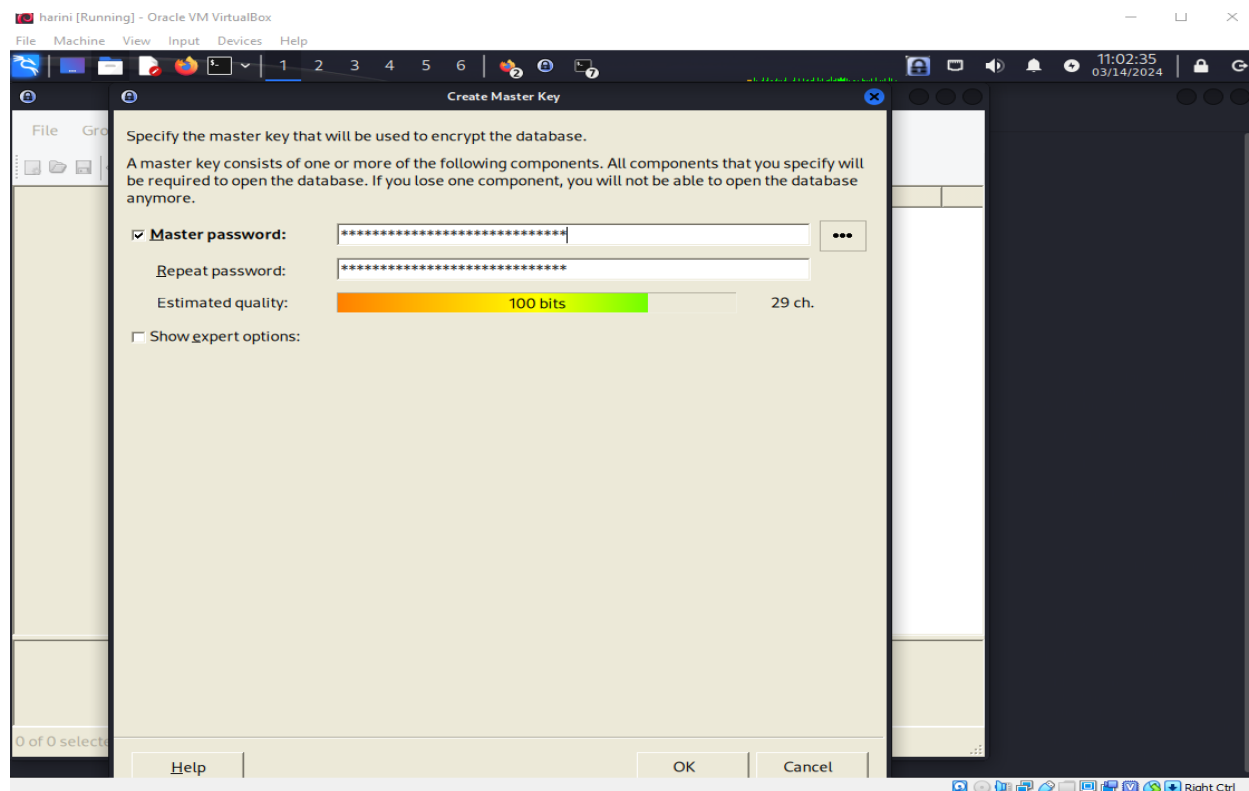
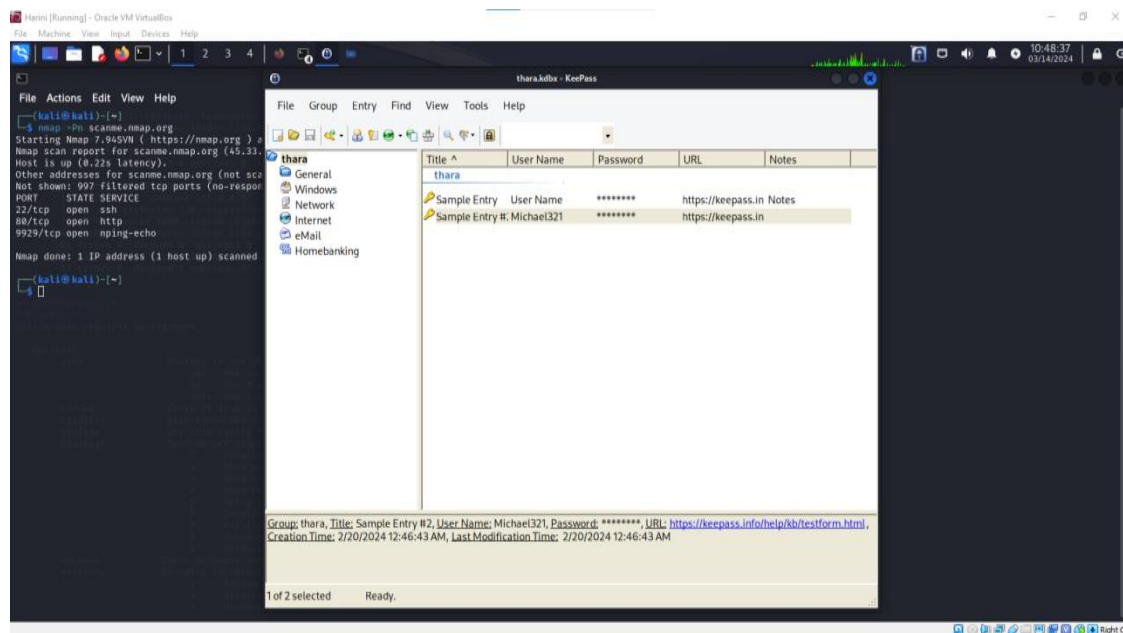
### PROGRAM

