Name: **Mareena Fernandes**
Roll No.: **8669**
Class: **TE IT**
Batch: **B**

EXPERIMENT NO: 8

1)

```
mareenalinux@mareenalinux:~Desktop$ sudo apt-get install arpwatch
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  libfprint-2-tod1
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  gawk ieee-data libsigsegv2
Suggested packages:
  gawk-doc
The following NEW packages will be installed:
  arpwatch gawk ieee-data libsigsegv2
0 upgraded, 4 newly installed, 0 to remove and 0 not upgraded.
Need to get 418 kB/2,065 kB of archives.
After this operation, 12.3 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://in.archive.ubuntu.com/ubuntu focal/main amd64 gawk amd64 1:5.0.1+dfsg-1 [418
kB]
Fetched 418 kB in 0s (1,357 kB/s)
Selecting previously unselected package libsigsegv2:amd64.
(Reading database ... 187038 files and directories currently installed.)
Preparing to unpack .../libsigsegv2_2.12-2_amd64.deb ...
Unpacking libsigsegv2:amd64 (2.12-2) ...
Setting up libsigsegv2:amd64 (2.12-2) ...
Selecting previously unselected package gawk.
(Reading database ... 187045 files and directories currently installed.)
Preparing to unpack .../gawk_1%3a5.0.1+dfsg-1_amd64.deb ...
Unpacking gawk (1:5.0.1+dfsg-1) ...
Selecting previously unselected package arpwatch.
Preparing to unpack .../arpwatch_2.1a15-7_amd64.deb ...
Unpacking arpwatch (2.1a15-7) ...
Selecting previously unselected package ieee-data.
Preparing to unpack .../ieee-data_20180805.1_all.deb ...
Unpacking ieee-data (20180805.1) ...
```

```
Setting up gawk (1:5.0.1+dfsg-1) ...
Setting up arpwatch (2.1a15-7) ...
Created symlink /etc/systemd/system/multi-user.target.wants/arpwatch.service →
/lib/systemd/system/arpwatch.service.
Setting up ieee-data (20180805.1) ...
Processing triggers for systemd (245.4-4ubuntu3.3) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for libc-bin (2.31-0ubuntu9.1) ...
```

2)

```
mareenalinux@mareenalinux:~Desktop$ sudo /etc/init.d/arpwatch start
Starting arpwatch (via systemctl): arpwatch.service.
```

3)

```
mareenalinux@mareenalinux:~Desktop$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::22a2:11af:4ecb:5311  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:13:b3:29  txqueuelen 1000  (Ethernet)
        RX packets 2350  bytes 2971453 (2.9 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 908  bytes 72862 (72.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 99  bytes 9179 (9.1 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 99  bytes 9179 (9.1 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

4)

```
mareenalinux@mareenalinux:~Desktop$ arpwatch -i enp0s3
mareenalinux@mareenalinux:~Desktop$ sudo arpwatch -i enp0s3
mareenalinux@mareenalinux:~Desktop$ sudo tail -f /var/log/messages
tail: cannot open '/var/log/messages' for reading: No such file or directory
tail: no files remaining
```

5)

```
mareenalinux@mareenalinux:~Desktop$ arp -a
_gateway (10.0.2.2) at 52:54:00:12:35:02 [ether] on enp0s3
```

6)

```
mareenalinux@mareenalinux:~Desktop$ sudo apt install ettercap-graphical
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  libfprint-2-tod1
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  ettercap-common geoip-database libgeoip1 libluajit-5.1-2 libluajit-5.1-common libnet1
Suggested packages:
  geoip-bin
The following NEW packages will be installed:
  ettercap-common ettercap-graphical geoip-database libgeoip1 libluajit-5.1-2 libluajit-5.1-
common libnet1
0 upgraded, 7 newly installed, 0 to remove and 0 not upgraded.
Need to get 4,325 kB of archives.
After this operation, 14.5 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 geoip-database all
20191224-2 [3,029 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 libgeoip1 amd64 1.6.12-
6build1 [70.5 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 libluajit-5.1-common all
2.1.0~beta3+dfsg-5.1build1 [44.3 kB]
Get:4 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 libluajit-5.1-2 amd64
2.1.0~beta3+dfsg-5.1build1 [228 kB]
Get:5 http://in.archive.ubuntu.com/ubuntu focal/main amd64 libnet1 amd64 1.1.6+dfsg-
3.1build1 [43.3 kB]
```

