

Network Security Practices
CY5150
Task 7

Submitted By:
Sonam Ghatode(001305171)

Table of Contents

Kali Source IP and MAC:	2
Target Details:	2
Introduction to Ettercap:	3
Target ARP table before and during the attack:	5
Target Desktop accessing khoury.neu.edu during attack:	6
Tcpdump output in kali displaying target IP passing traffic during ARP poisoning:	6
References:	8

Kali Source IP and MAC:

Source IP: 10.0.0.12

MAC: 00:0C:29:D3:BF:AE

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.0.12 netmask 255.255.255.0 broadcast 10.0.0.255
        inet6 fe80::20c:29ff:fed3:bfae prefixlen 64 scopeid 0x20<link>
        inet6 fe80::20c:29ff:fed3:bfae prefixlen 64 scopeid 0x0<global>
    ether 00:0c:29:d3:bf:ae txqueuelen 1000 (Ethernet)
        RX packets 28 bytes 4767 (4.6 KiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 89 bytes 9009 (8.7 KiB)
        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 8 bytes 396 (396.0 B)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 8 bytes 396 (396.0 B)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Target Details:

Target OS: Ubuntu

Target IP: 10.0.0.167

Target MAC(from victim's system): 00:0C:29:D8:9A:27

Target MAC(from Ettercap): 4C:1D:96:7D:E7:A4

```
File Edit View Search Terminal Help
bhariesshkumar@ubuntu:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.0.167 netmask 255.255.255.0 broadcast 10.0.0.255
        inet6 fe80::20c:29ff:fed3:bfae prefixlen 128 scopeid 0x20<link>
        inet6 fe80::3255:f1aa:92f2:509a prefixlen 64 scopeid 0x0<global>
        inet6 fe80::20c:29ff:fed3:bfae prefixlen 64 scopeid 0x0<global>
    ether 00:0c:29:d8:9a:27 txqueuelen 1000 (Ethernet)
        RX packets 24795 bytes 37127415 (37.1 MB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 1433 bytes 141425 (141.4 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 180 bytes 14324 (14.3 KB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 180 bytes 14324 (14.3 KB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Introduction to Ettercap:

Ettercap is an open source network security tool that launches Man-In-The-Middle(MITM) attacks on LAN and can be used for network protocol analysis and security auditing. It is capable of intercepting traffic on a network, capturing passwords, and active eavesdropping against a number of common protocols. It works by keeping the network interface into promiscuous mode and by ARP poisoning the target machines.

Ettercap has four modes of operation:

- IP-based: packets are filtered based on source and destination of IP packet.
- MAC-based: packets are filtered based on MAC address, useful for sniffing connections through a gateway.
- ARP-based: uses ARP poisoning to sniff on a switched LAN between two hosts.
- PublicARP-based: uses ARP poisoning to sniff on a switched LAN from a victim host to all other hosts.

In this task, ARP-poisoning had to be done. Ettercap is a UI-based application that uses Target 1 as the gateway(i.e. Router) via which the attacker is connected to the internet, and Target 2 as the IP of the scanned target in the same network. Ettercap allows to first search the hosts in the same network and then launch ARP spoofing on the desired target. To launch the ARP Spoof attack on the victim without DOSing the victim needed the attacker to enable IP forwarding in the system. In kali, the command **sudo sysctl -w net.ipv4.ip_forward=1** is used to enable IP forwarding to ensure traffic is forwarded to the gateway to prevent DOSing the target.

To attack a host in the network, scanning was done first using the ettercap tool. Following shows the screenshot of the scanned hosts:

IP Address	MAC Address	Description
10.0.0.1	D4:B9:2F:AB:71:A9	
10.0.0.54	A4:83:E7:77:84:37	
10.0.0.61	20:16:D8:D3:B2:30	
10.0.0.74	88:50:F6:05:66:1E	
10.0.0.75	8C:86:1E:D8:51:BB	
10.0.0.116	4C:1D:96:7D:E7:A4	
10.0.0.124	4C:1D:96:7D:E7:A4	
10.0.0.131	00:F6:20:84:EC:B7	
10.0.0.167	4C:1D:96:7D:E7:A4	
