Homework 2 - Information Security (ICS344)

Alfaifi, Ammar

1 My environment

In my case I have two real machines. The victim machine is an MacOS and the attacker is an Arch OS machine. All machines are connected to my home wireless LAN. Where the victim IP address is `192.168.0.101`, attacker's IP address `192.168.0.104`, the gateway's IP address `192.168.0.1`.

2 ARP Poisoning

2.1 Normal Operation

For the victim normal operation, I see that any packets going from the its IP address it goes directly to the network gateway, as it supposed to be. See Figure 1

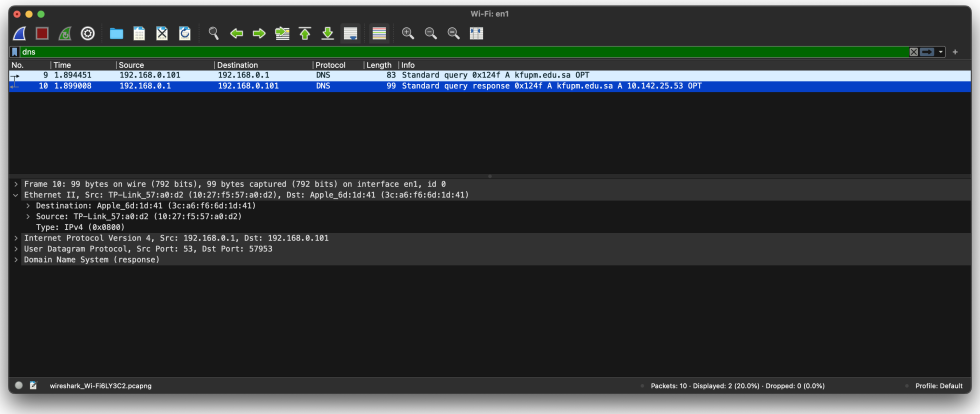

Figure 1: I used `dig kfupm.edu.sa` as test to see where the packet will travell thru. It passes thru the wireless gateway, no MITM exists.

Also, see Figure 2 for the victims's ARP table in normal operation.

```
➜  ~ arp -a
? (192.168.0.1) at 10:27:f5:57:a0:d2 on en1 ifscope [ethernet]
? (192.168.0.100) at 26:86:f6:3b:f9:e7 on en1 ifscope [ethernet]
? (192.168.0.101) at 3c:a6:f6:6d:1d:41 on en1 ifscope permanent [ethernet]
? (192.168.0.102) at 3c:6a:9d:11:51:25 on en1 ifscope [ethernet]
? (192.168.0.103) at f2:3e:7e:84:44:8b on en1 ifscope [ethernet]
? (192.168.0.104) at f4:f:24:1a:13:f1 on en1 ifscope [ethernet]
? (192.168.0.105) at 5e:f:9b:cc:c5:81 on en1 ifscope [ethernet]
```

Figure 2: This is the ARP table for victim's machine in normal operation, notice the gateway IP address as well as that for attacker.

3 Launching Attack

3.1 Get MAC addresses

To start the attack we need the the corresponding MAC addresses of both the network gateway and victime. I'll use `scapy` in interactive mode to send an ARO request to get theier MAC addresses. See Figure 7 for the

commands that I used.

```
>>> arp = Ether(dst=':'.join(['ff']*6)) / ARP(op=1, pdst='192.168.0.101')
>>> res, un = srp(arp)
Begin emission:
Finished sending 1 packets.
..^C
Received 2 packets, got 0 answers, remaining 1 packets
>>> res, un = srp(arp, timeout=2)
Begin emission:
Finished sending 1 packets.
*
Received 1 packets, got 1 answers, remaining 0 packets
>>> res[0][1].hwsrc
'3c:a6:f6:6d:1d:41'
>>> arp = Ether(dst=':'.join(['ff']*6)) / ARP(op=1, pdst='192.168.0.1')
>>> res, un = srp(arp, timeout=2)
Begin emission:
Finished sending 1 packets.
*
Received 1 packets, got 1 answers, remaining 0 packets
>>> res[0][1].hwsrc
'10:27:f5:57:a0:d2'
>>>
```

Figure 3: This is the ARP table for victim's machine in normal operation, notice the gateway IP address as well as that for attacker.

Now for the victim machin: IP address is `192.168.0.101` and MAC is `3c:a6:f6:6d:1d:41`
for the gateway router: IP address is `192.168.0.1` and MAC is `10:27:f5:57:a0:d2`

3.2 Spoof ARP Table

Note: In ARP layer, hwsrc and hwdst represent MAC address of source and destination respectively, while psrc and pdst represent the IP address of source and destination respectively. Also I run this command to allow port forwarding from the attacker's machine to the corresponding dst machine: `echo 1 > /proc/sys/net/ipv4/ip_forward`
See the commnads to spoof the victim ARP table Figure 4.

4 ARP Table

Let's see the victim's ARP table after attack, in Figure 4.

```
➜  ~ arp -a
? (192.168.0.1) at f4:f:24:1a:13:f1 on en1 ifscope [ethernet]
? (192.168.0.100) at 26:86:f6:3b:f9:e7 on en1 ifscope [ethernet]
? (192.168.0.101) at 3c:a6:f6:6d:1d:41 on en1 ifscope permanent [ethernet]
? (192.168.0.102) at 3c:6a:9d:11:51:25 on en1 ifscope [ethernet]
? (192.168.0.103) at f2:3e:7e:84:44:8b on en1 ifscope [ethernet]
? (192.168.0.104) at f4:f:24:1a:13:f1 on en1 ifscope [ethernet]
```

Figure 4: We can see now in the victim's ARP table the MAC address is the same is that for the attacker machine with an IP `192.168.0.104`.