```
Get:6 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 ettercap-common amd64 1:0.8.3-7 [684 kB]
Get:7 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 ettercap-graphical amd64 1:0.8.3-7 [226 kB]
Fetched 4,325 kB in 8s (514 kB/s)
Selecting previously unselected package geoip-database.
(Reading database ... 187261 files and directories currently installed.)
Preparing to unpack .../0-geoip-database_20191224-2_all.deb ...
Unpacking geoip-database (20191224-2) ...
Selecting previously unselected package libgeoip1:amd64.
Preparing to unpack .../1-libgeoip1_1.6.12-6build1_amd64.deb ...
Unpacking libgeoip1:amd64 (1.6.12-6build1) ...
Selecting previously unselected package libluajit-5.1-common.
Preparing to unpack .../2-libluajit-5.1-common_2.1.0~beta3+dfsg-5.1build1_all.deb ...
Unpacking libluajit-5.1-common (2.1.0~beta3+dfsg-5.1build1) ...
Selecting previously unselected package libluajit-5.1-2:amd64.
Preparing to unpack .../3-libluajit-5.1-2_2.1.0~beta3+dfsg-5.1build1_amd64.deb ...
Unpacking libluajit-5.1-2:amd64 (2.1.0~beta3+dfsg-5.1build1) ...
Selecting previously unselected package libnet1:amd64.
Preparing to unpack .../4-libnet1_1.1.6+dfsg-3.1build1_amd64.deb ...
Unpacking libnet1:amd64 (1.1.6+dfsg-3.1build1) ...
Selecting previously unselected package ettercap-common.
Preparing to unpack .../5-ettercap-common_1%3a0.8.3-7_amd64.deb ...
Unpacking ettercap-common (1:0.8.3-7) ...
Selecting previously unselected package ettercap-graphical.
Preparing to unpack .../6-ettercap-graphical_1%3a0.8.3-7_amd64.deb ...
Unpacking ettercap-graphical (1:0.8.3-7) ...
Setting up libnet1:amd64 (1.1.6+dfsg-3.1build1) ...
Setting up libluajit-5.1-common (2.1.0~beta3+dfsg-5.1build1) ...
Setting up libgeoip1:amd64 (1.6.12-6build1) ...
Setting up geoip-database (20191224-2) ...
Setting up libluajit-5.1-2:amd64 (2.1.0~beta3+dfsg-5.1build1) ...
Setting up ettercap-common (1:0.8.3-7) ...
Setting up ettercap-graphical (1:0.8.3-7) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for desktop-file-utils (0.24-1ubuntu3) ...
Processing triggers for mime-support (3.64ubuntu1) ...
Processing triggers for gnome-menus (3.36.0-1ubuntu1) ...
Processing triggers for libc-bin (2.31-0ubuntu9.1) ...
```

7)

```
mareenalinux@mareenalinux:~Desktop$ sudo ettercap -G

ettercap 0.8.3 copyright 2001-2019 Ettercap Development Team

Failed to create secure directory (/root/.config/pulse): Permission denied
Failed to create secure directory (/root/.config/pulse): Permission denied
Failed to create secure directory (/root/.config/pulse): Permission denied
Failed to create secure directory (/root/.config/pulse): Permission denied
```

8)

