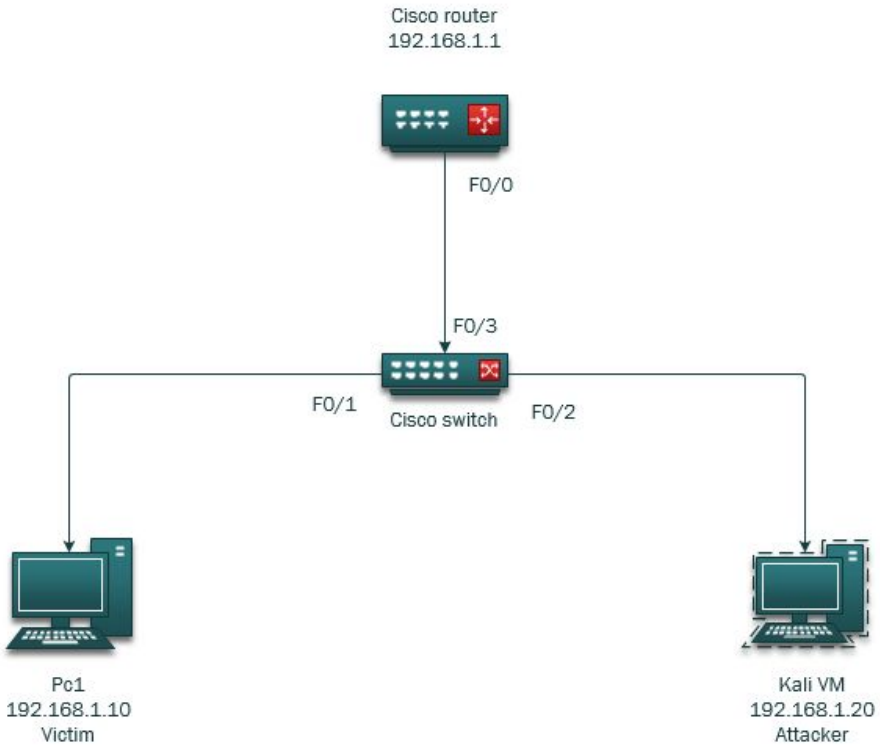
Dynamic ARP Inspection

Overview:

Attack → An ARP spoofing attack(MITM) happens when fake ARP messages are sent over a LAN. The attackers MAC address is then paired with the IP address of a legitimate PC. At this point, the attacker will begin receiving any data that is intended for that IP address. ARP spoofing allows for attackers to intercept, modify and stop data.

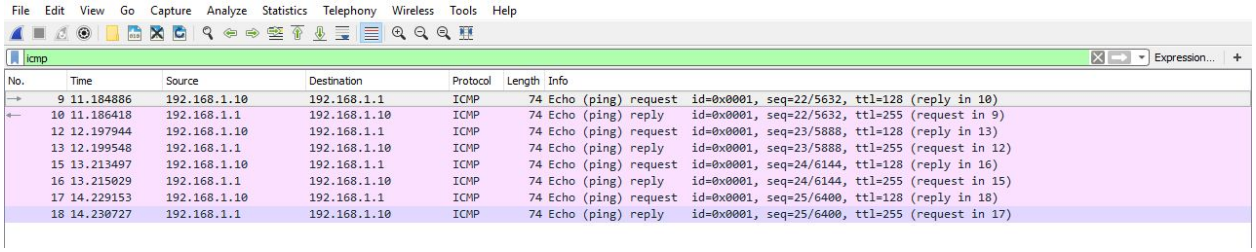
Mitigation → Dynamic ARP inspection (DAI) rejects invalid ARP packets. DAI relies on DHCP snooping because DHCP snooping builds a bindings database with MAC address & IP addresses. The switch will drop any ARP packet if the sender MAC address and sender IP address do not match the corresponding table entry in the DHCP snooping bindings database.