2601:197:b80:a460:111e:2032:18b0:74bb	A4:83:E7:6F:17:0A	
fe80::d6b9:2fff:feab:71a9	D4:B9:2F:AB:71:A9	
10.0.0.224	A4:83:E7:6F:17:0A	

Host 10.0.0.1 added to TARGET1
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
Scanning for merged targets (1 hosts)...
12 hosts added to the hosts list...

Among these, 10.0.0.167 was identified as the host I wanted to attack. Therefore, gateway(router) with IP 10.0.0.1 was added as Target 1 and 10.0.0.167 was added as Target 2 to launch ARP Spoofing attack:

The screenshot shows the Ettercap interface with the 'Host List' tab selected. A table lists network hosts with their IP addresses, MAC addresses, and descriptions. The host '10.0.0.167' is highlighted with a blue selection bar. Below the table are three buttons: 'Delete Host', 'Add to Target 1', and 'Add to Target 2'. A status message at the bottom indicates: 'Scanning the whole netmask for 255 hosts...', 'Scanning for merged targets (1 hosts)...', '12 hosts added to the hosts list...', 'Host 10.0.0.1 added to TARGET1', and 'Host 10.0.0.167 added to TARGET2'.

After adding the targets, MITM attack was launched:

The screenshot shows the Ettercap interface with the 'Host List' tab selected. A table lists network hosts. A 'MITM Attack: ARP Poisoning' dialog box is open over the host '10.0.0.167'. The dialog has 'Cancel' and 'OK' buttons. It contains an 'Optional parameters' section with two checkboxes: 'Sniff remote connections.' (checked) and 'Only poison one-way.' (unchecked). A green question mark icon is located in the bottom-left corner of the dialog. Below the dialog, the host list table continues with other hosts. Status messages at the bottom are identical to the previous screenshot.

After starting the attack, if the victim tried to access any site which did not have HTTPS, the credentials were in plaintext and prone to sniffing. We searched a site that did http login, following was the result when it was accessed using victim machine:

IP Address	MAC Address	Description
2601:197:b80:a460:111e:2032:18b0:74bb	A4:83:E7:6F:17:0A	
fe80::180b:c928:dc14:1cd1	A4:83:E7:6F:17:0A	
10.0.0.1	D4:B9:2F:AB:71:A9	
10.0.0.61	20:16:D8:D3:B2:30	
10.0.0.74	88:50:F6:05:66:1E	
10.0.0.116	4C:1D:96:7D:E7:A4	
10.0.0.124	4C:1D:96:7D:E7:A4	
10.0.0.131	00:F6:20:84:EC:B7	
fe80::d6b9:2fff:feab:71a9	D4:B9:2F:AB:71:A9	
10.0.0.167	4C:1D:96:7D:E7:A4	
10.0.0.175	74:42:8B:0C:1E:C0	
10.0.0.180	A4:83:E7:07:66:1C	
10.0.0.224	A4:83:E7:6F:17:0A	

13 hosts added to the hosts list...
Host 10.0.0.1 added to TARGET1
Host 10.0.0.167 added to TARGET2

ARP poisoning victims:

GROUP 1 : 10.0.0.1 D4:B9:2F:AB:71:A9

GROUP 2 : 10.0.0.167 4C:1D:96:7D:E7:A4

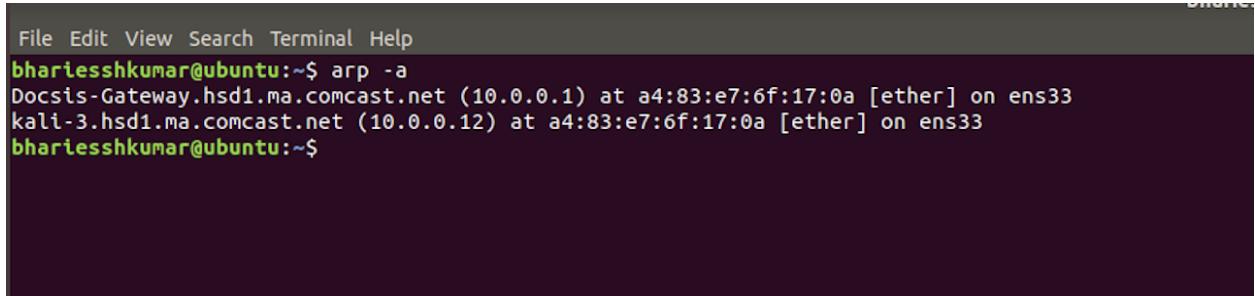
HTTP : 193.110.250.6:80 -> USER: hello PASS: Netsecrocks INFO: http://login.petrolweb.net/
CONTENT: UserName=hello&Password=Netsecrocks

Target ARP table before and during the attack:

In this screenshot, the gateway's actual MAC is there i.e. ARP entry before the attack:

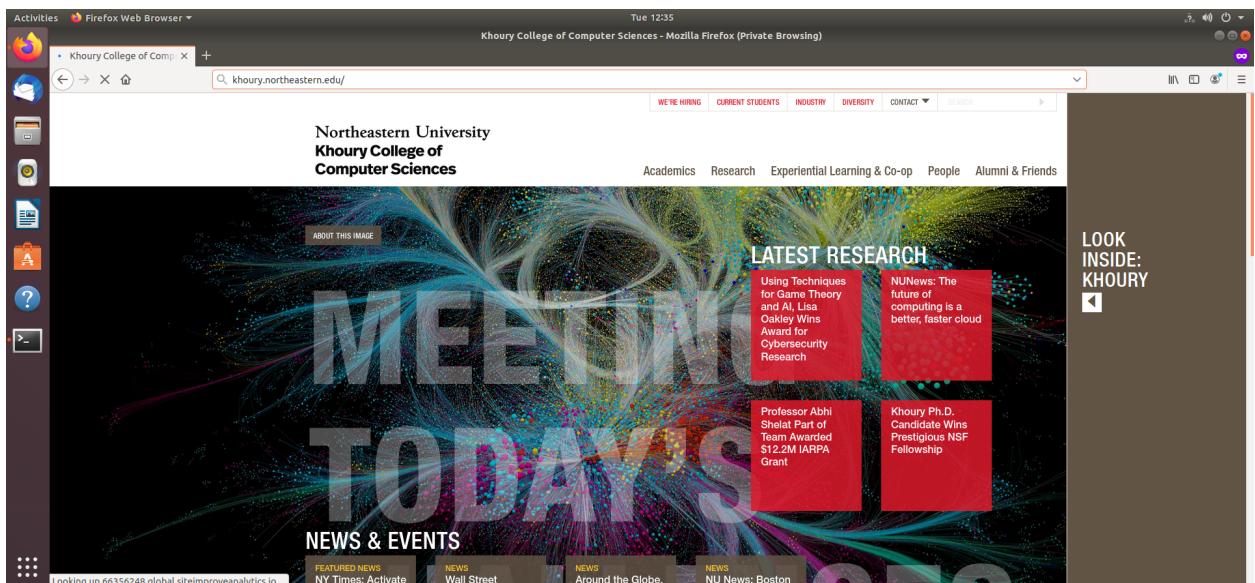
```
bhariesshkumar@ubuntu:~$ arp -a
Docsis-Gateway.hsd1.ma.comcast.net (10.0.0.1) at d4:b9:2f:ab:71:a9 [ether] on ens33
bhariesshkumar@ubuntu:~$
```

During the attack, Gateway's address got changed to the attacker's MAC(both the entries have same MAC):



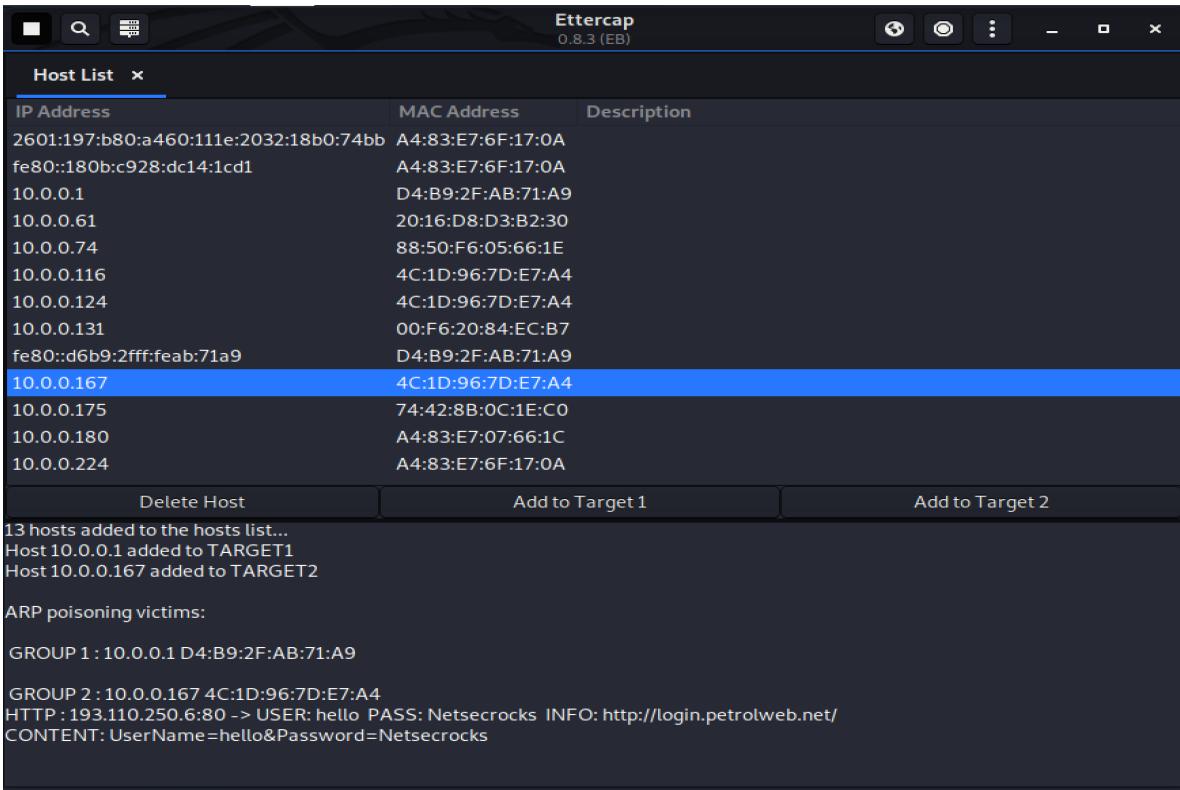
```
File Edit View Search Terminal Help
bhartiesshkumar@ubuntu:~$ arp -a
Docsis-Gateway.hsd1.ma.comcast.net (10.0.0.1) at a4:83:e7:6f:17:0a [ether] on ens33
kali-3.hsd1.ma.comcast.net (10.0.0.12) at a4:83:e7:6f:17:0a [ether] on ens33
bhartiesshkumar@ubuntu:~$
```

Target Desktop accessing khoury.neu.edu during attack:



Tcpdump output in kali displaying target IP passing traffic during ARP poisoning:

Screenshots showing the target scanned using Ettercap accessing khoury.neu.edu from attacker as gateway:



MAC, as scanned by Ettercap for 10.0.0.167 is 4C:1D:96:7D:E7:A4. The following screenshot shows the name for the listed MAC in tcpdump:

```
15:32:33.862292 ARP, Request who-has 10.0.0.196 tell kali-3.hsd1.ma.comcast.net, length 28
15:32:33.872642 ARP, Request who-has 10.0.0.181 tell kali-3.hsd1.ma.comcast.net, length 28
15:32:33.882001 ARP, Request who-has ubuntu.hsd1.ma.comcast.net tell kali-3.hsd1.ma.comcast.net, length 28
15:32:33.886671 ARP, Reply ubuntu.hsd1.ma.comcast.net is-at 4c:1d:96:7d:e7:a4 (oui Unknown), length 46
15:32:33.893176 ARP, Request who-has 10.0.0.157 tell kali-3.hsd1.ma.comcast.net, length 28
15:32:33.903413 ARP, Request who-has 10.0.0.151 tell kali-3.hsd1.ma.comcast.net, length 28
15:32:33.912715 ARP, Request who-has Google Home Mini hsd1.ma.comcast.net tell kali-3.hsd1.ma.comcast.net, length 28
```

And the screenshot of the victim's request going through system:

```
A 2601:9000:20ee:1c00:3:4b0::de80:93a1, AAAA 2600:9000:20ee:e200:3:4b0::de80:93a1, AAAA 2600:9000:20ee:1200:3:4b0::de80:93a1, AAAA 2600:9000:20ee:a000:3:4b0::de80:93a1 (295)
15:33:46.429052 IP 193.110.250.6.http > ubuntu.hsd1.ma.comcast.net.53018: Flags [.], ack 931, win 258, options [nop,nop,TS val 23539840 ecr 3590815698], length 0
15:33:46.431138 IP 193.110.250.6.http > ubuntu.hsd1.ma.comcast.net.53018: Flags [.], ack 931, win 258, options [nop,nop,TS val 23539840 ecr 3590815698], length 0
15:33:46.439194 IP ubuntu.hsd1.ma.comcast.net.50137 > cdns02.comcast.net.domain: 14732+ A? khoury.neu.edu. (32)
15:33:46.442123 IP ubuntu.hsd1.ma.comcast.net.51321 > cdns02.comcast.net.domain: 1615+ AAAA? khoury.neu.edu. (32)
15:33:46.447414 IP ubuntu.hsd1.ma.comcast.net.50137 > cdns02.comcast.net.domain: 14752+ A? khoury.neu.edu. (32)
15:33:46.447696 IP ubuntu.hsd1.ma.comcast.net.51321 > cdns02.comcast.net.domain: 1615+ AAAA? khoury.neu.edu. (32)
15:33:46.453462 IP ubuntu.hsd1.ma.comcast.net.53020 > 193.110.250.6.http: Flags [.], ack 410, win 501, options [nop,nop,TS val 3590825850 ecr 23538839], length 0
15:33:46.455108 IP ubuntu.hsd1.ma.comcast.net.53020 > 193.110.250.6.http: Flags [.], ack 410, win 501, options [nop,nop,TS val 3590825850 ecr 23538839], length 0
15:33:46.471591 IP ubuntu.hsd1.ma.comcast.net.54423 > cdns02.comcast.net.domain: 49564+ A? www.khoury.northeastern.edu. (45)
15:33:46.479388 IP ubuntu.hsd1.ma.comcast.net.54423 > cdns02.comcast.net.domain: 49564+ A? www.khoury.northeastern.edu. (45)
15:33:46.480712 IP cdns02.comcast.net.domain > ubuntu.hsd1.ma.comcast.net.50137: 14752 1/0/0 A 52.70.229.197 (48)
15:33:46.486992 IP cdns02.comcast.net.domain > ubuntu.hsd1.ma.comcast.net.50137: 14752 1/0/0 A 52.70.229.197 (48)
15:33:46.487097 IP cdns02.comcast.net.domain > ubuntu.hsd1.ma.comcast.net.51321: 6155 0/1/0 (87)
15:33:46.487109 IP cdns02.comcast.net.domain > ubuntu.hsd1.ma.comcast.net.51321: 6155 0/1/0 (87)
15:33:46.513080 IP cdns02.comcast.net.domain > ubuntu.hsd1.ma.comcast.net.54423: 49564 2/0/0 CNAME presscache.khoury.northeastern.edu., A 52.70.229.197 (86)
15:33:46.519045 IP cdns02.comcast.net.domain > ubuntu.hsd1.ma.comcast.net.54423: 49564 2/0/0 CNAME presscache.khoury.northeastern.edu., A 52.70.229.197 (86)
15:33:46.526881 IP ubuntu.hsd1.ma.comcast.net.40654 > cdns02.comcast.net.domain: 63797+ AAAA? presscache.khoury.northeastern.edu. (52)
15:33:46.535247 IP ubuntu.hsd1.ma.comcast.net.40654 > cdns02.comcast.net.domain: 63797+ AAAA? presscache.khoury.northeastern.edu. (52)
15:33:46.550317 IP 193.110.250.6.http > ubuntu.hsd1.ma.comcast.net.53020: Flags [.], ack 924, win 258, options [nop,nop,TS val 23539852 ecr 3590815830], length 0
15:33:46.550876 IP 193.110.250.6.http > ubuntu.hsd1.ma.comcast.net.53020: Flags [.], ack 924, win 258, options [nop,nop,TS val 23539852 ecr 3590815830], length 0
15:33:46.564921 IP cdns02.comcast.net.domain > ubuntu.hsd1.ma.comcast.net.40654: 63797 0/1/0 (111)
15:33:46.567029 IP cdns02.comcast.net.domain > ubuntu.hsd1.ma.comcast.net.40654: 63797 0/1/0 (111)
15:33:46.635280 IP6 fe80::180b:c928:dc14:1cd1 > fe80::d6b9:2fff:feab:71a9: ICMP6, neighbor advertisement, tgt is fe80::180b:c928:dc14:1cd1, length 24
15:33:47.028107 IP6 fe80::20c:29ff:fed3:bfae > ff02::16: BHB ICMP6, multicast listener report v2, 3 group record(s), length 68
15:33:47.634309 IP Sonams-MBP.hsd1.ma.comcast.net.61880 > 63.251.114.136.https: Flags [.], ack 9147, win 2047, options [nop,nop,TS val 607721582 ecr 3953303525], length 0
15:33:47.634312 IP Sonams-MBP.hsd1.ma.comcast.net.61880 > 63.251.114.136.https: Flags [.], ack 9148, win 2047, options [nop,nop,TS val 607721582 ecr 3953303525], length 0
```

References:

- [1] [https://en.wikipedia.org/wiki/Ettercap_\(software\)](https://en.wikipedia.org/wiki/Ettercap_(software))