```
mareenalinux@mareenalinux:~Desktop$ sudo apt install ettercap-0.8.3.1
Reading package lists... Done
Building dependency tree
Reading state information... Done
E: Unable to locate package ettercap-0.8.3.1
```

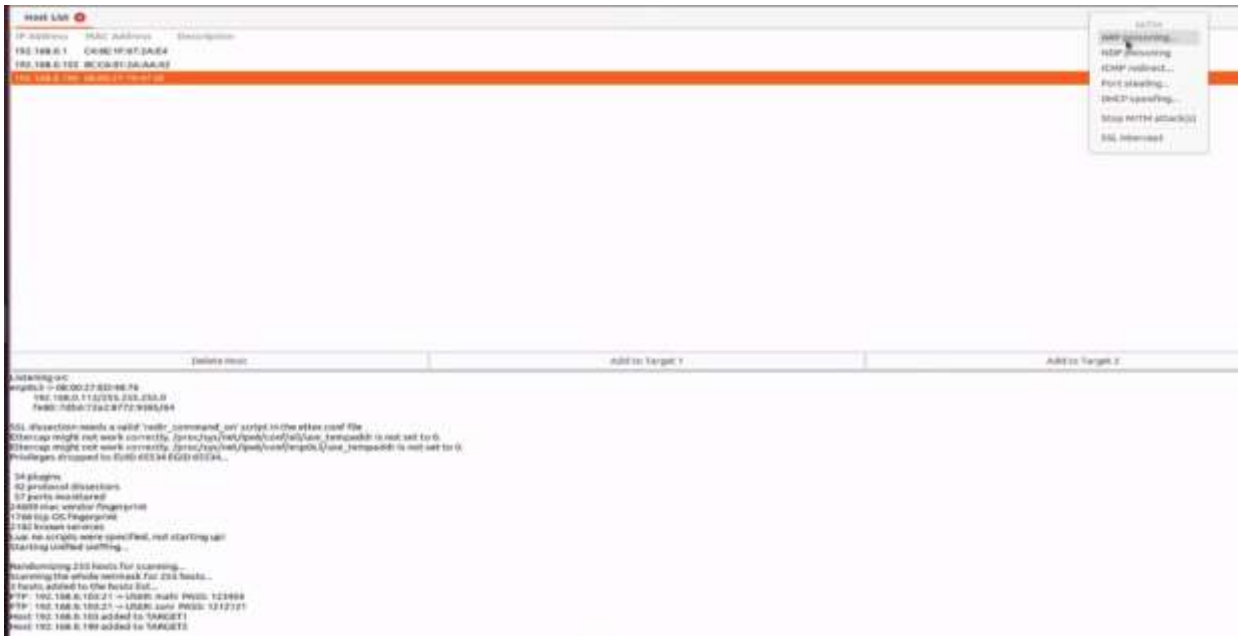
9)

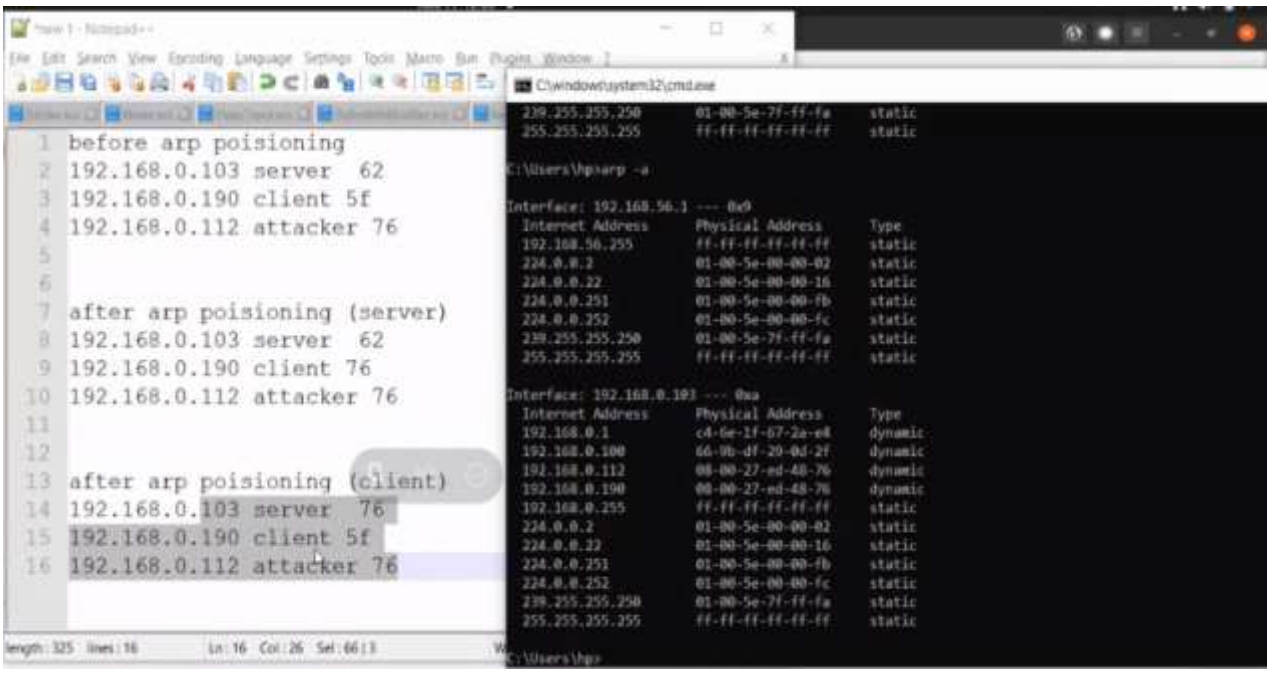
```
mareenalinux@mareenalinux:~Desktop$ sudo apt install ettercap-0.8.3.1 -G
E: Command line option 'G' [from -G] is not understood in combination with the other options.
```

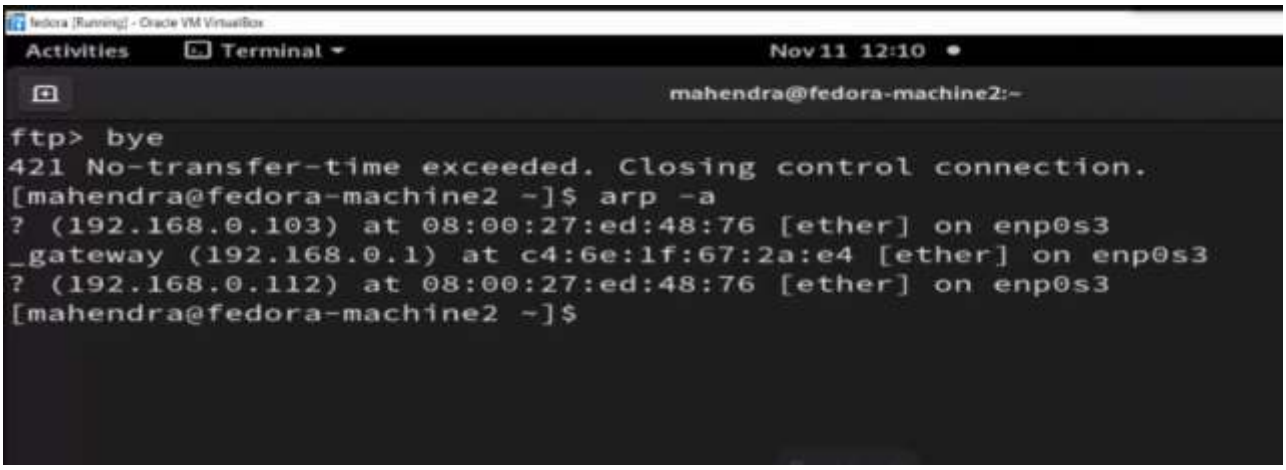
10)

