

Assignment #4

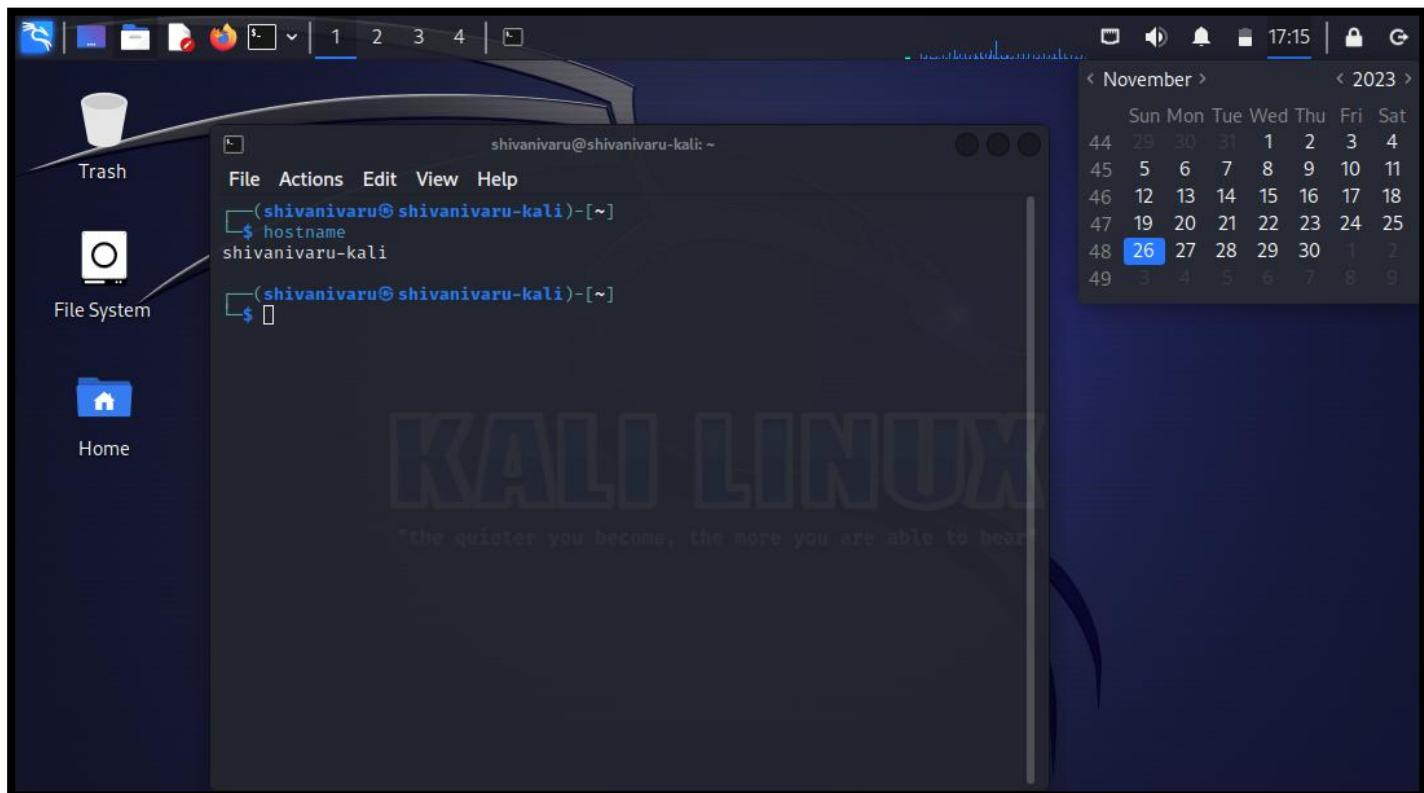
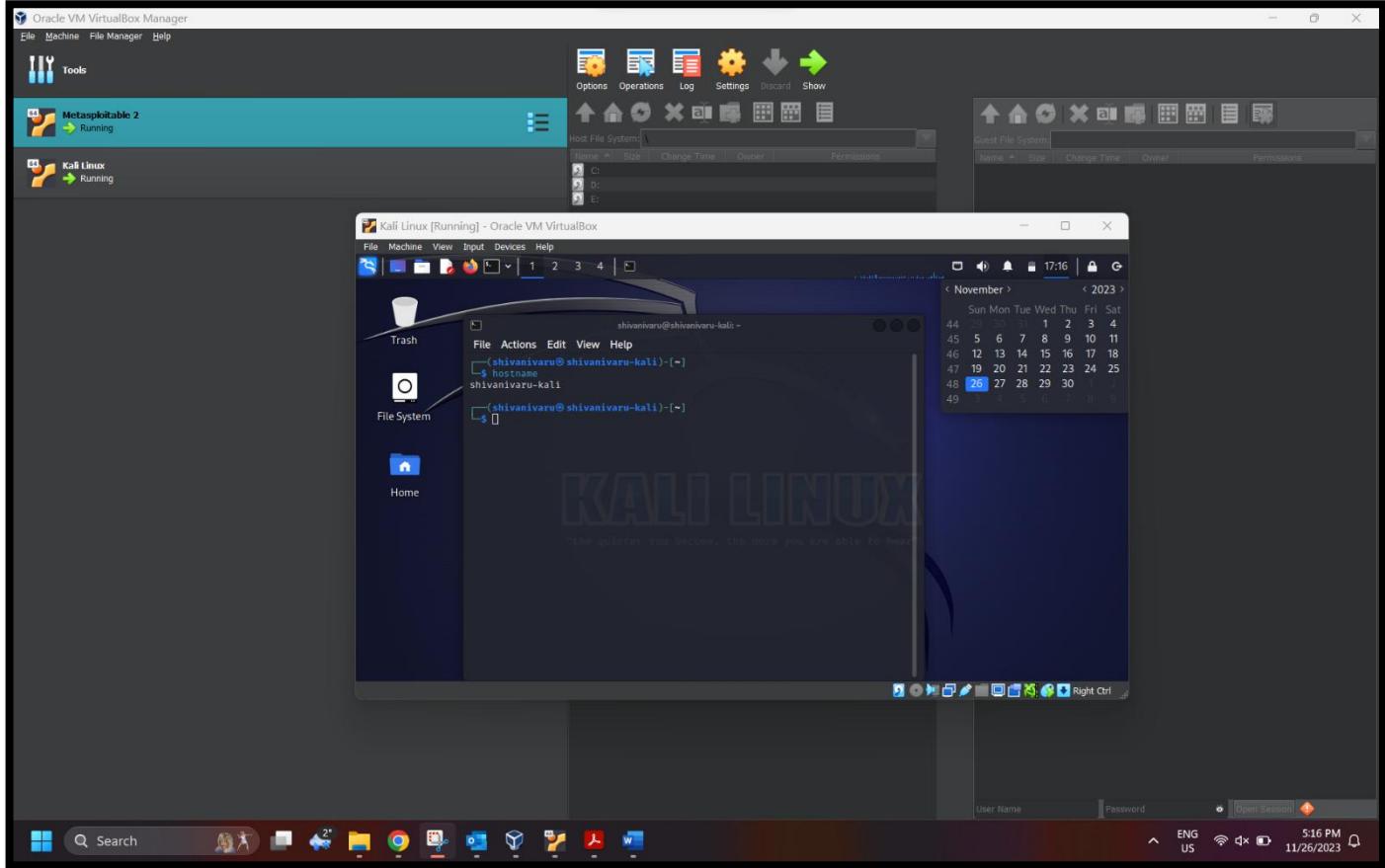
Name: Shivani Shaileshkumar Varu