Sudo apt-get update

Sudo apt install keepass2

Keepass2

## COMMAND OUTPUT:



## FINAL REPORT:

The screenshot displays a password manager application window. At the top is a menu bar with 'Database', 'Entries', 'Groups', 'Tools', 'View', and 'Help'. Below the menu is a toolbar with various icons for file operations, editing, and search. A search bar on the right of the toolbar contains the text 'Search (Ctrl+F)...'. The main area is titled 'Root • Add entry'. On the left is a vertical sidebar with icons and labels: 'Entry' (pencil icon), 'Advanced' (document icon), 'Icon' (smiley face icon), 'Auto-Type' (keyboard icon), and 'Properties' (document icon). The main form contains the following fields: 'Title' (empty text box), 'Username' (text box with a dropdown arrow), 'Password' (text box with a toggle icon and a lock icon), 'URL' (text box containing 'https://example.com' with a download icon), 'Tags' (empty text box), 'Expires' (checkbox and a date/time picker showing '3/21/24 3:06 AM' with a 'Presets' dropdown), and 'Notes' (a large text area). At the bottom right are 'OK' and 'Cancel' buttons. The status bar at the bottom right shows '0 Entries'.

Database Entries Groups Tools View Help

Search (Ctrl+F)...

Root • Add entry

Entry

Advanced

Icon

Auto-Type

Properties

Title:

Username:

Password:

URL: https://example.com

Tags:

Expires: ☐ 3/21/24 3:06 AM Presets

Notes:

OK Cancel

0 Entries

## 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 exist 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:

```
harini [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~/Downloads/compat-wireless-2010-06-28

(kali@kali)~$ sudo airmon-ng
[sudo] password for kali:
PHY      Interface      Driver      Chipset

(kali@kali)~$ cd downloads
cd: no such file or directory: downloads

(kali@kali)~$ ls
Desktop Documents Downloads Knock Music Pictures Public Templates Videos

(kali@kali)~$ cd Downloads

(kali@kali)~/Downloads$ ls
compat-wireless-2010-06-28  compat-wireless-2010-06-28.tar.bz2  'Screenshot 2024-02-17 at 01:14-07 Test Form - KeePass.png'

(kali@kali)~/Downloads$ cd compat-wireless-2010-06-28

(kali@kali)~/Downloads/compat-wireless-2010-06-28$ sudo make unload
[sudo] password for kali:
/sbin/modprobe: invalid option -- 'l'
/sbin/modprobe: invalid option -- 'l'
Stopping bluetooth service..
Stopping bluetooth (via systemctl): bluetooth.service.
o bluetooth.service - Bluetooth service
   Loaded: loaded (/lib/systemd/system/bluetooth.service; disabled; preset: disabled)
   Active: inactive (dead)
     Docs: man:bluetoothd(8)

(kali@kali)~/Downloads/compat-wireless-2010-06-28$ sudo make load
/sbin/modprobe: invalid option -- 'l'
/sbin/modprobe: invalid option -- 'l'
Stopping bluetooth service..
```

```
(kali@kali)~/Downloads$ ls
compat-wireless-2010-06-28      'compat-wireless-2010-06-28 (2)'      'compat-wireless-2010-06-28 (3)'
'compat-wireless-2010-06-28(1).tar.bz2'  'compat-wireless-2010-06-28(2).tar.bz2'  compat-wireless-2010-06-28.tar.bz2

(kali@kali)~/Downloads$ cd compat-wireless-2010-06-28

(kali@kali)~/Downloads/compat-wireless-2010-06-28$ sudo make unload
[sudo] password for kali:
/sbin/modprobe: invalid option -- 'l'
/sbin/modprobe: invalid option -- 'l'
Stopping bluetooth service..
Stopping bluetooth (via systemctl): bluetooth.service.
o bluetooth.service - Bluetooth service
   Loaded: loaded (/lib/systemd/system/bluetooth.service; disabled; preset: disabled)
   Active: inactive (dead)
     Docs: man:bluetoothd(8)

(kali@kali)~/Downloads/compat-wireless-2010-06-28$ sudo make load
/sbin/modprobe: invalid option -- 'l'
/sbin/modprobe: invalid option -- 'l'
Stopping bluetooth service..
Stopping bluetooth (via systemctl): bluetooth.service.
o bluetooth.service - Bluetooth service
   Loaded: loaded (/lib/systemd/system/bluetooth.service; disabled; preset: disabled)
   Active: inactive (dead)
     Docs: man:bluetoothd(8)
Loading ipw2100...
modprobe: FATAL: Module ipw2100 not found in directory /lib/modules/6.5.0-kali3-amd64
Loading ipw2200...
```