```
mareenalinux@mareenalinux:~Desktop$ sudo apt install ettercap-0.8.3.1-graphical
Reading package lists... Done
Building dependency tree
Reading state information... Done
E: Unable to locate package ettercap-0.8.3.1-graphical
```

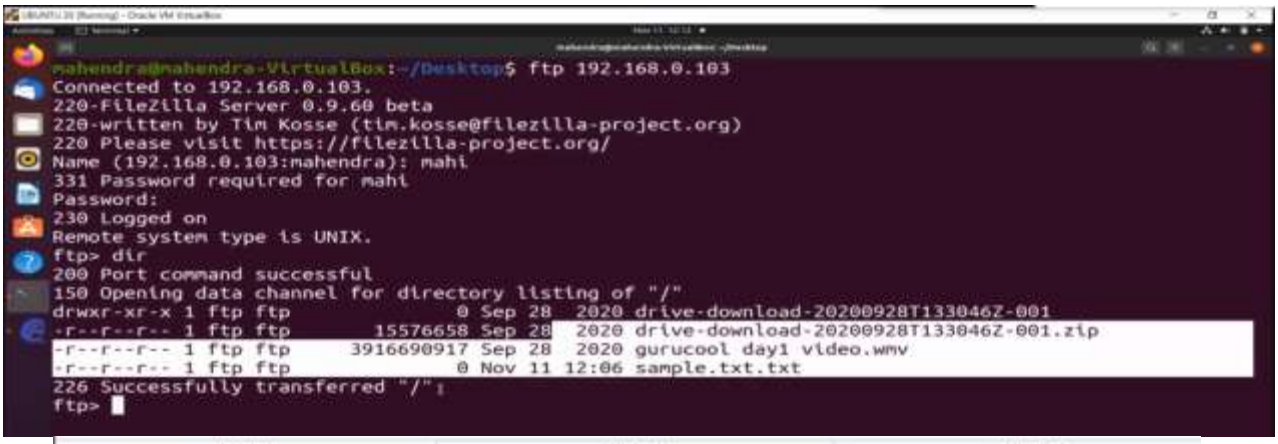
OUTPUTS:

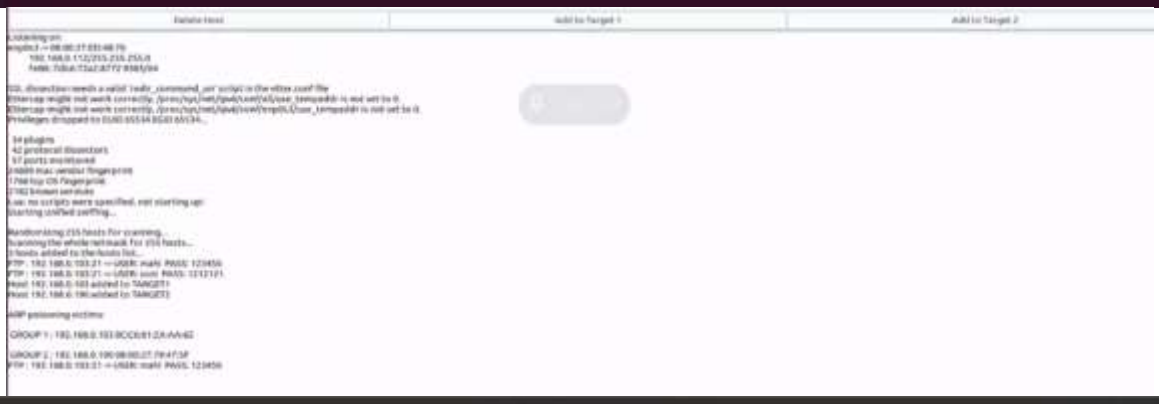


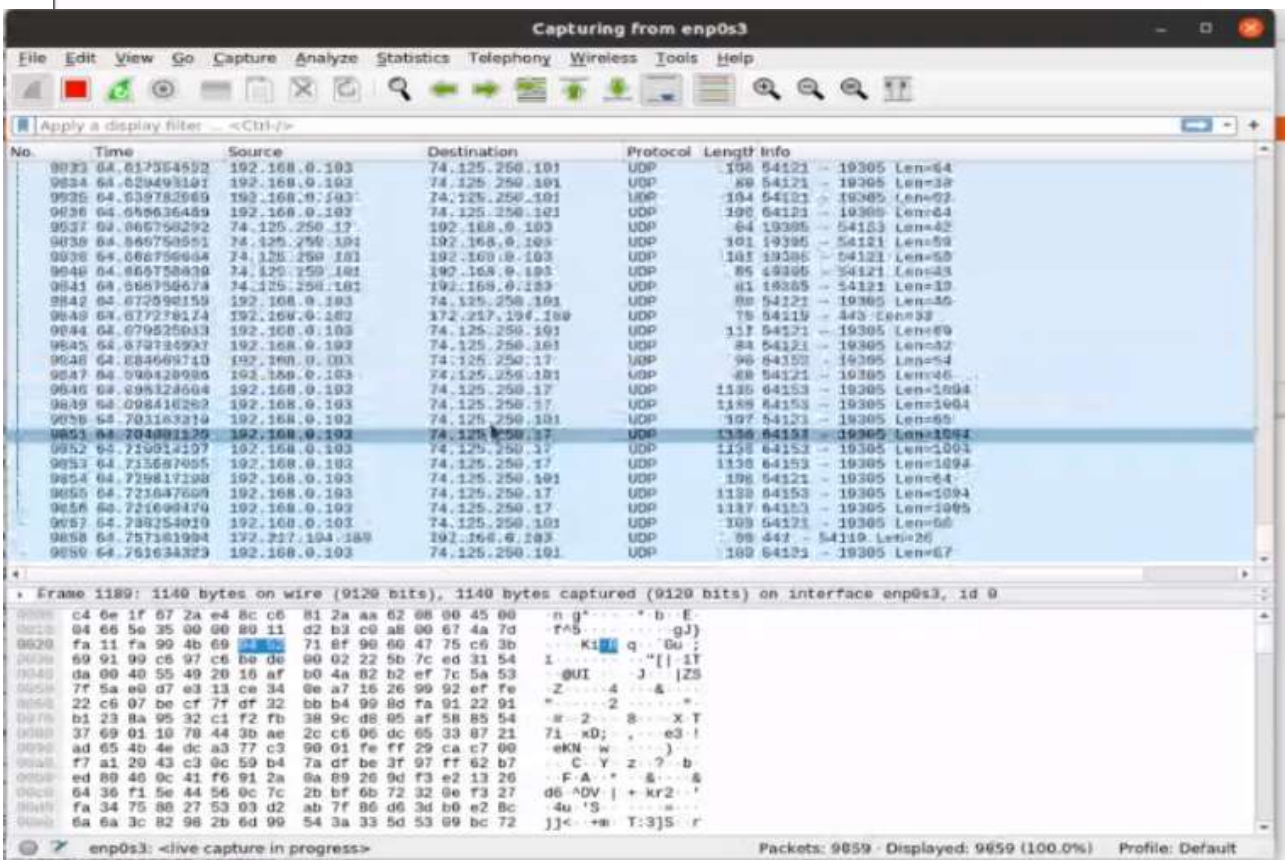

before arp poisioning
192.168.0.103 server 62
192.168.0.190 client 5f
192.168.0.112 attacker 76
after arp poisioning (server)
192.168.0.103 server 62
192.168.0.190 client 76
192.168.0.112 attacker 76
after arp poisioning (client)
192.168.0.103 server 76
192.168.0.190 client 5f
192.168.0.112 attacker 76
C:\windows\system32\cmd.exe
C:\Users\hp>arp -a
Interface: 192.168.56.1 --- 0x9
Internet Address Physical Address Type
192.168.56.255 ff-ff-ff-ff-ff-ff static
224.0.0.2 01-00-5e-00-00-02 static
224.0.0.22 01-00-5e-00-00-16 static
224.0.0.251 01-00-5e-00-00-fb static
224.0.0.252 01-00-5e-00-00-fc static
239.255.255.250 01-00-5e-7f-ff-fa static
255.255.255.255 ff-ff-ff-ff-ff-ff static
Interface: 192.168.0.103 --- 0xa
Internet Address Physical Address Type
192.168.0.1 c4-6e-1f-67-2a-e4 dynamic
192.168.0.100 66-9b-df-20-0d-2f dynamic
192.168.0.112 08-00-27-ed-48-7b dynamic
192.168.0.190 00-00-27-ed-48-7b dynamic
192.168.0.255 ff-ff-ff-ff-ff-ff static
224.0.0.2 01-00-5e-00-00-02 static
224.0.0.22 01-00-5e-00-00-16 static
224.0.0.251 01-00-5e-00-00-fb static
224.0.0.252 01-00-5e-00-00-fc static
239.255.255.250 01-00-5e-7f-ff-fa static