Student ID: 8941914

Date: 5-12-2023

Section Number: Section – 4

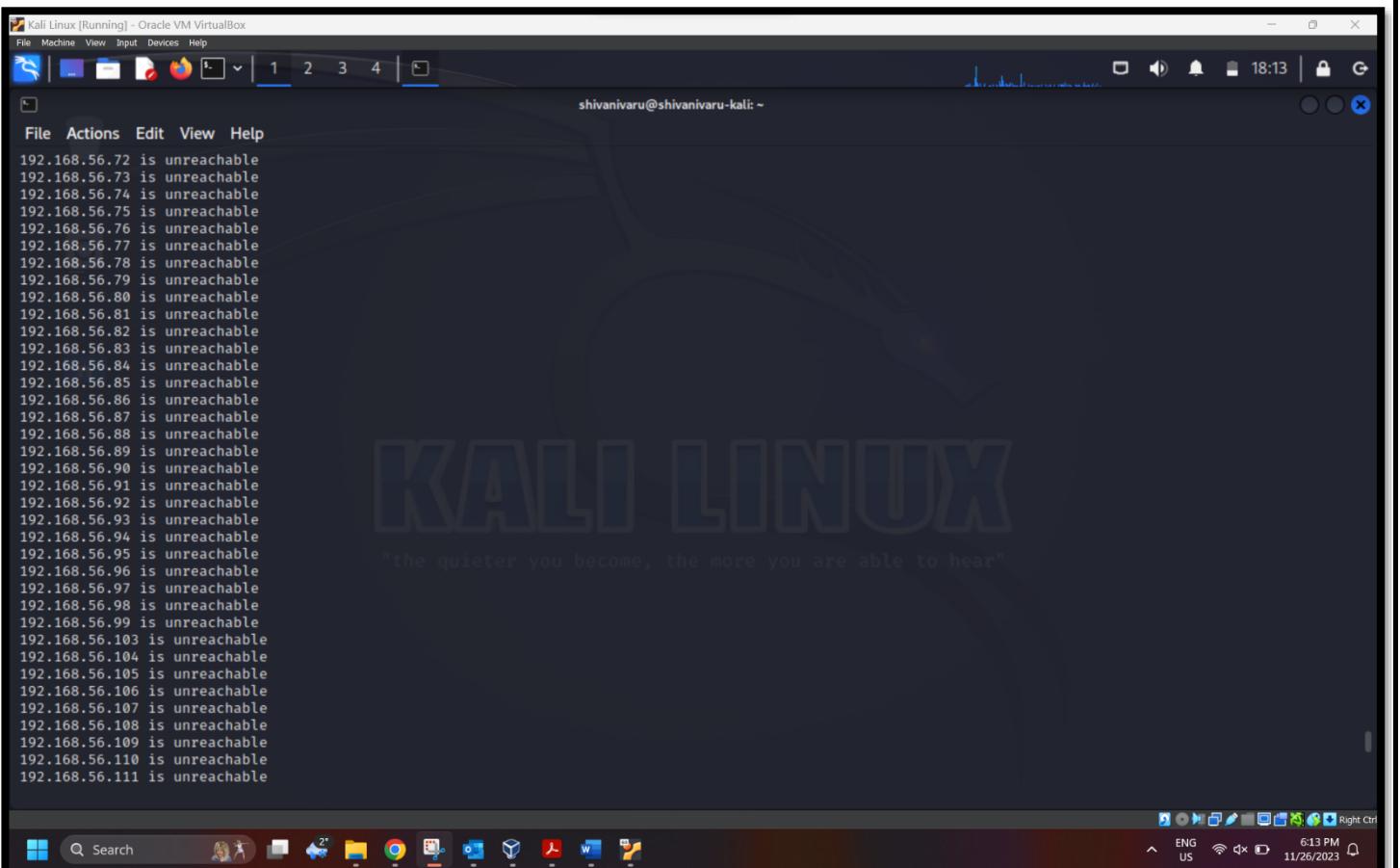
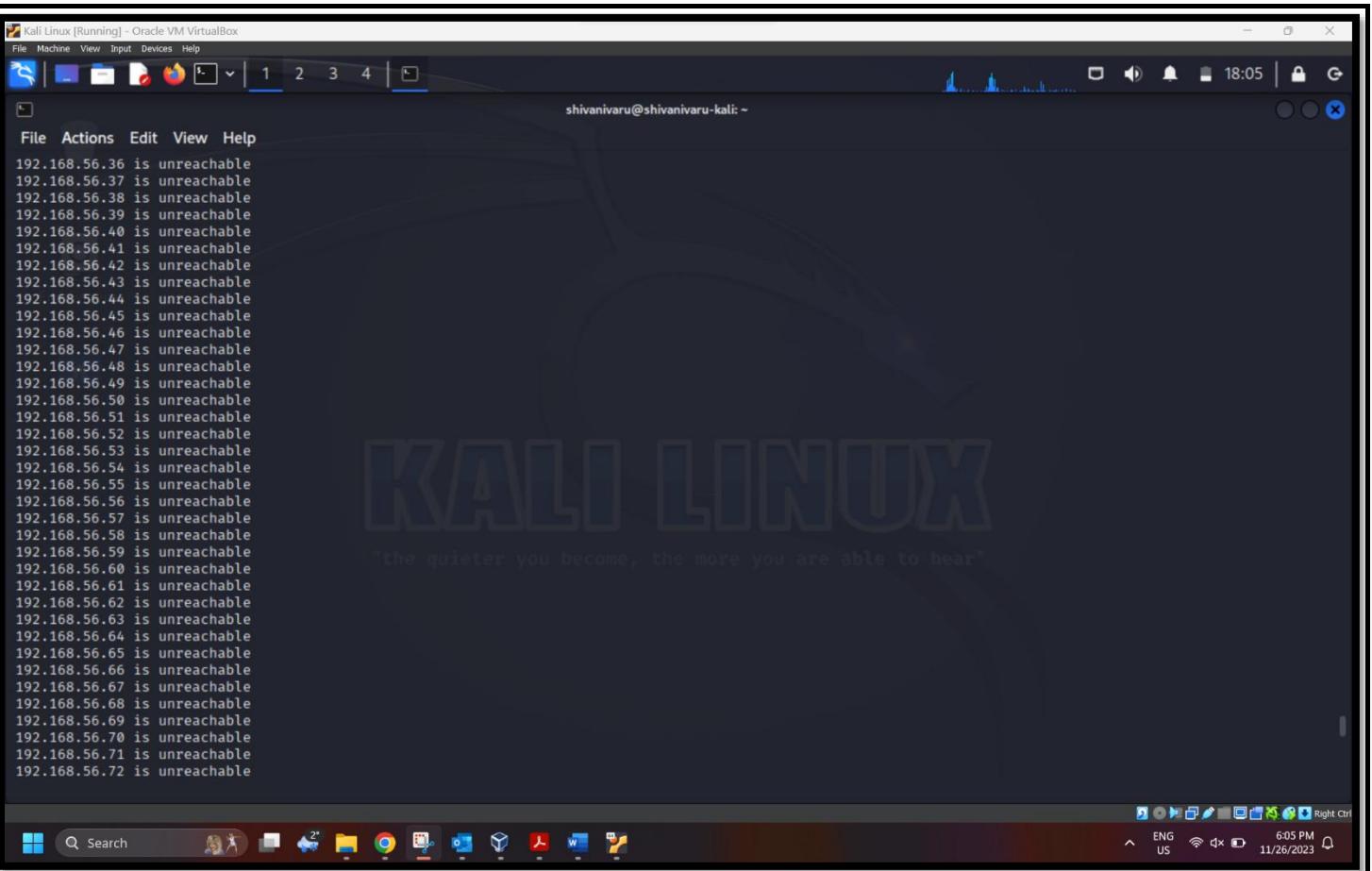
Screen Shot of Kali Setup With Time and Date.