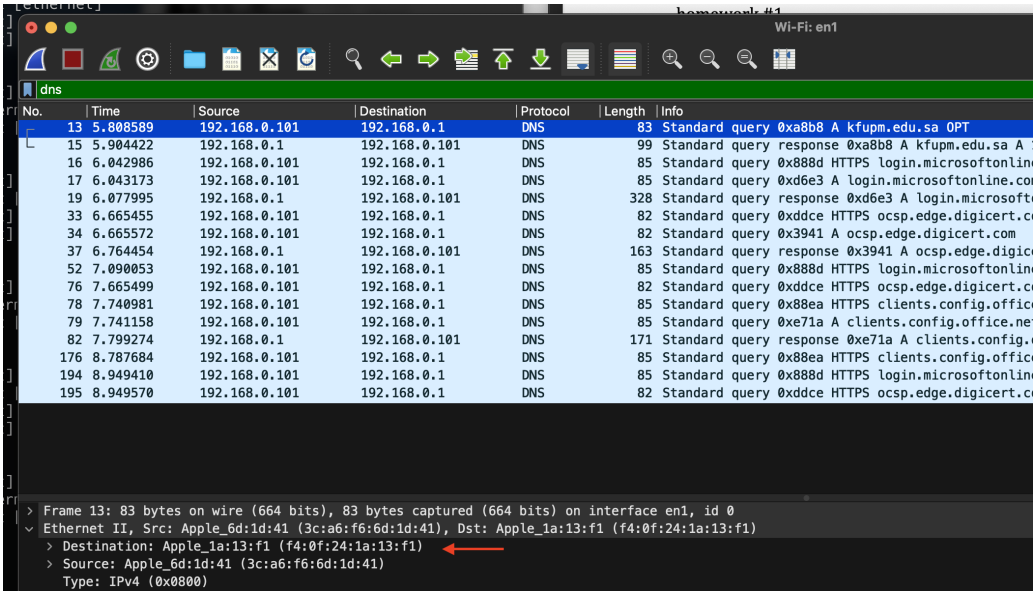

Figure 5: We send a dig request form the victim and in wireshark we see indeed the packet goest to the attacker machine first, MITM.

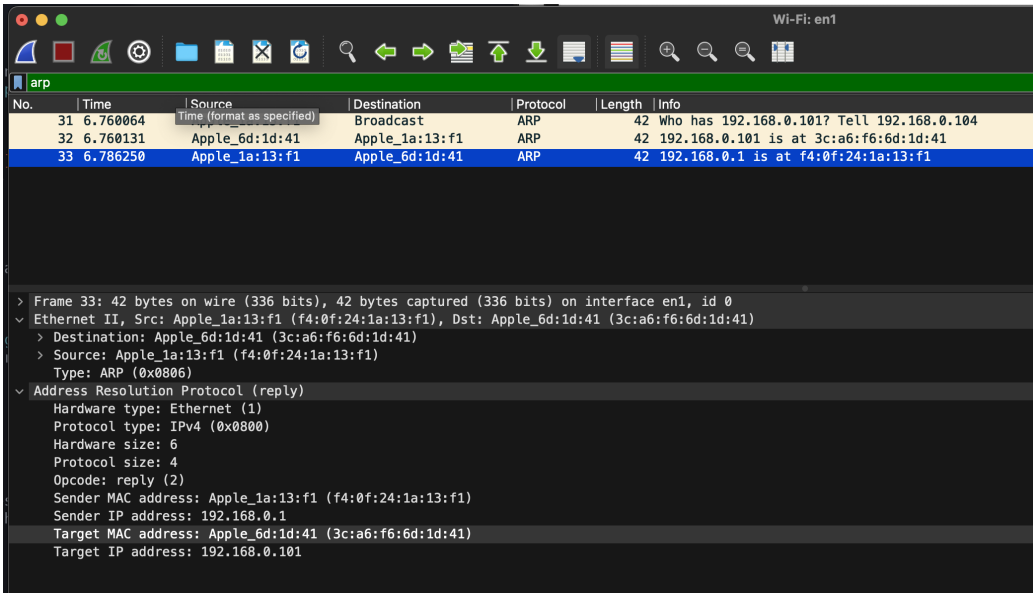

Figure 6: This is the ARP table for victim's machine in normal operation, notice the gateway IP address as well as that for attacker.

```
➜  ~ arp -a
? (192.168.0.1) at 10:27:f5:57:a0:d2 on en1 ifscope [ethernet]
? (192.168.0.100) at 26:86:f6:3b:f9:e7 on en1 ifscope [ethernet]
? (192.168.0.101) at 3c:a6:f6:6d:1d:41 on en1 ifscope permanent [ethernet]
? (192.168.0.102) at 3c:6a:9d:11:51:25 on en1 ifscope [ethernet]
? (192.168.0.103) at f2:3e:7e:84:44:8b on en1 ifscope [ethernet]
? (192.168.0.104) at f4:f:24:1a:13:f1 on en1 ifscope [ethernet]
? (192.168.0.105) at 5e:f:9b:cc:c5:81 on en1 ifscope [ethernet]
```

Figure 7: This is the ARP table for victim's machine in normal operation, notice the gateway IP address as well as that for attacker.