255.255.255.255 ff-ff-ff-ff-ff-ff static


fedora [Running] - Oracle VM VirtualBox
Activities
Terminal
Nov 11 12:10
mahendra@fedora-machine2:~
ftp> bye
421 No-transfer-time exceeded. Closing control connection.
[mahendra@fedora-machine2 ~]$ arp -a
? (192.168.0.103) at 08:00:27:ed:48:76 [ether] on enp0s3
_gateway (192.168.0.1) at c4:6e:1f:67:2a:e4 [ether] on enp0s3
? (192.168.0.112) at 08:00:27:ed:48:76 [ether] on enp0s3
[mahendra@fedora-machine2 ~]$


Activities
Terminal
Nov 11 12:11
mahendra@fedora-machine2:~ — ftp 192.168.0.103
[mahendra@fedora-machine2 ~]$ ftp 192.168.0.103
Connected to 192.168.0.103 (192.168.0.103).
220-FileZilla Server 0.9.60 beta
220-written by Tim Kosse (tim.kosse@filezilla-project.org)
220 Please visit https://filezilla-project.org/
Name (192.168.0.103:mahendra): mahi
331 Password required for mahi
Password:
230 Logged on
Remote system type is UNIX.
ftp> dir
227 Entering Passive Mode (192,168,0,103,225,118)
150 Opening data channel for directory listing of "/"
drwxr-xr-x 1 ftp ftp 0 Sep 28 2020 drive-download-20200928T133046Z-001
-r--r--r-- 1 ftp ftp 15576658 Sep 28 2020 drive-download-20200928T133046Z-001
.zip
-r--r--r-- 1 ftp ftp 3916690917 Sep 28 2020 gurucool day1 video.wmv
-r--r--r-- 1 ftp ftp 0 Nov 11 12:06 sample.txt.txt
226 Successfully transferred "/"
ftp>


mahendra@mahendra-VirtualBox:~/Desktop$ ftp 192.168.0.103
Connected to 192.168.0.103.
220-FileZilla Server 0.9.60 beta
220-written by Tim Kosse (tim.kosse@filezilla-project.org)
