Lab 03- ARP Poisoning and DHCP Security

Matthew Belanger

March 4, 2025

1 Task 1: ARP Poisoning Attack

1.1 Network configurations and ARP tables before and after the attack.

1.2 Scapy scripts used.

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

1.4 Discussion on mitigation strategies.

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 1

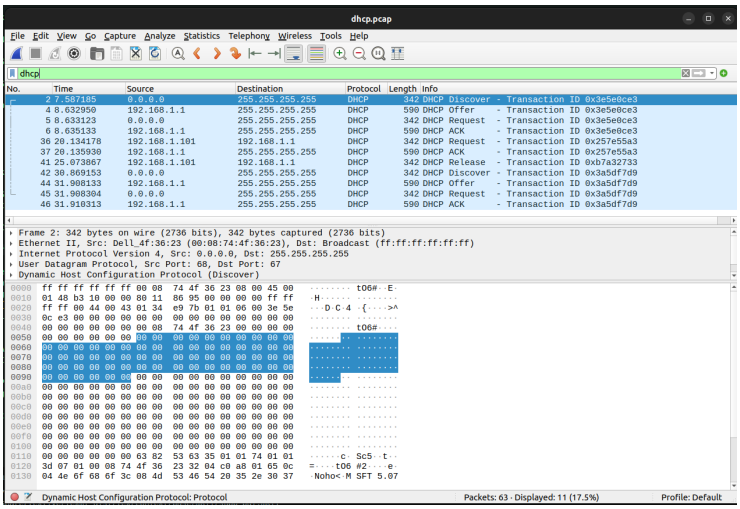

Figure 1: DHCP Packet List

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

See Figure 2

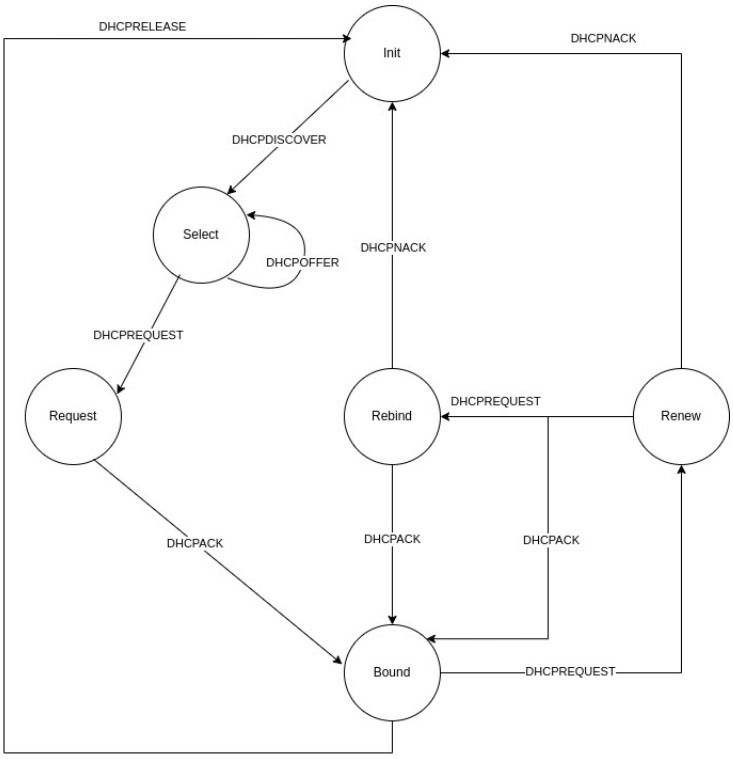

Figure 2: DHCP Finite State Machine

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 enhance- ments, 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