Aleyna Aydin
CS 646
Jun 18, 2024

Task 1:

Steps

1.
```
aleyna@aleyna-VMware-Virtual-Platform:~$ ping -c1 192.168.111.131
PING 192.168.111.131 (192.168.111.131) 56(84) bytes of data.
64 bytes from 192.168.111.131: icmp_seq=1 ttl=64 time=0.435 ms

--- 192.168.111.131 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.435/0.435/0.435/0.000 ms
```
Here, we are on Alice's machine where she is transmitting an ICMP echo request to Bob's machine where his IP address is 192.168.111.131.

2.
```
aleyna@aleyna-VMware-Virtual-Platform:~$ arp
Help                    HWtype  HWaddress           Flags Mask            Iface
192.168.111.254         ether   00:50:56:ee:35:ef   C                     ens33
192.168.111.131         ether   00:0c:29:8a:fb:04   C                     ens33
_gateway                ether   00:50:56:f2:75:18   C                     ens33
```
Through this command, we can see the ARP cache table listing the past IP/MAC addresses that we have been in contact with.

3.
```
aleyna@aleyna-VMware-Virtual-Platform:~$ sudo arp -d 192.168.111.131
aleyna@aleyna-VMware-Virtual-Platform:~$ arp
Address                 HWtype  HWaddress           Flags Mask            Iface
192.168.111.254         ether   00:50:56:ee:35:ef   C                     ens33
_gateway                ether   00:50:56:f2:75:18   C                     ens33
```
Here, we have deleted Bob's entry on the ARP table using the -d command and can see the updated ARP cache table which no longer contains Bob's IP address.

4.
```
aleyna@aleyna-VMware-Virtual-Platform:~$ ping -c1 192.168.111.131; ping -c1 192.
168.111.130
PING 192.168.111.131 (192.168.111.131) 56(84) bytes of data.
64 bytes from 192.168.111.131: icmp_seq=1 ttl=64 time=1.07 ms

--- 192.168.111.131 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.069/1.069/1.069/0.000 ms
PING 192.168.111.130 (192.168.111.130) 56(84) bytes of data.
64 bytes from 192.168.111.130: icmp_seq=1 ttl=64 time=0.741 ms

--- 192.168.111.130 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.741/0.741/0.741/0.000 ms
aleyna@aleyna-VMware-Virtual-Platform:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.111.130          ether   00:0c:29:80:9d:86   C                     ens33
192.168.111.254          ether   00:50:56:ee:35:ef   C                     ens33
192.168.111.131          ether   00:0c:29:8a:fb:04   C                     ens33
_gateway                 ether   00:50:56:f2:75:18   C                     ens33
aleyna@aleyna-VMware-Virtual-Platform:~$ sudo ip neigh flush all
aleyna@aleyna-VMware-Virtual-Platform:~$ arp
aleyna@aleyna-VMware-Virtual-Platform:~$
```

Lastly, we have sent an ICMP echo request to both Bob and Eve's machines where Eve's IP address is 192.168.111.130. Using the 'arp' command we can see that both requests have been logged in the ARP cache table. By using the 'ip neigh flush all' command, we have cleared the entirety of the ARP table rather than just a single entry. This is shown by there being no output after the last 'arp' command.

Task 2:

Steps

1.
```
bob@bob-VMware-Virtual-Platform:~$ sudo tcpdump -pi ens33 arp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on ens33, link-type EN10MB (Ethernet), snapshot length 262144 bytes
21:02:46.851887 ARP, Request who-has bob-VMware-Virtual-Platform tell 192.168.111.128, length 46
21:02:46.851911 ARP, Reply bob-VMware-Virtual-Platform is-at 00:0c:29:8a:fb:04 (oui Unknown), length 28
21:02:51.918705 ARP, Request who-has 192.168.111.128 tell bob-VMware-Virtual-Platform, length 28
21:02:51.919648 ARP, Reply 192.168.111.128 is-at 00:0c:29:13:64:74 (oui Unknown), length 46
21:02:52.431543 ARP, Request who-has _gateway tell bob-VMware-Virtual-Platform, length 28
21:02:52.431799 ARP, Reply _gateway is-at 00:50:56:f2:75:18 (oui Unknown), length 46
^C
6 packets captured
6 packets received by filter
0 packets dropped by kernel
```

Here, we are using tcpdump to only capture packets of the ARP protocol on Bob's virtual machine.

2.
```
aleyna@aleyna-VMware-Virtual-Platform:~$ sudo arp -d 192.168.111.131
[sudo] password for aleyna:
aleyna@aleyna-VMware-Virtual-Platform:~$ ping -c1 192.168.111.131
PING 192.168.111.131 (192.168.111.131) 56(84) bytes of data.
64 bytes from 192.168.111.131: icmp_seq=1 ttl=64 time=1.92 ms

--- 192.168.111.131 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.916/1.916/1.916/0.000 ms
aleyna@aleyna-VMware-Virtual-Platform:~$ sudo arp -d 192.168.111.131
```

Next, on Alice's machine, we are deleting the entry of Bob's machine from the ARP cache table. Then, we are sending another ICMP echo request to Bob's machine and deleting it once again. The packets captured from this are pictured above in Bob's terminal.

