Lab 9: DHCP Security

Instructor: Dr. Maryam R. Aliabadi
Start Date: Nov 20th, 2025
Due Date: Nov 30th, 2025

Lab Overview

This lab introduces the security risks associated with DHCP, a protocol used to automatically assign IP addresses in networks. Students will first configure a baseline DHCP server, then capture traffic, simulate DHCP-based attacks (such as rogue servers and starvation), and finally apply mitigation techniques. By the end, students will gain hands-on experience in securing DHCP environments through monitoring, configuration hardening, and automation.

Learning Objectives

- Understand DHCP operation and vulnerabilities.
- Identify rogue DHCP servers and mitigate attacks.
- Implement DHCP security controls on Linux.
- Monitor and analyze DHCP traffic.
- Safely simulate DHCP attacks in isolated VMs.

Lab Setup

This section prepares your virtual environment and ensures both server and client/attacker VMs have the required packages. Proper setup is critical because DHCP behavior depends on clean network isolation. Use two virtual machines in a Host-Only or NAT network:

- DHCP Server VM
- Client/Attacker VM

Install DHCP server on the server VM:

```
sudo apt update && sudo apt install isc-dhcp-server -y
```

Recommended attacker tools:

```
sudo apt install nmap tcpdump dhcping dnsmasq -y
```

Part A: Baseline DHCP Configuration

This section walks you through setting up a functional DHCP server. Establishing a clean baseline configuration is essential before introducing attacks or security controls.

a. Edit DHCP configuration:

```
sudo nano /etc/dhcp/dhcpd.conf
```

Example subnet configuration:

```
subnet 192.168.56.0 netmask 255.255.255.0 {
    range 192.168.56.100 192.168.56.200;
    option routers 192.168.56.1;
    option domain-name-servers 8.8.8.8, 8.8.4.4;
}
```

b. Restart DHCP service:

```
sudo systemctl restart isc-dhcp-server
sudo systemctl status isc-dhcp-server
```

c. On a client VM, verify DHCP IP assignment:

```
ip a
```

Part B: DHCP baseline Traffic Analysis

This section allows you to observe the normal behavior of DHCP through packet captures. Understanding the baseline traffic is essential for spotting abnormal or malicious DHCP activity.

Capture DHCP traffic:

```
sudo tcpdump -i any '(port 67 or 68)' -vv
```

Observe: DHCPDISCOVER, DHCPOFFER, DHCPREQUEST and DHCPACK.

Part C: Securing DHCP

Now that the baseline is established, you will apply controls that limit who can request IP addresses and who the server accepts. These hardening steps reduce the attack surface for DHCP-based threats.

a. Enable MAC filtering (Example):

```
host trustedclient {
    hardware ethernet 08:00:27:12:34:56;
```

```
    fixed-address 192.168.56.50;
}
```

b. Bind DHCP server to interface:

```
sudo nano /etc/default/isc-dhcp-server
INTERFACESv4="enp0s3"
```

c. Enable logging of DHCP events:

```
journalctl -u isc-dhcp-server -f
```

Part D: Testing Security

In this section, you test how your DHCP server behaves under malicious conditions. You will simulate real attacks like rogue DHCP servers and starvation while analyzing how the legitimate server responds. Common Threats to Observe:

- DHCP Starvation: Exhausting IP addresses.
- Rogue DHCP server: Malicious server giving wrong IP/gateway.
- Packet sniffing: Eavesdropping DHCP assignments.

Your task is to capture DHCP traffic after security attacks and compare to baseline.

1. MAC Filtering Test

Attempt to connect a client not on the allowed list and confirm the following:

- Client should not receive an IP address.
- Logs should show ignored DISCOVER/REQUEST messages.

2. Attacker VM Setup

```
sudo apt install -y nmap tcpdump dhcping dnsmasq
```

3. Simulating Rogue DHCP Server

Edit dnsmasq config:

```
sudo nano /etc/dnsmasq.conf

interface=enp0s3
dhcp-range=192.168.56.120,192.168.56.140,12h
dhcp-option=3,192.168.56.254
dhcp-option=6,8.8.8.8
```

Start rogue server:

```
sudo systemctl restart dnsmasq
sudo systemctl status dnsmasq
```

4. Simulating DHCP Starvation (Safe Mode)

In this step, you will simulate a DHCP starvation attack by generating many fake DHCP requests using randomized MAC addresses. With the default 100-IP DHCP pool, the script will consume many addresses and allow you to observe abnormal server behavior in logs — even if the pool is not fully exhausted. This script must be executed only on the Attacker VM, not on the server.

```
for i in {1..120}; do
  MAC=$(printf '02:11:22:%02x:%02x:%02x
' $RANDOM $RANDOM $RANDOM)
  sudo dhclient -r -v
  sudo dhclient -v -H client$i -cf /dev/null -sf /bin/true -ll /tmp/lease$i
done
```

5. Traffic Monitoring During Attack

On server VM:

```
journalctl -u isc-dhcp-server -f
```

On attacker VM:

```
sudo tcpdump -i any '(port 67 or 68)' -vv
```

Wireshark Filters (Optional)

```
bootp
udp.port == 67 or udp.port == 68
```

Part E: Automation Script

Write a bash script to monitor DHCP logs for anomalies and schedule it with cron to run hourly. (e.g., dhcp_monitor.sh)

Deliverables

- DHCP server configuration files.
- Screenshots/logs showing:
    - Baseline DHCP assignments
    - DHCP traffic capture before and after security attacks
- Automation script and cron job setup.
- Submit your report with the following name format through the Learning Hub.

Filename: Lab9-FirstName-Lastname-StdNo.PDF

Good luck!