## 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
```

The screenshot shows a Kali Linux desktop environment with a terminal window open. The terminal displays the output of the command `msf5 auxiliary(scanner/portscan/tcp) > show options`. The output lists module options for the `auxiliary/scanner/portscan/tcp` module.

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

The terminal also shows the command prompt `msf5 auxiliary(scanner/portscan/tcp) >`.

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

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

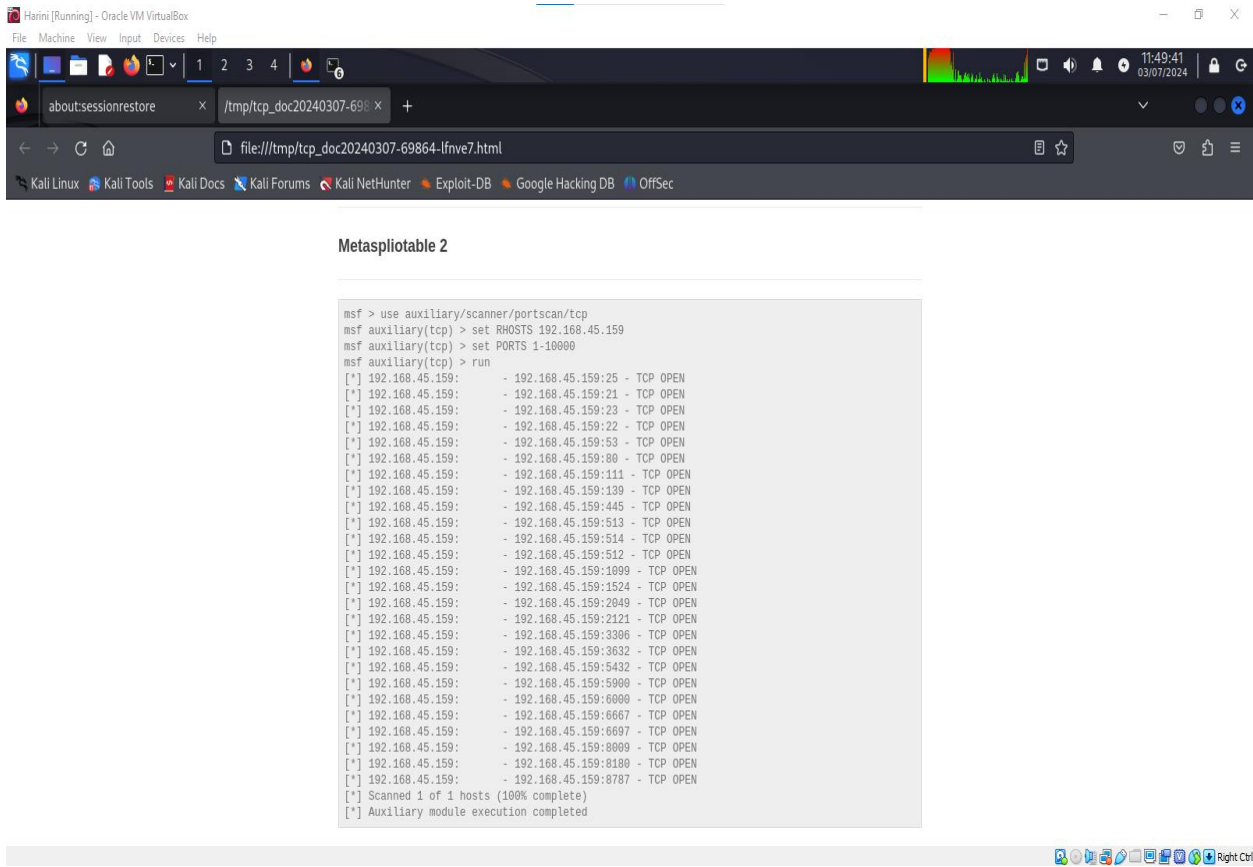
  Name           Current Setting  Required  Description
  --
  CONCURRENCY    10              yes       The number of concurrent ports to check per host
  DELAY          0               yes       The delay between connections, per thread, in milliseconds
  JITTER         0               yes       The delay 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         192.168.56.103  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.

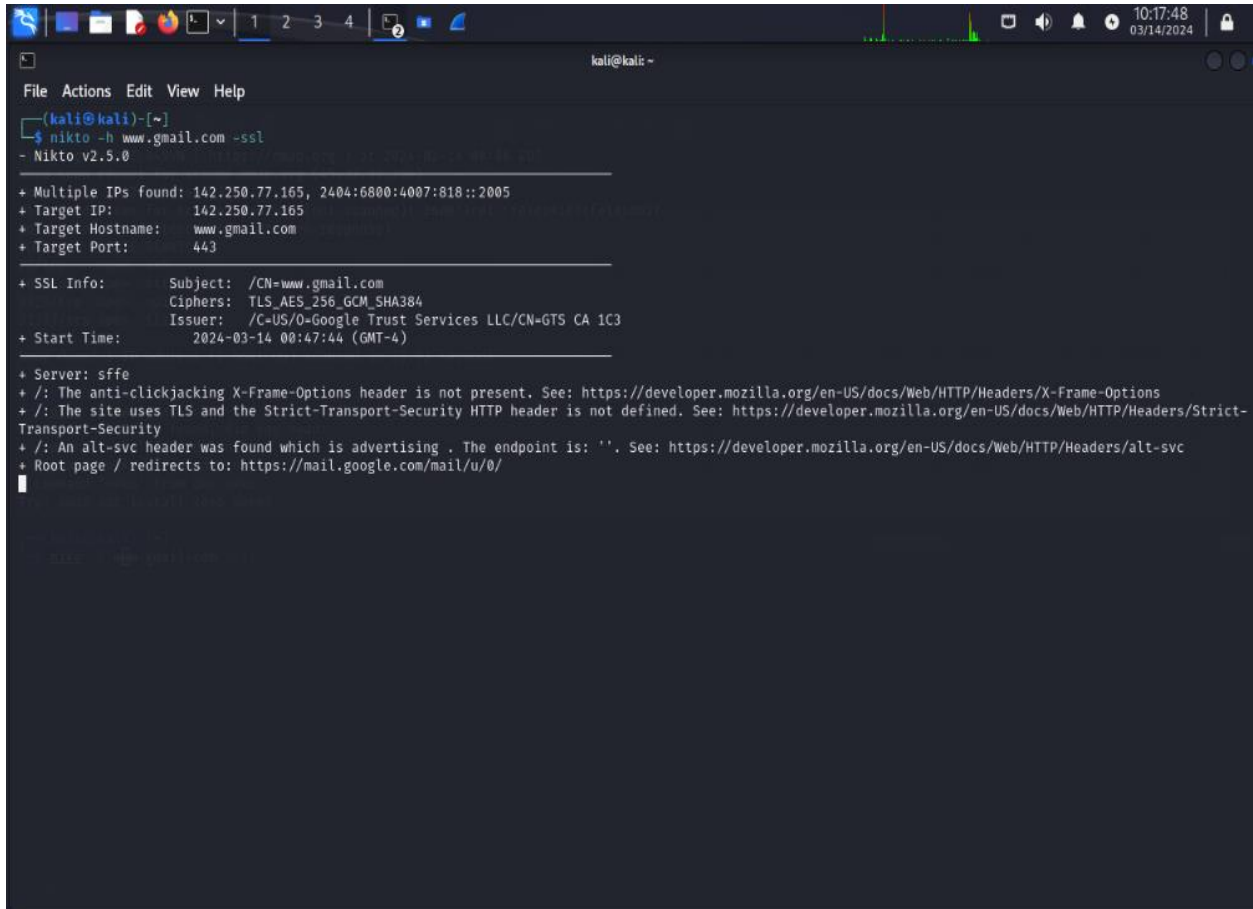
(command:for example: nikto -h [www.google.com](http://www.google.com) -ssl)

### PROGRAM:

```
Sudo apt-get install nikto
```

```
Nikto -h www.google.com
```

## FINAL REPORT:



```
kali@kali: ~  
File Actions Edit View Help  
(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 in 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 fingerprinting. 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 overrides the default]**

**Website: nmap.org**

#### **PROGRAM:**

**sudo apt install nmap**

**nmap -Pn scanme.nmap.org**



## FINAL REPORT:



The screenshot shows a Kali Linux virtual machine window titled 'vengat [Running] - Oracle VM VirtualBox'. The terminal window is titled 'kali@kali: ~' and displays the output of an Nmap scan. The scan was performed on 'scanme.nmap.org' (45.33.32.156) at 2024-03-14 00:46 EDT. The output shows that the host is up with a latency of 0.22s. Other addresses for scanme.nmap.org (not scanned) are listed as 2600:3c01::f03c:91ff:fe18:bb2f. The scan also shows 998 filtered TCP ports (no-response). The open ports are 22/tcp (ssh) and 80/tcp (http). The scan was completed in 17.44 seconds.

```
(kali@kali)-[~]  
$ nmap -Pn scanme.nmap.org  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-14 00:46 EDT  
Nmap scan report for scanme.nmap.org (45.33.32.156)  
Host is up (0.22s latency).  
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f  
Not shown: 998 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
22/tcp    open  ssh  
80/tcp    open  http  
  
Nmap done: 1 IP address (1 host up) scanned in 17.44 seconds  
  
(kali@kali)-[~]  
$
```

