

# Lab 03- ARP Poisoning and DHCP Security

Matthew Belanger

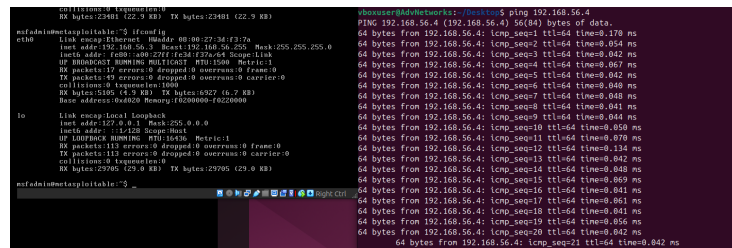
March 4, 2025

# 1 Task 1: ARP Poisoning Attack

## Tasks

- 1.1 Environment Setup: Create a simple network with two virtual machines (VM1 and VM2) connected through a virtual switch or host-only network. Ensure both VMs can ping each other, confirming network connectivity.

See Figure 1



The image shows two terminal windows side-by-side. The left window displays the output of the 'ifconfig' command for the 'eth0' interface, showing IP address 192.168.56.1, netmask 255.255.0.0, and other details. The right window shows the output of a 'ping' command from 192.168.56.1 to 192.168.56.4, displaying successful ping results with 64 bytes of data and various TTL and time values.

Figure 1: VMs Connected

- 1.2 ARP Security Testing: Write a script using Scapy to perform ARP security testing (pentesting), follow the STRIDE methodology we applied in the class to test and verify the identified vulnerabilities.

See code Repo

- 1.3 Mitigation and Report: Discuss and implement basic mitigation strategies against ARP poisoning, such as static ARP entries or using ARP spoofing detection tools.

## Report Requirements

Network configurations and ARP tables before and after the attack.

Before

See Figure 2

```
msfadmin@metasploitable:~$ arp
msfadmin@metasploitable:~$ arp -a
msfadmin@metasploitable:~$ _

vboxuser@AdvNetworks:~/Desktop$ arp -a
? (192.168.56.2) at 08:00:27:d9:bd:42 [ether] on enp0s3
vboxuser@AdvNetworks:~/Desktop$
```

Figure 2: VMs Connected

After

See Figure 3

```
msfadmin@metasploitable:~$ arp
msfadmin@metasploitable:~$ arp -a
msfadmin@metasploitable:~$ _

vboxuser@AdvNetworks:~/Desktop$ arp -a
? (192.168.56.2) at 08:00:27:d9:bd:42 [ether] on enp0s3
vboxuser@AdvNetworks:~/Desktop$
```

Figure 3: VMs Connected

Scapy scripts used.

See code Repo

Screenshots demonstrating the success of the attack, including Wireshark captures.

Discussion on mitigation strategies.

See section 1.3

## 2 Task 2: Security Analysis of The DHCP

2.1 Start Wireshark open the enclosed pcap trace file and list all the DHCP packets in the trace. Use screenshots to support your answer.

See Figure 4

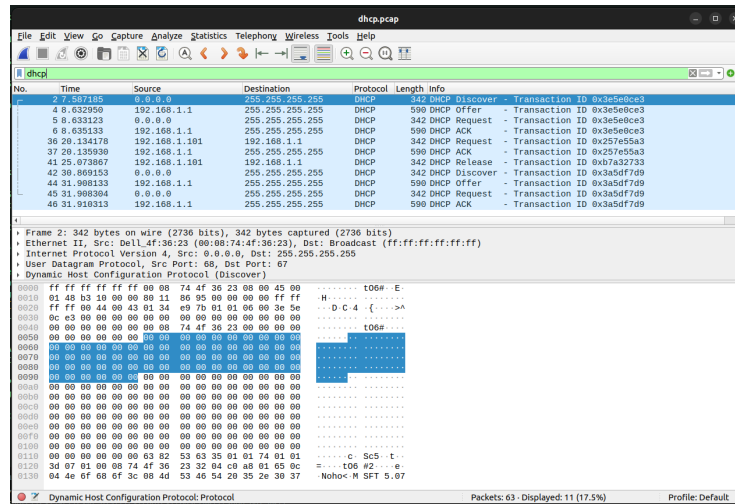


Figure 4: DHCP Packet List

2.2 Create a Finite State Machine model for the DHCP process.

See Figure 5

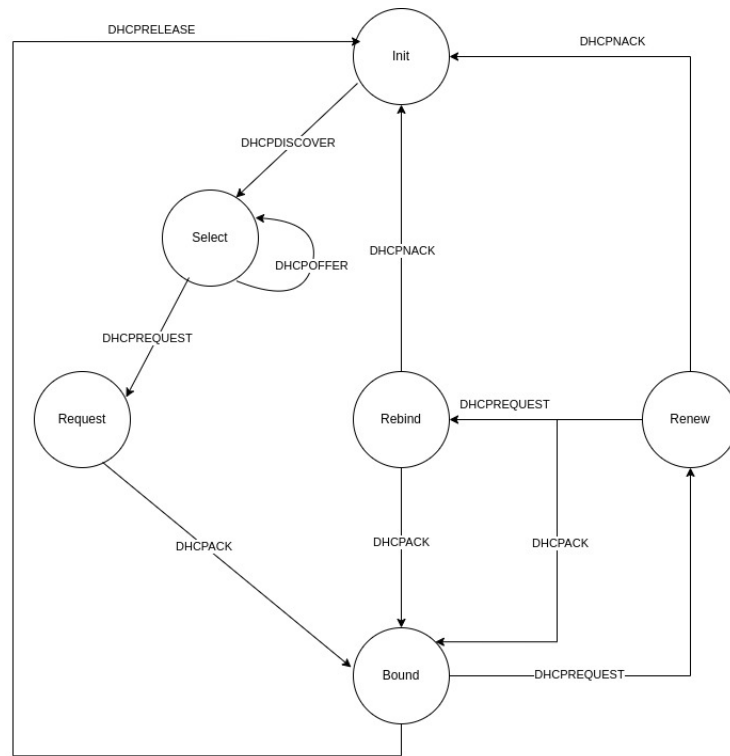


Figure 5: DHCP Finite State Machine

- 2.3 Apply the STRIDE methodology to the FSM model of DHCP to identify potential security threats. For each STRIDE element, identify possible vulnerabilities in the DHCP process.
  - 2.3.1 Spoofing
  - 2.3.2 Tampering
  - 2.3.3 Repudiation
  - 2.3.4 Information Disclosure
  - 2.3.5 Denial of Service
  - 2.3.6 Elevation of Privilege
- 2.4 Propose mitigation strategies for each identified vulnerability. This could involve protocol enhancements, configuration changes, or additional security mechanisms.
  - 2.4.1 Spoofing
  - 2.4.2 Tampering
  - 2.4.3 Repudiation
  - 2.4.4 Information Disclosure
  - 2.4.5 Denial of Service
  - 2.4.6 Elevation of Privilege