LAB Topology:

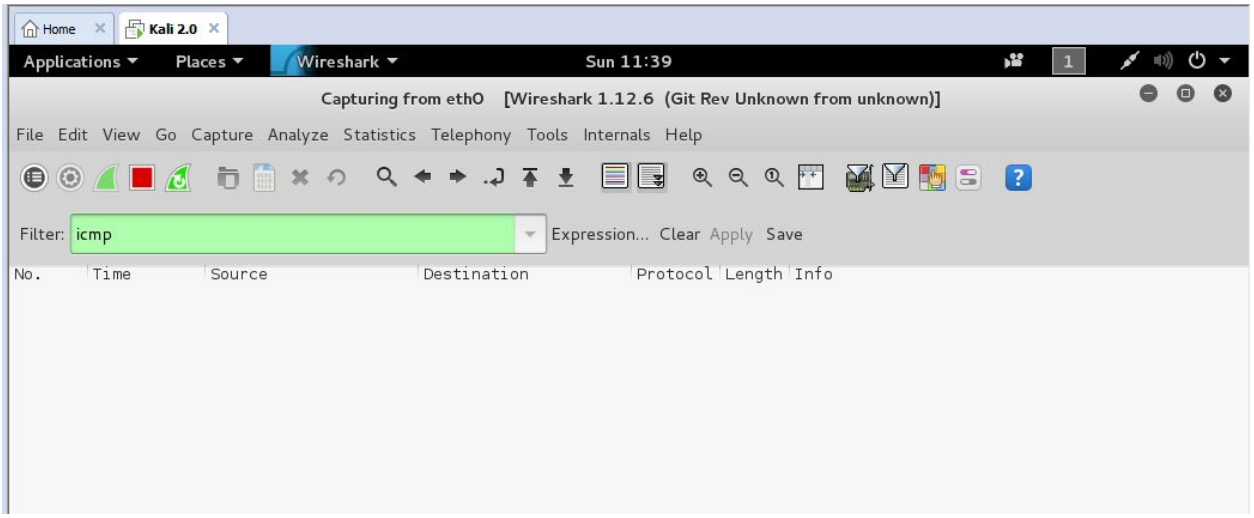


PART 1 : Initial Setup
Non attack network → successful ping from victim pc to default gateway

192.168.1.1	192.168.1.10



Non attack network → no activity on attacker pc after ping from [pc1 → default gateway]

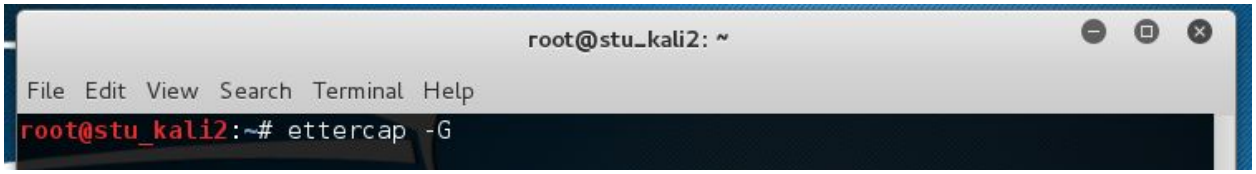


PART 2 : Attack

The basic steps to run exploit:

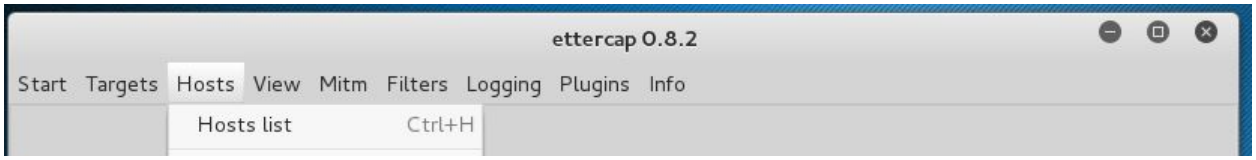
Launch ettercap -G in Kali terminal
Step 1: Click sniff to begin unified sniffing
Step 2: Go to hosts & scan **|** after scan → go to hosts list
Step 3: In hosts list, add victim pc 1.10 to target 2, and add default gateway 1.1 to target 1
Step 4: select arp poisoning & choose sniff remote connections
Results: View Wireshark ARP messages on Victim PC[1.10]
Results: View Wireshark pings between victim and gateway on Attacker VM