Output From fping:

I have three IP addresses alive in the above output and referred to two options from the fping tool, -g to generate and -s to show the stats of all targets.

A screenshot of a Kali Linux terminal window titled "Kali Linux [Running] - Oracle VM VirtualBox". The terminal window has a dark background with a large watermark in the center reading "KALI LINUX" in blue and white, with the quote "the quieter you become, the more you are able to hear" below it. The terminal prompt is "shivanivar@shivanivar-kali: ~". The menu bar includes "File", "Machine", "View", "Input", "Devices", and "Help". The toolbar contains icons for file operations like Open, Save, Print, and a search bar. The bottom taskbar shows various application icons including a browser, file manager, terminal, and system monitor. The system tray at the bottom right shows the date and time as "11/26/2023 6:04 PM", battery status, and network connectivity. The terminal itself displays a series of ICMP host unreachable messages from port 1 to 4, indicating that the host at 192.168.56.102 is unreachable for ICMP traffic.



```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
S F D 1 2 3 4 | 
shivanivar@shivanivar-kali: ~
File Actions Edit View Help
192.168.56.111 is unreachable
192.168.56.112 is unreachable
192.168.56.113 is unreachable
192.168.56.114 is unreachable
192.168.56.115 is unreachable
192.168.56.116 is unreachable
192.168.56.117 is unreachable
192.168.56.118 is unreachable
192.168.56.119 is unreachable
192.168.56.120 is unreachable
192.168.56.121 is unreachable
192.168.56.122 is unreachable
192.168.56.123 is unreachable
192.168.56.124 is unreachable
192.168.56.125 is unreachable
192.168.56.126 is unreachable
192.168.56.127 is unreachable
192.168.56.128 is unreachable
192.168.56.129 is unreachable
192.168.56.130 is unreachable
192.168.56.131 is unreachable
192.168.56.132 is unreachable
192.168.56.133 is unreachable
192.168.56.134 is unreachable
192.168.56.135 is unreachable
192.168.56.136 is unreachable
192.168.56.137 is unreachable
192.168.56.138 is unreachable
192.168.56.139 is unreachable
192.168.56.140 is unreachable
192.168.56.141 is unreachable
192.168.56.142 is unreachable
192.168.56.143 is unreachable
192.168.56.144 is unreachable
192.168.56.145 is unreachable
192.168.56.146 is unreachable
192.168.56.147 is unreachable
"the quieter you become, the more you are able to hear"
File Search 
ENG US 6:13 PM 11/26/2023 Right Ctrl
```

```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
S F D 1 2 3 4 | 
shivanivar@shivanivar-kali: ~
File Actions Edit View Help
192.168.56.147 is unreachable
192.168.56.148 is unreachable
192.168.56.149 is unreachable
192.168.56.150 is unreachable
192.168.56.151 is unreachable
192.168.56.152 is unreachable
192.168.56.153 is unreachable
192.168.56.154 is unreachable
192.168.56.155 is unreachable
192.168.56.156 is unreachable
192.168.56.157 is unreachable
192.168.56.158 is unreachable
192.168.56.159 is unreachable
192.168.56.160 is unreachable
192.168.56.161 is unreachable
192.168.56.162 is unreachable
192.168.56.163 is unreachable
192.168.56.164 is unreachable
192.168.56.165 is unreachable
192.168.56.166 is unreachable
192.168.56.167 is unreachable
192.168.56.168 is unreachable
192.168.56.169 is unreachable
192.168.56.170 is unreachable
192.168.56.171 is unreachable
192.168.56.172 is unreachable
192.168.56.173 is unreachable
192.168.56.174 is unreachable
192.168.56.175 is unreachable
192.168.56.176 is unreachable
192.168.56.177 is unreachable
192.168.56.178 is unreachable
192.168.56.179 is unreachable
192.168.56.180 is unreachable
192.168.56.181 is unreachable
192.168.56.182 is unreachable
192.168.56.183 is unreachable
"the quieter you become, the more you are able to hear"
File Search 
ENG US 6:14 PM 11/26/2023 Right Ctrl
```