3.
```
bob@bob-VMware-Virtual-Platform:~$ sudo tcpdump -epi ens33 arp
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on ens33, link-type EN10MB (Ethernet), snapshot length 262144 bytes
21:03:37.735795 00:50:56:c0:00:08 (oui Unknown) > Broadcast, ethertype ARP (0x0806), length 60: Request who-has _gateway
 tell 192.168.111.1, length 46
21:03:39.007514 00:50:56:c0:00:08 (oui Unknown) > Broadcast, ethertype ARP (0x0806), length 60: Request who-has _gateway
 tell 192.168.111.1, length 46
21:03:39.736115 00:50:56:c0:00:08 (oui Unknown) > Broadcast, ethertype ARP (0x0806), length 60: Request who-has _gateway
 tell 192.168.111.1, length 46
21:03:40.726489 00:50:56:c0:00:08 (oui Unknown) > Broadcast, ethertype ARP (0x0806), length 60: Request who-has _gateway
 tell 192.168.111.1, length 46
21:03:42.658765 00:0c:29:13:64:74 (oui Unknown) > Broadcast, ethertype ARP (0x0806), length 60: Request who-has bob-VMwa
re-Virtual-Platform tell 192.168.111.128, length 46
21:03:42.658781 00:0c:29:8a:fb:04 (oui Unknown) > 00:0c:29:13:64:74 (oui Unknown), ethertype ARP (0x0806), length 42: Re
ply bob-VMware-Virtual-Platform is-at 00:0c:29:8a:fb:04 (oui Unknown), length 28
21:03:43.118709 00:0c:29:8a:fb:04 (oui Unknown) > 00:50:56:f2:75:18 (oui Unknown), ethertype ARP (0x0806), length 42: Re
quest who-has _gateway tell bob-VMware-Virtual-Platform, length 28
21:03:43.118973 00:50:56:f2:75:18 (oui Unknown) > 00:0c:29:8a:fb:04 (oui Unknown), ethertype ARP (0x0806), length 60: Re
ply _gateway is-at 00:50:56:f2:75:18 (oui Unknown), length 46
21:03:46.544258 00:50:56:c0:00:08 (oui Unknown) > Broadcast, ethertype ARP (0x0806), length 60: Request who-has _gateway
 tell 192.168.111.1, length 46
21:03:47.240257 00:50:56:c0:00:08 (oui Unknown) > Broadcast, ethertype ARP (0x0806), length 60: Request who-has _gateway
 tell 192.168.111.1, length 46
21:03:47.726897 00:0c:29:8a:fb:04 (oui Unknown) > 00:0c:29:13:64:74 (oui Unknown), ethertype ARP (0x0806), length 42: Re
quest who-has 192.168.111.128 tell bob-VMware-Virtual-Platform, length 28
21:03:47.727338 00:0c:29:13:64:74 (oui Unknown) > 00:0c:29:8a:fb:04 (oui Unknown), ethertype ARP (0x0806), length 60: Re
ply 192.168.111.128 is-at 00:0c:29:13:64:74 (oui Unknown), length 46
21:03:48.229661 00:50:56:c0:00:08 (oui Unknown) > Broadcast, ethertype ARP (0x0806), length 60: Request who-has _gateway
 tell 192.168.111.1, length 46
21:03:49.560319 00:50:56:c0:00:08 (oui Unknown) > Broadcast, ethertype ARP (0x0806), length 60: Request who-has _gateway
 tell 192.168.111.1, length 46
```

Here. we can see the ARP protocol packets captured by tcpdump through the commands inputted on Alice's machine in the next step. The next command we are inputting on Bob's machine is to capture packets once again through tcpdump while also choosing to print link-level information.

4.
```
aleyna@aleyna-VMware-Virtual-Platform:~$ ping -c1 192.168.111.131
PING 192.168.111.131 (192.168.111.131) 56(84) bytes of data.
64 bytes from 192.168.111.131: icmp_seq=1 ttl=64 time=1.05 ms

--- 192.168.111.131 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.054/1.054/1.054/0.000 ms
```

Once again, we are sending the ICMP echo request to Bob's machine from Alice and its packets can be seen above which is includes the header information.