Launch ettercap -G in Kali terminal

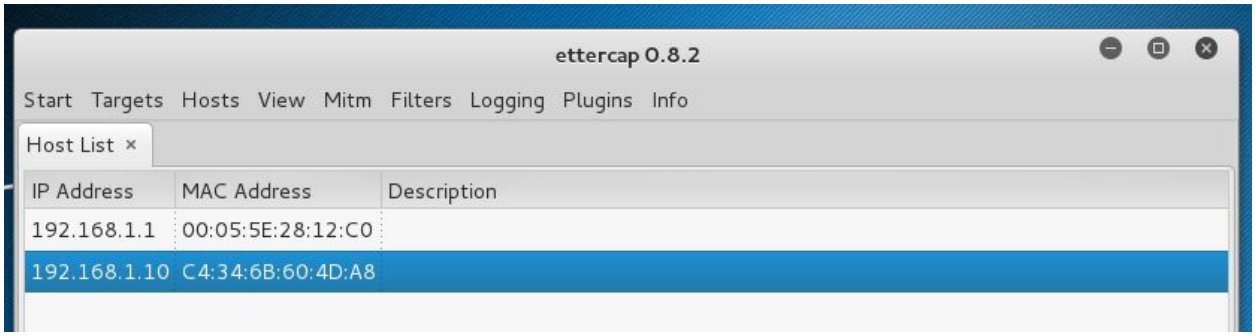


Step 1: Click sniff to begin unified sniffing

Step 2: Go to hosts & scan **|** after scan → go to hosts list



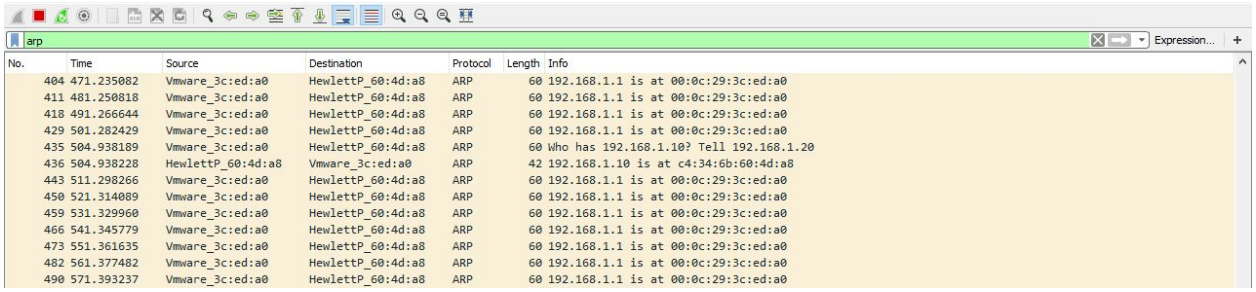
Step 3: In hosts list, add victim pc 1.10 to target 2, and add default gateway 1.1 to target 1



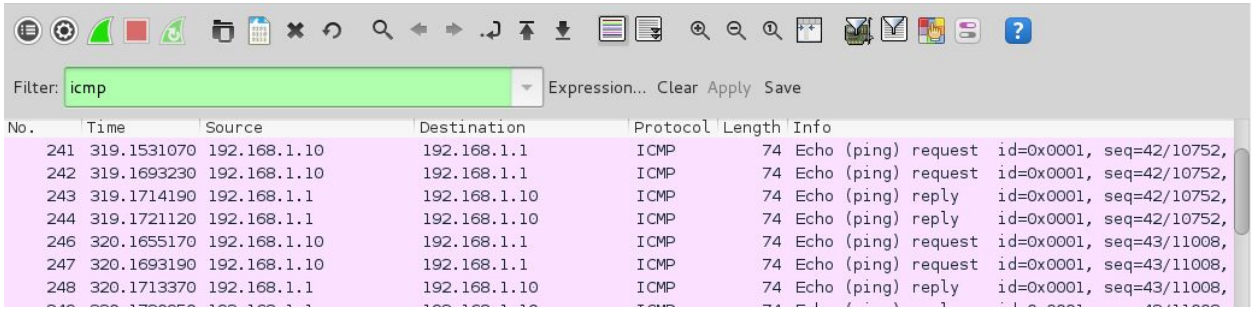
Step 4: select arp poisoning & choose sniff remote connections