Kali Linux [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

shivanivar@shivanivar-kali: ~

File Actions Edit View Help

```
192.168.56.178 is unreachable
192.168.56.179 is unreachable
192.168.56.180 is unreachable
192.168.56.181 is unreachable
192.168.56.182 is unreachable
192.168.56.183 is unreachable
192.168.56.184 is unreachable
192.168.56.185 is unreachable
192.168.56.186 is unreachable
192.168.56.187 is unreachable
192.168.56.188 is unreachable
192.168.56.189 is unreachable
192.168.56.190 is unreachable
192.168.56.191 is unreachable
192.168.56.192 is unreachable
192.168.56.193 is unreachable
192.168.56.194 is unreachable
192.168.56.195 is unreachable
192.168.56.196 is unreachable
192.168.56.197 is unreachable
192.168.56.198 is unreachable
192.168.56.199 is unreachable
192.168.56.200 is unreachable
192.168.56.201 is unreachable
192.168.56.202 is unreachable
192.168.56.203 is unreachable
192.168.56.204 is unreachable
192.168.56.205 is unreachable
192.168.56.206 is unreachable
192.168.56.207 is unreachable
192.168.56.208 is unreachable
192.168.56.209 is unreachable
192.168.56.210 is unreachable
192.168.56.211 is unreachable
192.168.56.212 is unreachable
192.168.56.213 is unreachable
192.168.56.214 is unreachable
192.168.56.215 is unreachable
192.168.56.216 is unreachable
192.168.56.217 is unreachable
192.168.56.218 is unreachable
192.168.56.219 is unreachable
```

File Actions Edit View Help

```
$ nbtscan.sh
"Human-readable service names" (-h) option cannot be used without
l option.
Usage:
nbtscan [-v] [-d] [-e] [-U] [-t timeout] [-b bandwidth] [-r] [-n]
or] [-m retransmits] [-f filename] [-c scan_range>
-v verbose output. Print all names received
from each host.
-d dump packets. Print whole packet contents.
-e Format output in /etc/hosts format.
-t timeout. Cannot be used with -v, -s or -h options.
-w wait timeout milliseconds for response.
Default 1000.
-b bandwidth. Output throttling. Slow down output
so that it uses no more than bandwidth bps.
Useful on slow links, so that outgoing quer-
ies don't get dropped.
-l local port 137 for scans. Win95 boxes
respond to this only.
You need to be root to use this option on
Linux.
-q suppress banners and error messages.
-s separator. Script-friendly output. Don't print
column and record headers, separate fields
with separator.
-f filename. Save the results to a file.
-c scan_range. Scan a range of hosts.
```

In the above screenshots, the list of IP addresses unreachable is displayed.

Kali Linux [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

shivanivar@shivanivar-kali: ~

File Actions Edit View Help

```
192.168.56.219 is unreachable
192.168.56.220 is unreachable
192.168.56.221 is unreachable
192.168.56.222 is unreachable
192.168.56.223 is unreachable
192.168.56.224 is unreachable
192.168.56.225 is unreachable
192.168.56.226 is unreachable
192.168.56.227 is unreachable
192.168.56.228 is unreachable
192.168.56.229 is unreachable
192.168.56.230 is unreachable
192.168.56.231 is unreachable
192.168.56.232 is unreachable
192.168.56.233 is unreachable
192.168.56.234 is unreachable
192.168.56.235 is unreachable
192.168.56.236 is unreachable
192.168.56.237 is unreachable
192.168.56.238 is unreachable
192.168.56.239 is unreachable
192.168.56.240 is unreachable
192.168.56.241 is unreachable
192.168.56.242 is unreachable
192.168.56.243 is unreachable
192.168.56.244 is unreachable
192.168.56.245 is unreachable
192.168.56.246 is unreachable
192.168.56.247 is unreachable
192.168.56.248 is unreachable
192.168.56.249 is unreachable
192.168.56.250 is unreachable
192.168.56.251 is unreachable
192.168.56.252 is unreachable
192.168.56.253 is unreachable
192.168.56.254 is unreachable
```