5.

```
 tell 192.168.111.1, length 46
21:03:49.560319 00:50:56:c0:00:08 (oui Unknown) > Broadcast, ethertype ARP (0x0806), length 60: Request who-has _gateway
 tell 192.168.111.1, length 46
^C
14 packets captured
15 packets received by filter
0 packets dropped by kernel
```

```
bob@bob-VMware-Virtual-Platform:~$ sudo tcpdump -Xpi ens33 port telnet
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on ens33, link-type EN10MB (Ethernet), snapshot length 262144 bytes
21:04:18.333729 IP 192.168.111.128.52008 > bob-VMware-Virtual-Platform.telnet: Flags [S], seq 345226178, win 32120, opti
ons [mss 1460,sackOK,TS val 2662307416 ecr 0,nop,wscale 7], length 0
        0x0000:  4500 003c 003c 4000 4006 da2b c0a8 6f80  E..<.<@.@..+..o.
        0x0010:  c0a8 6f83 cb28 0017 1493 bbc2 0000 0000  ..o..(..........
        0x0020:  a002 7d78 9995 0000 0204 05b4 0402 080a  ..}x............
        0x0030:  9eaf 9658 0000 0000 0103 0307            ...X........
21:04:18.333801 IP bob-VMware-Virtual-Platform.telnet > 192.168.111.128.52008: Flags [S.], seq 1692013397, ack 345226179
, win 31856, options [mss 1460,sackOK,TS val 292062910 ecr 2662307416,nop,wscale 7], length 0
        0x0000:  4500 003c 0000 4000 4006 da67 c0a8 6f83  E..<..@.@..g..o.
        0x0010:  c0a8 6f80 0017 cb28 64da 1355 1493 bbc3  ..o....(d..U....
        0x0020:  a012 7c70 6083 0000 0204 05b4 0402 080a  ..|p`...........
        0x0030:  1168 86be 9eaf 9658 0103 0307            .h.....X....
21:04:18.334380 IP 192.168.111.128.52008 > bob-VMware-Virtual-Platform.telnet: Flags [.], ack 1, win 251, options [nop,n
op,TS val 2662307416 ecr 292062910], length 0
        0x0000:  4500 0034 003d 4000 4006 da32 c0a8 6f80  E..4.=@.@..2..o.
        0x0010:  c0a8 6f83 cb28 0017 1493 bbc3 64da 1356  ..o..(......d..V
        0x0020:  8010 00fb 3478 0000 0101 080a 9eaf 9658  ....4x.........X
        0x0030:  1168 86be                                .h..
21:04:18.334901 IP 192.168.111.128.52008 > bob-VMware-Virtual-Platform.telnet: Flags [P.], seq 1:34, ack 1, win 251, opt
ions [nop,nop,TS val 2662307417 ecr 292062910], length 33 [telnet DO ENCRYPT, WILL ENCRYPT, DO SUPPRESS GO AHEAD, WILL T
ERMINAL TYPE, WILL NAWS, WILL TSPEED, WILL LFLOW, WILL LINEMODE, WILL NEW-ENVIRON, DO STATUS, WILL XDISPLOC]
        0x0000:  4500 0055 003e 4000 4006 da10 c0a8 6f80  E..U.>@.@.....o.
        0x0010:  c0a8 6f83 cb28 0017 1493 bbc3 64da 1356  ..o..(......d..V
        0x0020:  8018 00fb 92dc 0000 0101 080a 9eaf 9659  ...............Y
        0x0030:  1168 86be fffd 26ff fb26 fffd 03ff fb18  .h....&..&......
        0x0040:  fffb 1fff fb20 fffb 21ff fb22 fffb 27ff  ........!.."..'.
```