Attack Results:

Wireshark capture of victim pc [1.10] showing ARP messages stating:
NOTE: The default gateway is at the MAC Address of the Attacker



Wireshark capture of the Attacker [1.20]
NOTE: Attacker VM received all pings between the victim PC1 [1.10] & the default gateway [1.1]



PART 3 : Attack Mitigation

The basic mitigation steps:

Step 1: Configure switchport security on ports 1-3
Step 2: Configure Dynamic Arp Inspection & DHCP snooping
NOTE: Run Attack again
Results: view Invalid arp spoofing dhcp snooping deny error
Results: view pings from victim to default gateway are no longer successful

Step 1 : Configure switchport security on ports 1-3

```
Switch>en
Switch#
Switch#
Switch#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int range f0/1 - 3
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#switchport port-security
Switch(config-if-range)#switchport port-security max 1
Switch(config-if-range)#sw
*Mar  1 02:54:19.987: %PM-4-ERR_DISABLE: psecure-violation error detected on Fa0/2, putting Fa0/2 in err-disable state
*Mar  1 02:54:19.995: %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address ecb1.d740.d9f9 on port FastEthernet0/2.itch
*Mar  1 02:54:20.991: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down
*Mar  1 02:54:21.995: %LINK-3-UPDOWN: Interface FastEthernet0/2, changed state to down
Switch(config-if-range)#switchport port-security violation restrict
Switch(config-if-range)#exit
Switch(config)#
```

Step 2: Configure Dynamic Arp Inspection & DHCP snooping in order to prevent false mac addresses tied to real IP Addresses from being stored in the victim's table

```
Switch(config)#
Switch(config)#int f0/1
Switch(config-if)#ip arp inspection trust
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#exit
Switch(config)#int f0/3
Switch(config-if)#ip arp in
Switch(config-if)#ip arp inspection
% Incomplete command.

Switch(config-if)#ip arp inspection trust
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#
Switch(config-if)#
```

Mitigation results:
Results after IP ARP inspection & DHCP snooping configs set

Results: While Running ARP Spoofing Attack → Invalid arp spoofing dhcp snooping deny error

```
Switch(config-if)#
*Mar  1 03:44:54.599: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa0/1, vlan 1.([c434.6b60.4da8/192.168.1.10/0005.5e28.12c0/192.168.1.1/03:44:54 U
TC Mon Mar 1 1993])
*Mar  1 03:44:55.599: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa0/1, vlan 1.([c434.6b60.4da8/192.168.1.10/0005.5e28.12c0/192.168.1.1/03:44:55 U
TC Mon Mar 1 1993])
*Mar  1 03:44:56.599: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa0/1, vlan 1.([c434.6b60.4da8/192.168.1.10/0005.5e28.12c0/192.168.1.1/03:44:56 U
TC Mon Mar 1 1993])
*Mar  1 03:44:58.599: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa0/1, vlan 1.([c434.6b60.4da8/192.168.1.10/0000.0000.0000/192.168.1.1/03:44:58 U
TC Mon Mar 1 1993])
*Mar  1 03:44:59.599: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Fa0/1, vlan 1.([c434.6b60.4da8/192.168.1.10/0000.0000.0000/192.168.1.1/03:44:59 U
TC Mon Mar 1 1993])
```

Results: pings from victim PC1 [1.10] to Default gateway[1.1] are no longer successful

```
C:\Users\Student>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.10: Destination host unreachable.
Reply from 192.168.1.10: Destination host unreachable.
Reply from 192.168.1.10: Destination host unreachable.
Reply from 192.168.1.10: Destination host unreachable.
```