## 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

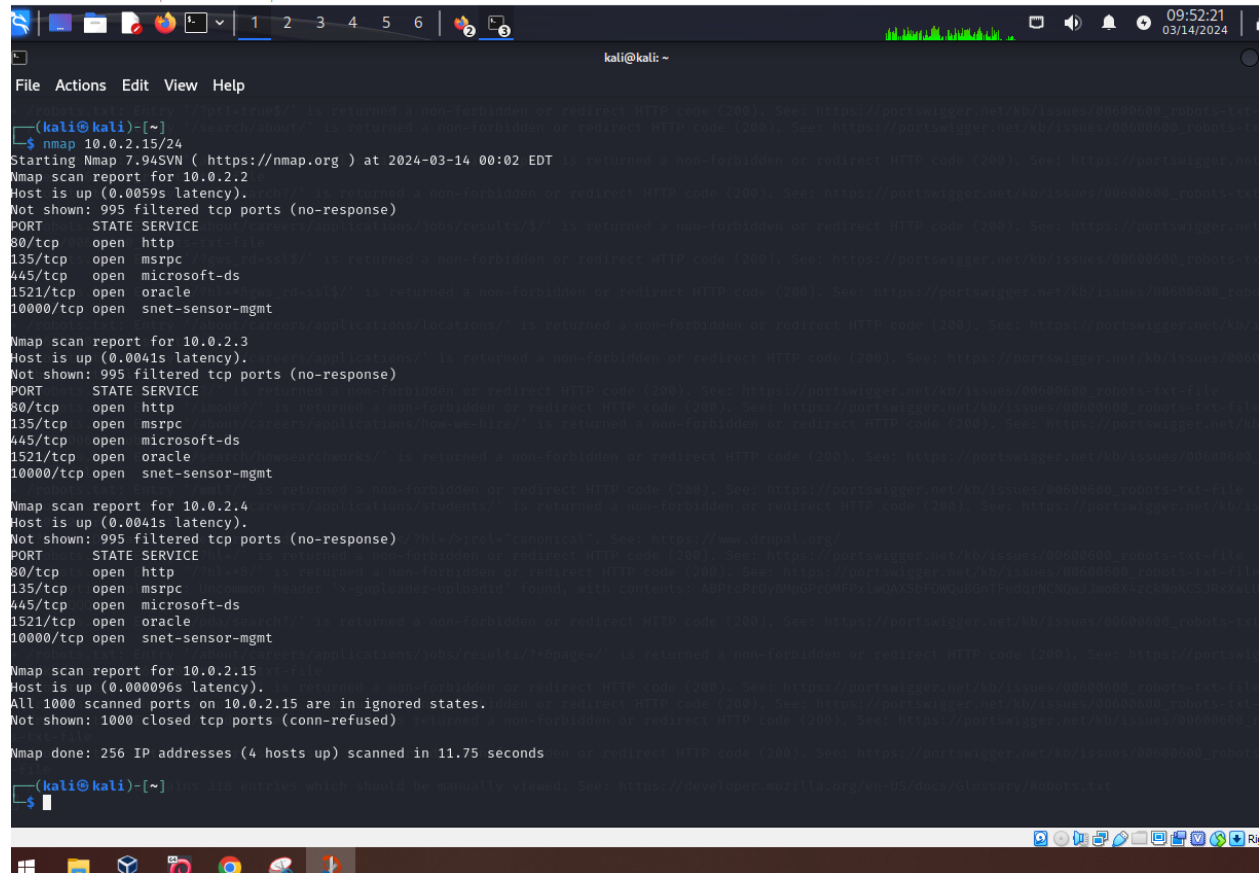
ifconfig

sudo nmap 10.0.2.15/24

## FINAL REPORT:

harini [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help



```
(kali@kali)-[~]
└─$ nmap 10.0.2.15/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-14 00:02 EDT
Nmap scan report for 10.0.2.2
Host is up (0.0059s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
1521/tcp  open  oracle
10000/tcp open  snet-sensor-mgmt

Nmap scan report for 10.0.2.3
Host is up (0.0041s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
1521/tcp  open  oracle
10000/tcp open  snet-sensor-mgmt

Nmap scan report for 10.0.2.4
Host is up (0.0041s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
1521/tcp  open  oracle
10000/tcp open  snet-sensor-mgmt

Nmap scan report for 10.0.2.15
Host is up (0.00096s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap done: 256 IP addresses (4 hosts up) scanned in 11.75 seconds
```

## 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:

The image shows a Wireshark network traffic capture interface. The top bar indicates the capture is running on interface eth0. The main window is divided into three panes: a packet list, a packet details pane, and a packet bytes pane.

**Packet List:** A table showing captured packets. The columns are No., Time, Source, Destination, Protocol, and Length. The first 15 packets are highlighted in blue, indicating they are the selected packet's details. A red arrow points to this list with the label "Captured Packets".