220 Please visit https://filezilla-project.org/
Name (192.168.0.103:mahendra): mahi
331 Password required for mahi
Password:
230 Logged on
Remote system type is UNIX.
ftp> dir
200 Port command successful
150 Opening data channel for directory listing of "/"
drwxr-xr-x 1 ftp ftp 0 Sep 28 2020 drive-download-20200928T133046Z-001
-r--r--r-- 1 ftp ftp 15576658 Sep 28 2020 drive-download-20200928T133046Z-001.zip
-r--r--r-- 1 ftp ftp 3916690917 Sep 28 2020 gurucool day1 video.wmv
-r--r--r-- 1 ftp ftp 0 Nov 11 12:06 sample.txt.txt
226 Successfully transferred "/"
ftp>




Capturing from enp0s3
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
9833 64.617354552 192.168.0.103 74.125.250.101 UDP 198 54121 → 19305 Len=64
9834 64.629493101 192.168.0.103 74.125.250.101 UDP 69 54121 → 19305 Len=38
9835 64.639782069 192.168.0.103 74.125.250.101 UDP 104 54121 → 19305 Len=62
9836 64.656636489 192.168.0.103 74.125.250.101 UDP 198 54121 → 19305 Len=64
9837 64.866750292 74.125.250.17 192.168.0.103 UDP 64 19305 → 54153 Len=42
9838 64.866750551 74.125.250.101 192.168.0.103 UDP 101 19305 → 54121 Len=59
9839 64.866750604 74.125.250.101 192.168.0.103 UDP 101 19305 → 54121 Len=59
9840 64.866750839 74.125.250.101 192.168.0.103 UDP 85 19305 → 54121 Len=43
9841 64.866750874 74.125.250.101 192.168.0.103 UDP 81 19305 → 54121 Len=39
9842 64.872598159 192.168.0.103 74.125.250.101 UDP 80 54121 → 19305 Len=38
9843 64.877278174 192.168.0.103 172.217.194.188 UDP 75 54119 → 443 Len=33
