

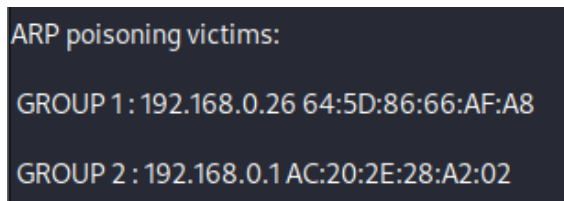
# Extreme Man in the Middle Basics

For this section:

- Router IP is 192.168.0.1
- Poison target IP is 192.168.0.26

How this attack was conducted:

1. Open ettercap-graphical and validate login
2. Ensure the correct primary interface is selected and click the checkmark button
3. Click the 3 vertical dots button, then Targets -> Current Targets
4. On the left side under Target 1, click Add
5. Enter the victim's IP address and click OK
6. On the right side under Target 2, click Add
7. Enter the router's IP address and click OK
8. Click the 3 vertical dots button, then Hosts -> Scan for hosts
9. Click the globe button, then ARP poisoning...
10. Observe the default values, then click OK.

A screenshot of the Ettercap graphical interface showing the 'ARP poisoning victims' window. The window has a dark background with light-colored text. It lists two groups of victims: GROUP 1 with IP 192.168.0.26 and MAC 64:5D:86:66:AF:A8, and GROUP 2 with IP 192.168.0.1 and MAC AC:20:2E:28:A2:02.

```
ARP poisoning victims:
GROUP 1 : 192.168.0.26 64:5D:86:66:AF:A8
GROUP 2 : 192.168.0.1 AC:20:2E:28:A2:02
```

*Figure 1: Beginning ARP Poisoning*

Once these steps are completed you should see the ARP poisoning victims being split into two separate and equally unaware groups.

The tcpdump command used in the following screen shot was:

```
sudo tcpdump -i eth0 src 192.168.0.26
```



```
File Actions Edit View Help
23:24:57.792374 IP 192.168.0.26.64095 > 192.168.0.1.domain: 36194+ A? api.ste
ampowered.com. (38)
23:24:57.792375 IP 192.168.0.26.51285 > 192.168.0.1.domain: 41440+ AAAA? api.
steampowered.com. (38)
23:24:59.799546 IP 192.168.0.26.64095 > 192.168.0.1.domain: 36194+ A? api.ste
ampowered.com. (38)
23:24:59.799546 IP 192.168.0.26.51285 > 192.168.0.1.domain: 41440+ AAAA? api.
steampowered.com. (38)
23:25:00.886726 IP 192.168.0.26.63158 > 192.168.0.1.domain: 3536+ A? test.ste
ampowered.com. (39)
23:25:00.917596 IP 192.168.0.26.63158 > 192.168.0.1.domain: 3536+ A? test.ste
ampowered.com. (39)
23:25:01.928258 IP 192.168.0.26.63158 > 192.168.0.1.domain: 3536+ A? test.ste
ampowered.com. (39)
23:25:03.803433 IP 192.168.0.26.51285 > 192.168.0.1.domain: 41440+ AAAA? api.
steampowered.com. (38)
23:25:03.803433 IP 192.168.0.26.64095 > 192.168.0.1.domain: 36194+ A? api.ste
ampowered.com. (38)
```

Figure 2: Man in the Middle Attack in Progress

If the attack was not successful then there would be no way for us to see the DNS queries from the victim to the router because while ARP is a broadcast DNS is not.

The attack ended here because the victim's internet connection got so slow the victim realized an attack was going on. DDOS was suspected but however incorrect the assumption the damage was already done.

## Dynamic ARP Inspection

The DHCP snooping builds a database mapping IP addresses and MAC addresses. ARP inspection then uses this database to stop arp poisoning before it can even take place.

Insert these lines into your configuration on a compatible Cisco switch to enable ARP inspection.

```
ip dhcp snooping vlan 1
ip dhcp snooping
ip arp inspection vlan 1
!
interface FastEthernet0/3
ip arp inspection trust
ip dhcp snooping trust
```

Sorry for the small font in the pictures I'll try a different format next time. However, if you zoom in everything remains legible.

For this section:

- Router IP is 172.16.102.254
- Poison target IP is 172.16.102.252
- Attacker is connected to interface F0/1