No.	Time	Source	Destination	Protocol	Length	Info
1149	12.112766478	172.217.166.194	10.0.2.15	TCP	60	443 → 51398 [ACK] Seq=4362 Ack=1245 Win=65535 Len=0
1147	12.116799039	10.0.2.15	172.217.166.66	TLSv1.3	180	Application Data
1148	12.117192953	172.217.166.66	10.0.2.15	TCP	60	443 → 41918 [ACK] Seq=4336 Ack=1212 Win=65535 Len=0
1149	12.23035491	172.217.166.66	10.0.2.15	TLSv1.3	135	Application Data
1150	12.230415502	10.0.2.15	172.217.166.66	TCP	54	41918 → 443 [ACK] Seq=1212 Ack=4417 Win=63000 Len=0
1151	12.232214935	172.217.166.66	10.0.2.15	TLSv1.3	85	Application Data
1152	12.232229861	10.0.2.15	172.217.166.66	TCP	54	41918 → 443 [ACK] Seq=1212 Ack=4448 Win=63000 Len=0
1153	12.232348841	172.217.166.66	10.0.2.15	TLSv1.3	93	Application Data
1154	12.232354466	10.0.2.15	172.217.166.66	TCP	54	41918 → 443 [ACK] Seq=1212 Ack=4487 Win=63000 Len=0
1155	12.232354365	10.0.2.15	172.217.166.66	TLSv1.3	93	Application Data
1156	12.232565908	172.217.166.66	10.0.2.15	TCP	60	443 → 41919 [ACK] Seq=4487 Ack=1251 Win=65535 Len=0
1157	12.232659745	10.0.2.15	172.217.166.66	TCP	54	[TCP Keep-Alive] 41918 → 443 [ACK] Seq=1507 Ack=1503 Win=63000
1158	13.168677448	23.55.188.51	10.0.2.15	TCP	60	[TCP Keep-Alive] 443 → 47584 [ACK] Seq=4833 Ack=1503 Win=63000
1159	14.192131538	10.0.2.15	192.124.249.36	TCP	54	[TCP Keep-Alive] 33678 → 80 [ACK] Seq=363 Ack=2343 Win=63000
1160	14.192167223	10.0.2.15	192.124.249.36	TCP	54	[TCP Keep-Alive] 33678 → 80 [ACK] Seq=363 Ack=2343 Win=63000
1161	14.192340283	192.124.249.36	10.0.2.15	TCP	60	[TCP Keep-Alive] 80 → 33680 [ACK] Seq=2343 Ack=364 Win=65535
1162	14.192340254	192.124.249.36	10.0.2.15	TCP	60	[TCP Keep-Alive] 80 → 33679 [ACK] Seq=2343 Ack=364 Win=65535

**Packet Details:** The details pane shows the structure of the selected packet (No. 1162). It includes fields for Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Domain Name System (query). A red arrow points to this pane with the label "Packet Details".

**Packet Bytes:** The bytes pane shows the raw data of the selected packet in hexadecimal and ASCII. A red arrow points to this pane with the label "Packet Binaries".

0000 52 54 00 12 35 02 08 00 27 23 ff 90 08 00 45 00 RT-5... 'a---E-  
0010 00 49 e5 67 40 00 40 11 50 84 0a 00 02 0f c0 a8 I-0 0 ] .....  
0020 2a 61 84 c3 00 35 00 35 17 7e 30 c3 01 00 00 01 \*...-5-5 -@....  
0030 00 00 00 00 00 00 00 73 65 61 72 63 68 08 73 65 .....s earch se  
0040 72 76 09 63 65 73 07 6d ff 7a 69 6c 6c 61 02 63 rvoices n ozilla c  
0050 6f 6d 00 00 01 00 01 om.....

eth0: <live capture in progress> Packets: 1506 · Displayed: 1506 (100.0%) Profile: Default

## FINAL REPORT:

The image shows a Wireshark packet capture analysis of an HTTP POST request. The top pane displays a list of captured packets, with packet 17 selected. The middle pane shows the details of the selected packet, and the bottom pane shows the raw packet data in hexadecimal and ASCII.

**Packet List:**

No.	Time	Source	Destination	Protocol	Length	Info
15	3.008862860	10.0.2.15	64.91.242.213	HTTP	424	GET / HTTP/1.1
17	3.705498651	64.91.242.213	10.0.2.15	HTTP	1182	HTTP/1.1 200 OK (text/html)
75	168.165661741	10.0.2.15	64.91.242.213	HTTP	611	POST /index.php HTTP/1.1 (application/x-www-form-urlencoded)
81	168.478978429	64.91.242.213	10.0.2.15	HTTP	1222	HTTP/1.1 302 Moved Temporarily (text/html)
83	168.481933903	10.0.2.15	64.91.242.213	HTTP	469	GET /dashboard.php HTTP/1.1
87	168.779240538	64.91.242.213	10.0.2.15	HTTP	385	HTTP/1.1 200 OK (text/html)