9844 64.879525033 192.168.0.103 74.125.250.101 UDP 111 54121 → 19305 Len=69
9845 64.879736937 192.168.0.103 74.125.250.101 UDP 84 54121 → 19305 Len=42
9846 64.884669719 192.168.0.103 74.125.250.17 UDP 96 54153 → 19305 Len=54
9847 64.890428986 192.168.0.103 74.125.250.101 UDP 88 54121 → 19305 Len=46
9848 64.896126604 192.168.0.103 74.125.250.17 UDP 1135 64153 → 19305 Len=1094
9849 64.898416262 192.168.0.103 74.125.250.17 UDP 1189 64153 → 19305 Len=1094
9850 64.703163219 192.168.0.103 74.125.250.101 UDP 197 54121 → 19305 Len=65
9851 64.704081175 192.168.0.103 74.125.250.17 UDP 1136 64153 → 19305 Len=1094
9852 64.719014197 192.168.0.103 74.125.250.17 UDP 1136 64153 → 19305 Len=1094
9853 64.715687055 192.168.0.103 74.125.250.17 UDP 1136 64153 → 19305 Len=1094
9854 64.729817198 192.168.0.103 74.125.250.101 UDP 198 54121 → 19305 Len=64
9855 64.721047609 192.168.0.103 74.125.250.17 UDP 1139 64153 → 19305 Len=1094
9856 64.721698479 192.168.0.103 74.125.250.17 UDP 1137 64153 → 19305 Len=1095
9857 64.738254019 192.168.0.103 74.125.250.101 UDP 109 54121 → 19305 Len=66
9858 64.757181994 172.217.194.188 192.168.0.103 UDP 88 443 → 54119 Len=26
9859 64.761634323 192.168.0.103 74.125.250.101 UDP 180 54121 → 19305 Len=67
Frame 1189: 1140 bytes on wire (9120 bits), 1140 bytes captured (9120 bits) on interface enp0s3, id 0
enp0s3: <live capture in progress>
Packets: 9859 · Displayed: 9859 (100.0%)
Profile: Default

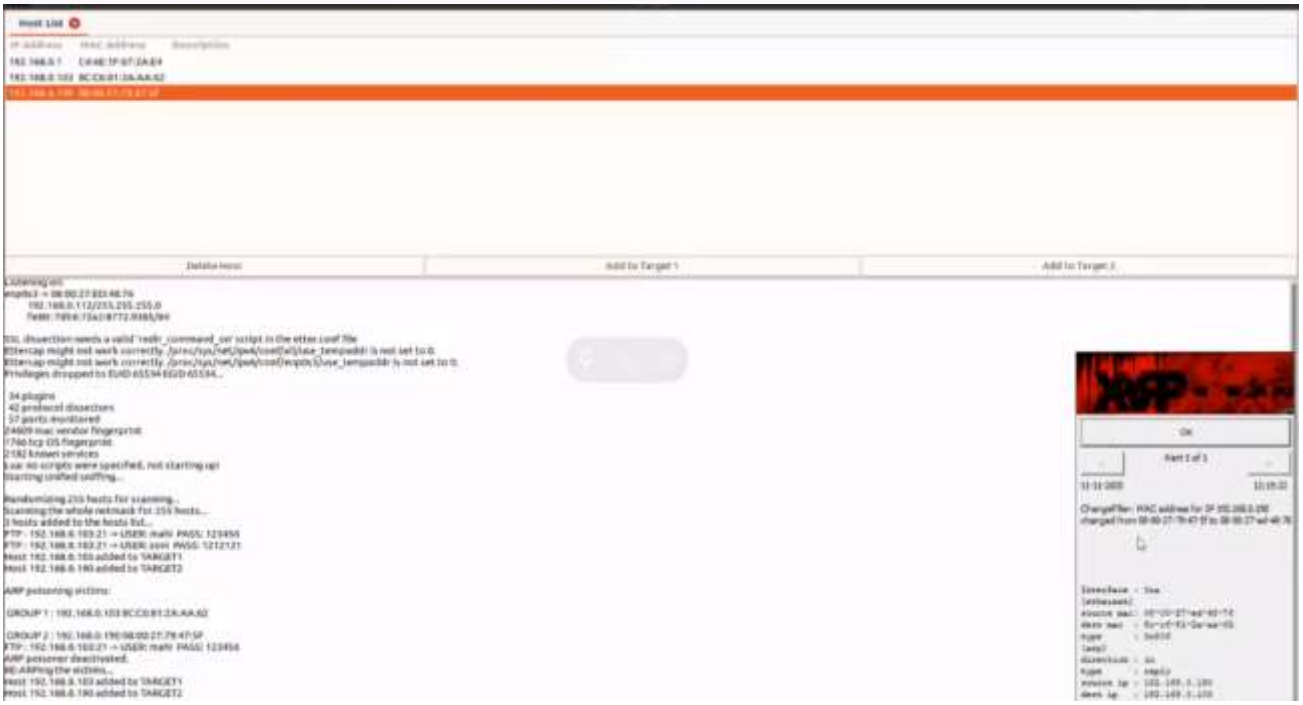
Select C:\windows\system32\cmd.exe