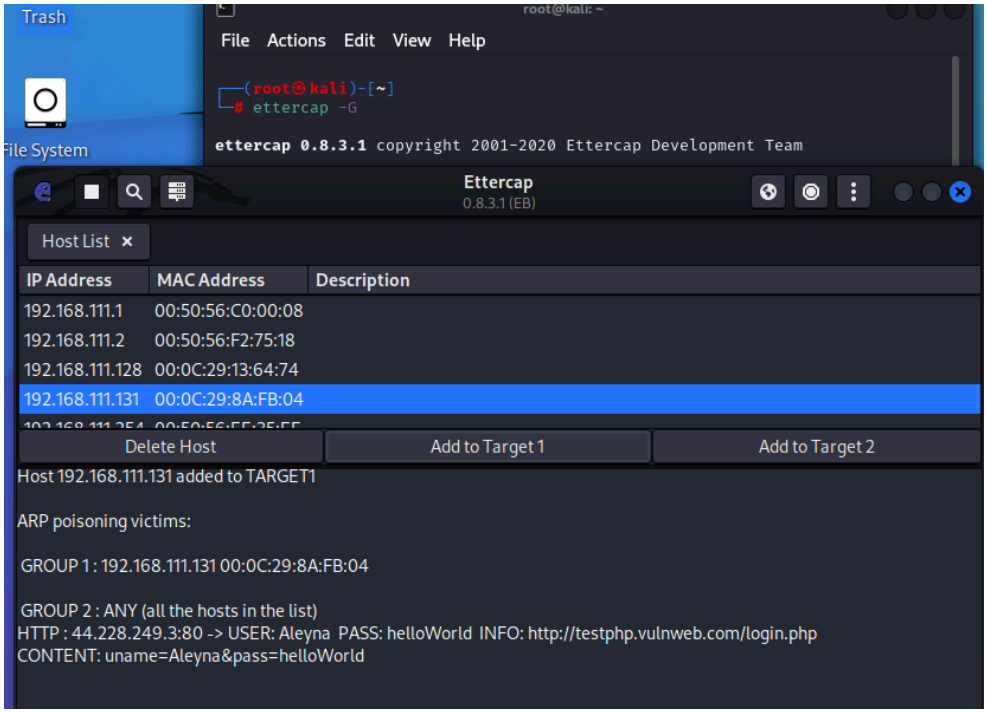
Here, we have once again used Bob's machine to restart tcpdump and this time, he is printing the data of each packet and only capturing the telnet protocol. The packets captured from Alice's next command is seen here as well.

```
aleyna@aleyna-VMware-Virtual-Platform:~$ telnet 192.168.111.131
Trying 192.168.111.131...
Connected to 192.168.111.131.
Escape character is '^]'.

Linux 6.8.0-35-generic (bob-VMware-Virtual-Platform) (pts/9)

bob-VMware-Virtual-Platform login: bob
Password:
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.0-35-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

40 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

bob@bob-VMware-Virtual-Platform:~$
```

6. Here we are using telnet from Alice's machine to login as Bob on her VM.

Task 3:

Steps

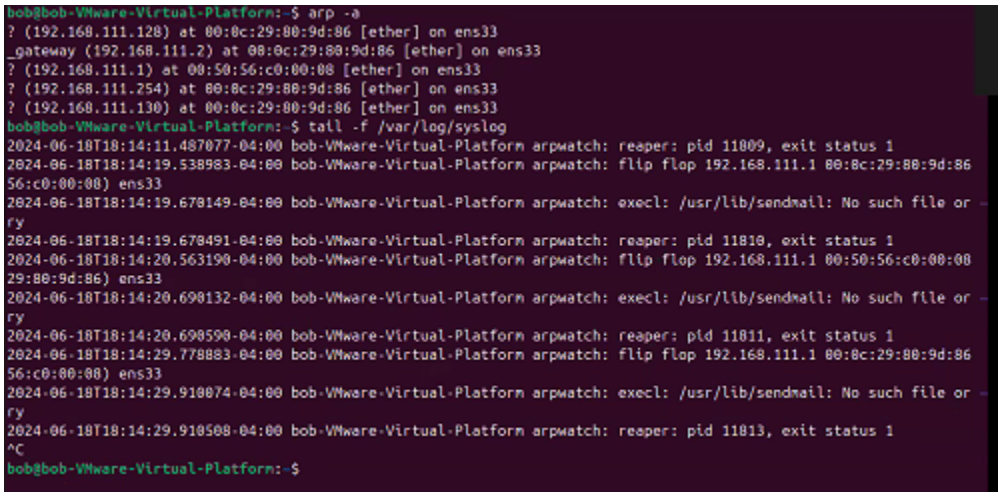


1. Here, Eve has launched an ARP poisoning attack on Bob's machine from Alice's machine. To do this, I have logged into Bob's machine through Alice's VM. By using

telnet in the last task, I now have access to Bob through Alice. In Ettercap on Eve's machine, I have selected Bob's IP address as my target host and began the ARP poisoning attack. From Alice's machine, I visited a website and have logged in using credentials which have been captured by Ettercap (USER = Aleyna, PASS = helloWorld). Since Alice is logged into Bob, Bob's IP address's activity is being captured through Alice's machine. This screenshot shows the stolen credentials from the website on Alice's machine through the target of Bob's IP address.

Task 4:

Steps

1. 

Here, arpwatch is installed on Bob's VM. By using the last attack through Ettercap, the ARP attack can be detected through arpwatch. Through the commands inputted in the terminal, the ARP cache table shows that multiple different IP addresses are mapped to identical MAC addresses, insinuating the threat of an ARP spoofing attack. From the command of "tail -f /var/log/syslog", we can see the activity through arpwatch where we see multiple "flip flop" attributes. These show the MAC addresses associated with a certain IP address has been changed. For example, the first instance of this is "flip flop 192.168.111.1 80:8c:29:80:9d:86 56:c0:80:08…", where the IP address 192.168.111.1 being monitored has the associated MAC addresses of both 80:8c:29:80:9d:86 and 56:c0:80:08… where 56:c0:80:08… is a truncated address. Through these outputs, we can see that arpwatch has detected the arp poisoning attack from Eve's VM.