**Packet Details:**

- Frame 17: 1182 bytes on wire (9456 bits), 1182 bytes captured (9456 bits) on interface eth0, id 0
- Ethernet II, Src: RealtekU\_12:35:00 (52:54:00:12:35:00), Dst: PcsCompu\_ab:08:1c (08:00:27:ab:08:1c)
- Internet Protocol Version 4, Src: 64.91.242.213, Dst: 10.0.2.15
- Transmission Control Protocol, Src Port: 80, Dst Port: 35680, Seq: 1, Ack: 371, Len: 1128
- Hypertext Transfer Protocol
- Line-based text data: text/html (22 lines)

**Raw Data:**

```
0000 08 00 27 ab 08 1c 52 54 00 12 35 00 08 00 45 00  ...RT...E
0010 04 00 0f 06 00 00 ff 06 60 22 40 5b f2 d5 0a 00  .....1"Q[....
0020 02 0f 00 50 8b 60 00 01 05 ec 29 30 17 8c 50 18  ...P...j0-P
0030 7e 0e 08 02 00 00 48 54 54 50 2f 31 2e 31 20 32  ~....HTP/1.1 2
0040 30 30 20 4f 4b 0d 0a 44 61 74 65 3a 20 4d 6f 6e  00 OK - Date: Mon
0050 2c 20 32 38 20 44 65 63 20 32 30 32 30 20 31 33  , 28 Dec 2020 13
0060 3a 30 33 3a 31 33 20 47 4d 54 0d 0a 53 65 72 76  :03:13 GMT - Serv
0070 65 72 3a 20 41 70 61 63 68 65 0d 0a 68 20 50 6f  er: Apache/2.4.18
0080 77 65 72 65 64 20 42 79 3a 20 50 48 50 2f 35 2e  vered-by: PHP/5.
0090 36 2e 3a 30 0d 0a 45 78 70 69 72 65 73 3a 20 54  6.40 - Expires: T
00a0 68 75 2c 20 31 39 20 4e 6f 76 20 31 39 38 31 20  hu, 19 Nov 2018
00b0 30 38 3a 35 32 3a 30 30 20 47 4d 54 0d 0a 43 61  08:52:00 GMT - Ca
```

**Summary:**

- Frame (1182 bytes)
- Uncompressed entity body (1679 bytes)
- Hypertext Transfer Protocol: Protocol
- Packets: 104 - Displayed: 6 (5.8%) - Dropped: 0 (0.0%)
- Profile: Default

## 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, registration date, expiry

Date, and sometimes contact information of the owner.

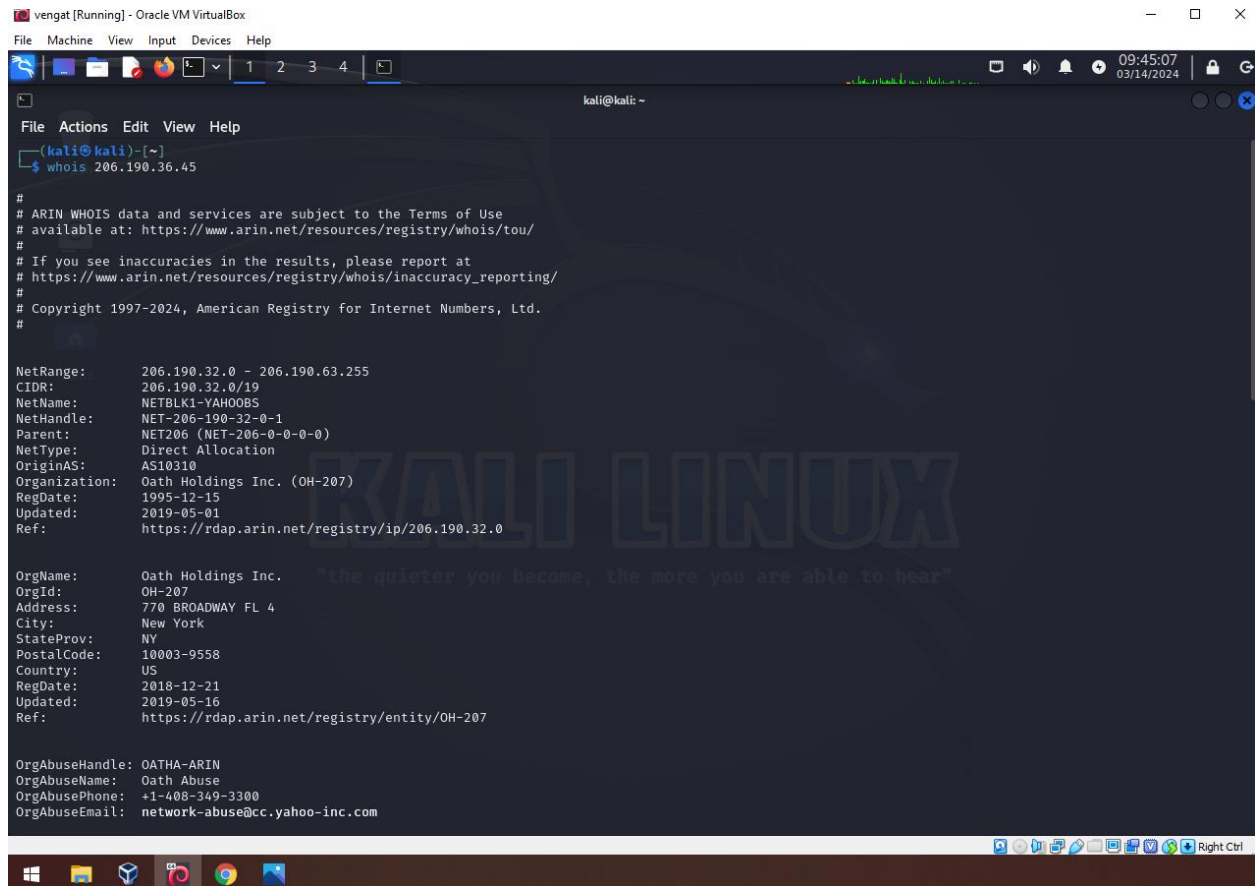
#### **PROGRAM:**

```
sudo apt update
```

```
sudo apt upgrade
```

```
whois 206.190.36.45
```