Kali Linux [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

shivanivar@shivanivar-kali: ~

```
File Actions Edit View Help
192.168.56.234 is unreachable
192.168.56.235 is unreachable
192.168.56.236 is unreachable
192.168.56.237 is unreachable
192.168.56.238 is unreachable
192.168.56.239 is unreachable
192.168.56.240 is unreachable
192.168.56.241 is unreachable
192.168.56.242 is unreachable
192.168.56.243 is unreachable
192.168.56.244 is unreachable
192.168.56.245 is unreachable
192.168.56.246 is unreachable
192.168.56.247 is unreachable
192.168.56.248 is unreachable
192.168.56.249 is unreachable
192.168.56.250 is unreachable
192.168.56.251 is unreachable
192.168.56.252 is unreachable
192.168.56.253 is unreachable
192.168.56.254 is unreachable

254 targets
  3 alive
  251 unreachable
  0 unknown addresses

  1004 timeouts (waiting for response)
  1007 ICMP Echos sent
    3 ICMP Echo Replies received
  1000 other ICMP received

  0.026 ms (min round trip time)
  0.582 ms (avg round trip time)
  0.939 ms (max round trip time)
  9.958 sec (elapsed real time)

  KALI LINUX
  "the quieter you become, the more you are able to hear"
```

File Machine View Input Devices Help

shivanivar@shivanivar-kali: ~

```
File Actions Edit View Help
192.168.56.234 is unreachable
192.168.56.235 is unreachable
192.168.56.236 is unreachable
192.168.56.237 is unreachable
192.168.56.238 is unreachable
192.168.56.239 is unreachable
192.168.56.240 is unreachable
192.168.56.241 is unreachable
192.168.56.242 is unreachable
192.168.56.243 is unreachable
192.168.56.244 is unreachable
192.168.56.245 is unreachable
192.168.56.246 is unreachable
192.168.56.247 is unreachable
192.168.56.248 is unreachable
192.168.56.249 is unreachable
192.168.56.250 is unreachable
192.168.56.251 is unreachable
192.168.56.252 is unreachable
192.168.56.253 is unreachable
192.168.56.254 is unreachable

254 targets
  3 alive
  251 unreachable
  0 unknown addresses

  1004 timeouts (waiting for response)
  1007 ICMP Echos sent
    3 ICMP Echo Replies received
  1000 other ICMP received

  0.026 ms (min round trip time)
  0.582 ms (avg round trip time)
  0.939 ms (max round trip time)
  9.958 sec (elapsed real time)

  KALI LINUX
  "the quieter you become, the more you are able to hear"
```

The above screenshot shows the final stats with **254 targets** out of which **3** are alive and **251 targets** are **unreachable**.

Kali Linux [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

shivanivaru@shivanivaru-kali: ~

File Actions Edit View Help

```
(shivanivaru@shivanivaru-kali)-[~]
$ nbtscan 192.168.56.100
Doing NBT name scan for addresses from 192.168.56.100
```

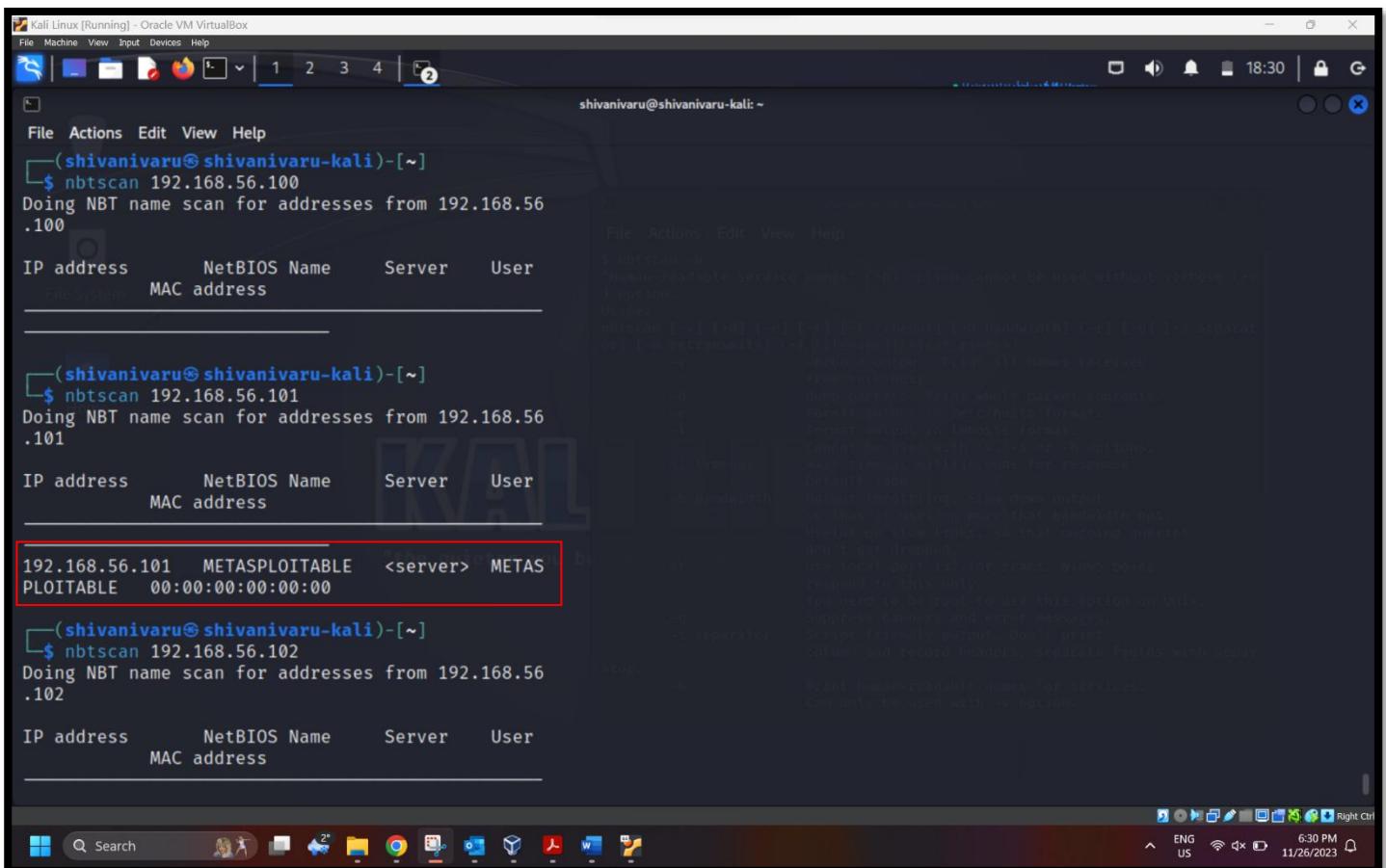
IP address	NetBIOS Name	Server	User	MAC address	Actions	Edit	View	Help
------------	--------------	--------	------	-------------	---------	------	------	------

```
(shivanivaru@shivanivaru-kali)-[~]
$ nmap -sn 192.168.56.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-26 18:36 EST
Nmap scan report for 192.168.56.101
Host is up (0.0030s latency).
Nmap scan report for 192.168.56.102
Host is up (0.00011s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 19.72 seconds
```

```
(shivanivaru@shivanivaru-kali)-[~]
$ home
```