```
C:\Users\hp>arp -a

Interface: 192.168.56.1 --- 0x9
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 192.168.0.103 --- 0xa
  Internet Address      Physical Address      Type
  192.168.0.1           c4-6e-1f-67-2a-e4     dynamic
  192.168.0.100         66-9b-df-29-0d-2f     dynamic
  192.168.0.112         08-00-27-ed-48-76     dynamic
  192.168.0.190         08-00-27-79-47-5f     dynamic
  192.168.0.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.2             01-00-5e-00-00-02     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

C:\Users\hp>_
```



Post labs:

1. What is proxy and gratuitous proxy?

Ans:

Proxy ARP

Proxy server refers to a server that acts as an intermediary between the request made by clients, and a particular server for some services or requests for some resources. There are different types of proxy servers available that are put into use according to the purpose of a request made by the clients to the servers. The basic purpose of Proxy servers is to protect the direct connection of Internet clients and internet resources. The proxy server also prevents the identification of the client's IP address when the client makes any request is made to any other servers.

a. **Internet Client and Internet resources:** For internet clients, Proxy servers also act as a shield for an internal network against the request coming from a client to access the data stored on the server. It makes the original IP address of the node remains hidden while accessing data from that server.
b. **Protects true host identity:** In this method, outgoing traffic appears to come from the proxy server rather than internet navigation. It must be configured to the specific application such as HTTPs or FTP. For example, organizations can use a proxy to observe the traffic of its employees to get the work efficiently done. It can also be used to keep a check on any kind of highly confidential data leakage. Some can also use it to increase their websites rank.

Well, the ASA proxy arps for all its global addresses, meaning, we will answer who we are if someone asked us. When an ARP request is made for the global IP address of the Iron-port server, 14.36.10.138, the security appliance responds with its own MAC address.
If the router were to ask the ASA, it would reply as below:
28: 04:09:44.939007 arp who-has 14.36.10.138 tell 14.36.10.142
29: 04:09:44.939053 arp reply 14.36.10.138 is-at 0:16:c7:9f:73:ef

Gratuitous ARP

Gratuitous ARP could mean both gratuitous ARP *request* or gratuitous ARP *reply*. Gratuitous in this case means a request/reply that is not normally needed according to the ARP specification (RFC 826) but could be used in some cases. A gratuitous ARP request is an AddressResolutionProtocol request packet where the source and destination IP are both set to the IP of the machine issuing the packet and the destination MAC is the broadcast address ff:ff:ff:ff:ff:ff. Ordinarily, no reply packet will occur. A gratuitous ARP reply is a reply to which no request has been made.

In this case we needed the ASA to send a gratuitous arp meaning we wanted the ASA to announce to everyone that it owns this IP address 14.36.10.138. An ARP announcement is not intended to solicit a reply; instead it updates any cached entries in the ARP tables of other hosts that receive the packet.

1: 03:38:35.873840 0016.c79f.73ef ffff.ffff.ffff 0x0806 42: arp who-has 14.36.10.138 tell 14.36.10.138