## FINAL REPORT:



```
vengat [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
kali@kali: ~
File Actions Edit View Help
(kali@kali)~$ whois 206.190.36.45

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2024, American Registry for Internet Numbers, Ltd.
#

NetRange:      206.190.32.0 - 206.190.63.255
CIDR:          206.190.32.0/19
NetName:       NETBLK1-YAHOOS
NetHandle:     NET-206-190-32-0-1
Parent:        NET206 (NET-206-0-0-0-0)
NetType:       Direct Allocation
OriginAS:      AS10310
Organization:  Oath Holdings Inc. (OH-207)
RegDate:       1995-12-15
Updated:       2019-05-01
Ref:           https://rdap.arin.net/registry/ip/206.190.32.0

OrgName:       Oath Holdings Inc.
OrgId:          OH-207
Address:        770 BROADWAY FL 4
City:           New York
StateProv:      NY
PostalCode:     10003-9558
Country:        US
RegDate:        2018-12-21
Updated:        2019-05-16
Ref:           https://rdap.arin.net/registry/entity/OH-207

OrgAbuseHandle: OATHA-ARIN
OrgAbuseName:   Oath Abuse
OrgAbusePhone:   +1-408-349-3300
OrgAbuseEmail:   network-abuse@cc.yahoo-inc.com
```

## 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)

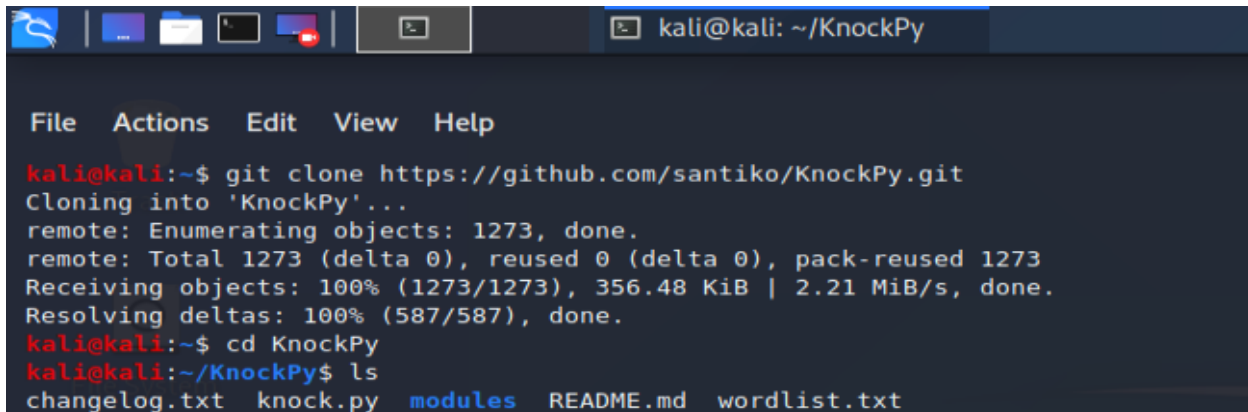
cd knockpy

knockpy google.com

knockpy -d google.com

knockpy -d facebook.com -recon -bruteforce.

## COMMAND OUTPUT:

A terminal window screenshot from a Kali Linux system. The window title is 'kali@kali: ~/KnockPy'. The terminal shows the following commands and output:

```
kali@kali:~$ git clone https://github.com/santiko/KnockPy.git
Cloning into 'KnockPy'...
remote: Enumerating objects: 1273, done.
remote: Total 1273 (delta 0), reused 0 (delta 0), pack-reused 1273
Receiving objects: 100% (1273/1273), 356.48 KiB | 2.21 MiB/s, done.
Resolving deltas: 100% (587/587), done.
kali@kali:~$ cd KnockPy
kali@kali:~/KnockPy$ ls
changelog.txt  knock.py  modules  README.md  wordlist.txt
```

## 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     el792.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.