To find the exact IP address, I have referred to using the **-sn** command from the Nmap tool to find only the available host. This option helps in the reconnaissance of the target. This can be used to find available machines

Output from NBTSCAN :



```
shivanivaru@shivanivaru-kali:~$ nbtscan 192.168.56.100
Doing NBT name scan for addresses from 192.168.56
.100
IP address      NetBIOS Name      Server      User
MAC address

(shivanivaru@shivanivaru-kali)-[~]
$ nbtscan 192.168.56.101
Doing NBT name scan for addresses from 192.168.56
.101
IP address      NetBIOS Name      Server      User
MAC address

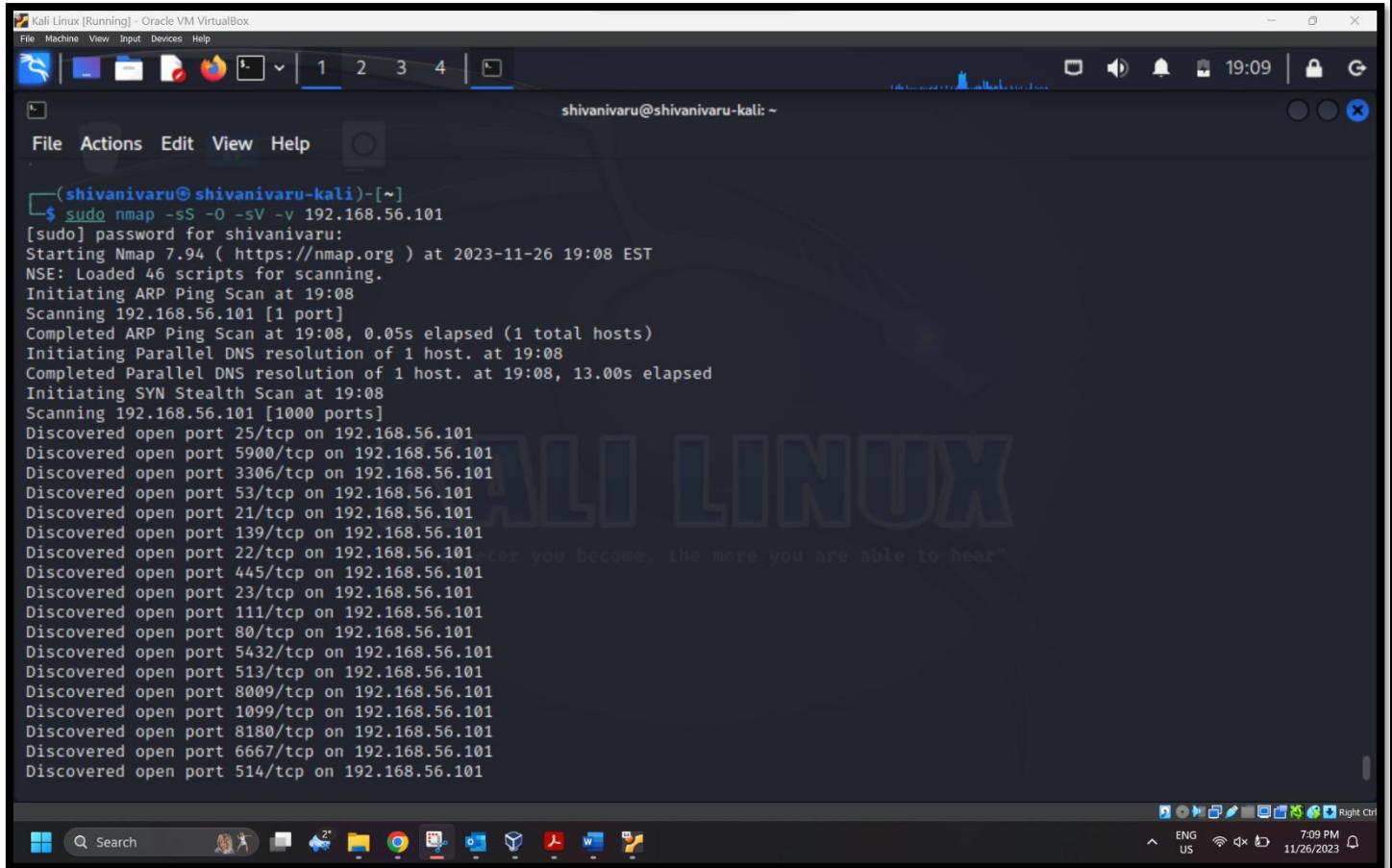
192.168.56.101    METASPLOITABLE    <server>    METAS
PLOITABLE    00:00:00:00:00:00

(shivanivaru@shivanivaru-kali)-[~]
$ nbtscan 192.168.56.102
Doing NBT name scan for addresses from 192.168.56
.102
IP address      NetBIOS Name      Server      User
MAC address
```

The screenshot shows a terminal window on a Kali Linux desktop. The user has run the command \$ nbtscan 192.168.56.100, followed by \$ nbtscan 192.168.56.101, and finally \$ nbtscan 192.168.56.102. The output lists NetBIOS names and server details for each address. The row for address 192.168.56.101 is highlighted with a red box.

The above output shows the execution of the nbtscan tool on the list of 3 IP addresses that I have found. **The IP address for Metaspitable is 192.168.56.101 which I have highlighted with red box.**

Nmap for Detailed Scanning:



The screenshot shows a terminal window titled "Kali Linux [Running] - Oracle VM VirtualBox". The command entered is `sudo nmap -sS -O -v 192.168.56.101`. The output details the scanning process, starting with an ARP Ping Scan, followed by DNS resolution and SYN Stealth Scan, and finally a detailed port scan (-O) which identifies numerous open ports on the target host 192.168.56.101.

```
shivanivaru@shivanivaru-kali: ~
$ sudo nmap -sS -O -v 192.168.56.101
[sudo] password for shivanivaru:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-26 19:08 EST
NSE: Loaded 46 scripts for scanning.
Initiating ARP Ping Scan at 19:08
Scanning 192.168.56.101 [1 port]
Completed ARP Ping Scan at 19:08, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:08
Completed Parallel DNS resolution of 1 host. at 19:08, 13.00s elapsed
Initiating SYN Stealth Scan at 19:08
Scanning 192.168.56.101 [1000 ports]
Discovered open port 25/tcp on 192.168.56.101
Discovered open port 5900/tcp on 192.168.56.101
Discovered open port 3306/tcp on 192.168.56.101
Discovered open port 53/tcp on 192.168.56.101
Discovered open port 21/tcp on 192.168.56.101
Discovered open port 139/tcp on 192.168.56.101
Discovered open port 22/tcp on 192.168.56.101
Discovered open port 445/tcp on 192.168.56.101
Discovered open port 23/tcp on 192.168.56.101
Discovered open port 111/tcp on 192.168.56.101
Discovered open port 80/tcp on 192.168.56.101
Discovered open port 5432/tcp on 192.168.56.101
Discovered open port 513/tcp on 192.168.56.101
Discovered open port 8009/tcp on 192.168.56.101
Discovered open port 1099/tcp on 192.168.56.101
Discovered open port 8180/tcp on 192.168.56.101
Discovered open port 6667/tcp on 192.168.56.101
Discovered open port 514/tcp on 192.168.56.101
```

I have highlighted the Nmap command with all the correct options below:

1. -sS is used to check if the host is up, and also Nmap attempts the TCP SYN connection.
2. -O helps in OS Scanning.
3. -sV helps in version detection
4. -v helps with more information about scanning progress, and it also provides an estimation of completion time.

Kali Linux [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

shivanivar@shivanivar-kali: ~

File Actions Edit View Help

Not shown: 977 closed tcp ports (reset)

PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	vsftpd 2.3.4
22/tcp	open	ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp	open	telnet	Linux telnetd
25/tcp	open	smtp	Postfix smtpd
53/tcp	open	domain	ISC BIND 9.4.2
80/tcp	open	http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp	open	rpcbind	2 (RPC #100000)
139/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp	open	exec	netkit-rsh rexecd
513/tcp	open	login	
514/tcp	open	shell	Netkit rshd
1099/tcp	open	java-rmi	GNU Classpath grmiregistry
1524/tcp	open	bindshell	Metasploitable root shell
2049/tcp	open	nfs	2-4 (RPC #100003)
2121/tcp	open	ftp	ProFTPD 1.3.1
3306/tcp	open	mysql	MySQL 5.0.51a-3ubuntu5
5432/tcp	open	postgresql	PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp	open	vnc	VNC (protocol 3.3)
6000/tcp	open	X11	(access denied)
6667/tcp	open	irc	UnrealIRCd
8009/tcp	open	ajp13	Apache Jserv (Protocol v1.3)
8180/tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1

MAC Address: 08:00:27:52:5A:99 (Oracle VirtualBox virtual NIC)

Device type: general purpose

Running: Linux 2.6.X

OS CPE: cpe:/o:linux:linux_kernel:2.6

OS details: Linux 2.6.9 - 2.6.33

Uptime guess: 0.064 days (since Sun Nov 26 17:36:33 2023)

In the above screenshot, I have highlighted all the open ports and services.

Kali Linux [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

shivanivar@shivanivar-kali: ~

File Actions Edit View Help

```
513/tcp open  login
514/tcp open  shell      Netkit rshd
1099/tcp open  java-rmi   GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs        2-4 (RPC #100003)
2121/tcp open  ftp        ProFTPD 1.3.1
3306/tcp open  mysql     MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc        VNC (protocol 3.3)
6000/tcp open  X11        (access denied)
6667/tcp open  irc        UnrealIRCd
8009/tcp open  ajp13     Apache Jserv (Protocol v1.3)
8180/tcp open  http       Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:52:5A:99 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Uptime guess: 0.064 days (since Sun Nov 26 17:36:33 2023)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=206 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.66 seconds
Raw packets sent: 1020 (45.626KB) | Rcvd: 1016 (41.430KB)
```

(shivanivar@shivanivar-kali)-[~]

\$

File Machine View Input Devices Help

shivanivar@shivanivar-kali: ~

File Actions Edit View Help

```
513/tcp open  login
514/tcp open  shell      Netkit rshd
1099/tcp open  java-rmi   GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs        2-4 (RPC #100003)
2121/tcp open  ftp        ProFTPD 1.3.1
3306/tcp open  mysql     MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc        VNC (protocol 3.3)
6000/tcp open  X11        (access denied)
6667/tcp open  irc        UnrealIRCd
8009/tcp open  ajp13     Apache Jserv (Protocol v1.3)
8180/tcp open  http       Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:52:5A:99 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Uptime guess: 0.064 days (since Sun Nov 26 17:36:33 2023)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=206 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.66 seconds
Raw packets sent: 1020 (45.626KB) | Rcvd: 1016 (41.430KB)
```

(shivanivar@shivanivar-kali)-[~]

\$

```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
shivanivaru@shivanivaru-kali: ~

File Actions Edit View Help
Discovered open port 514/tcp on 192.168.56.101
Discovered open port 512/tcp on 192.168.56.101
Discovered open port 6000/tcp on 192.168.56.101
Discovered open port 1524/tcp on 192.168.56.101
Discovered open port 2049/tcp on 192.168.56.101
Discovered open port 2121/tcp on 192.168.56.101
Completed SYN Stealth Scan at 19:08, 0.50s elapsed (1000 total ports)
Initiating Service scan at 19:08
Scanning 23 services on 192.168.56.101
Completed Service scan at 19:08, 11.24s elapsed (23 services on 1 host)
Initiating OS detection (try #1) against 192.168.56.101
NSE: Script scanning 192.168.56.101.
Initiating NSE at 19:08
Completed NSE at 19:08, 0.21s elapsed
Initiating NSE at 19:08
Completed NSE at 19:08, 0.10s elapsed
Nmap scan report for 192.168.56.101
Host is up (0.0036s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain      ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login       

Search 7:21 PM 11/26/2023
```

In the above output, I have highlighted the service name Apache httpd 2.2.8 that I will conduct.

Answer for research on Apache HTTPD server 2.2.8:

The Apache HTTP Server, a critical component of web hosting, has gone through various versions. Version 1.3, released on June 6, 1998, remained in use until its final release, 1.3.42, on February 3, 2010. Versions 2.0 (April 6, 2002), 2.2 (December 1, 2005), and 2.4 (February 21, 2012) followed. The most recent, 2.4.57, released on April 6, 2023, reflects continual improvements. The first initial release began on April 27, 1995, with version 0.6.2, which marked the beginning of Apache's impact on web hosting.

However, there are numerous known vulnerabilities in Apache HTTP Server version 2.2.8.

Optionsbleed is one of the vulnerabilities that lets remote attackers access confidential information from process memory. This might happen if there are certain misconfigurations in httpd.conf or if the Limit directive is set in a user.htaccess file. To access the secret data, the attacker might submit an unauthenticated OPTIONS HTTP request.

As a penetration tester, the information about the Optionsbleed vulnerability would be crucial in assessing the security of a system. Here's how I would proceed: Here's how I would proceed:

Step 1: Defining Scope and Goals

Defining the goals and scope of the test is the first stage in every penetration test. This involves identifying the systems to be tested, the processes to be followed, and agreeing on the format for reporting the results.

Step 2: Reconnaissance

Next, I would gather as much information as possible about the target system. This could include identifying the version of Apache being used, the configuration of the .htaccess file, and any other relevant details.

Step 3: Scanning and Exploitation

After getting sufficient details, I'd use Kali Linux's penetration testing tools to check the target system for the Optionsbleed vulnerability. This might include sending an OPTIONS HTTP request to the server without authentication and examining the response for indications of memory leakage.

Here is an example of a command that could be used in Kali Linux to send an OPTIONS request:

```
curl -X OPTIONS http://target-server.com
```

If the server is vulnerable to Optionsbleed, the response could contain confidential information from the server's memory.

Step 4: Reporting

After the test, I would compile a report detailing the findings. This would include information about the vulnerability, the potential impact, and recommended mitigation strategies.

❖ **To safeguard systems from the Optionsbleed vulnerability,**

I can suggest some points that clients should do: -

- Apply the patch for Optionsbleed available from the Apache source code servers. This is a critical step to address the vulnerability and prevent potential data leakage.
- Review the httpd.conf and .htaccess files to ensure that they are properly configured. Avoid misconfigurations that could trigger the Optionsbleed vulnerability.
- Conduct regular security audits and penetration tests to identify and address vulnerabilities, including Optionsbleed. This will help in proactively identifying and mitigating any potential risks.
- Stay informed about the latest security vulnerabilities and patches. Subscribe to security advisories and news sources to stay updated on emerging threats and mitigation strategies.

End users can, however, stay informed about the security of the systems they use and report any unusual or suspicious activity to their IT department or system administrators.

❖ **References**

1. *Apache HTTP server*. Wikidata. (n.d.). <https://www.wikidata.org/wiki/Q11354>
2. Chauhan, B. (2023, October 26). *3 most critical Apache vulnerabilities found*. Astra Security Blog. <https://www.getastral.com/blog/911/top-3-most-critical-apache-vulnerabilities-found/>
3. Apache < 2.2.8 multiple vulnerabilities. Tenable. (n.d.). <https://www.tenable.com/plugins/lce/800581>
4. *10 apache web server security and hardening tips*. Online Tutorials, Courses, and eBooks Library. (n.d.). <https://www.tutorialspoint.com/10-apache-web-server-security-and-hardening-tips>
5. *Apache HTTP server version 2.2.8 : Security vulnerabilities, CVES*. Apache Http Server version 2.2.8 : Security vulnerabilities, CVEs. (n.d.). https://www.cvedetails.com/vulnerability-list/vendor_id-45/product_id-66/version_id-416233/Apache-Http-Server_2.2.8.html?page=2&order=1&trc=67&sha=614e10502c7f37a061f7932cc90f7534419090d
6. Ducklin. (2017, September 19). *Apache “Optionsbleed” vulnerability – what you need to know*. Sophos News. <https://news.sophos.com/en-us/2017/09/19/apache-optionsbleed-vulnerability-what-you-need-to-know/>
7. Maury, J. (2023, October 10). *Kali Linux penetration testing tutorial: How to use Kali linux*. eSecurity Planet. <https://www.esecurityplanet.com/networks/kali-linux-tutorial/>
8. Thorat, B. P., Authors, Pavan Thorat Vulnerability Researcher William Gamazo Sanchez Sr. Threat Researcher, Researcher, P. T. V., Thorat, P., Researcher, V., Researcher, W. G. S. Sr. T., Sanchez, W. G., Researcher, Sr. T., Us, C., & Subscribe. (2017, September 22). *OptionsBleed – the apache HTTP server now bleeds*. Trend Micro. https://www.trendmicro.com/en_ph/research/17/i/optionsbleed-apache-http-server-now-bleeds.html
9. Sanders, C. (2017, September 20). *Chaim sanders*. OWASP ModSecurity Core Rule Set. <https://coreruleset.org/20170920/optionsbleed/>