Lab Report

## Your Performance

Your Score: 5 of 5 (100%)

Pass Status: Pass

Elapsed Time: 51 minutes 2 seconds

Required Score: 100%

## Task Summary

Required Actions & Questions

✓ On IT-Laptop, launch a DHCP MITM attack using Ettercap

✓ On Support:Show Details

✓ Q1How many DHCP packets were captured in Wireshark?
Your answer: 5
Correct answer: 5

✓ Q2Which gateway addresses are provided in the ACK packets?
Your answer: 192.168.0.5, 192.168.0.46
Correct answer: 192.168.0.5, 192.168.0.46

✓ On Office1:Show Details

## Explanation

In this lab, your task is to complete the following:

- On IT-Laptop, use Ettercap to launch a man-in-the-middle DHCP spoofing attack using the following parameters:
  - Netmask: **255.255.255.0**
  - DNS Server IP: **192.168.0.11**
- On Support, complete the following tasks:
  - Start a capture in Wireshark and filter the display for DHCP traffic.
  - View the IP address and the gateway in Terminal.
  - Bring the network interface down and back up to request a new DHCP address.
  - In Wireshark, how many DHCP packets were exchanged?
  - View the IP address and gateway again. What has changed?
- On Office1, complete the following tasks:
  - Use tracert to rmksupplies.com to find the path. What is the path?
  - Check the IP address of the computer.
  - Release and renew the IP address assigned by DHCP.
  - Check the IP address of the computer again. What has changed?
  - Use tracert to rmksupplies.com to find the path again. What has changed?
  - Login to the rmksupplies.com Employee Portal with the following credentials:
    - Username: **bjackson**
    - Password: **$uper$ecret1**
- On IT-Laptop, find the captured username and password in Ettercap.
- Answer the questions

Complete this lab as follows:

1. On IT-Laptop, start unified sniffing on the enp2s0 interface as follows:
   a. From the Favorites bar, open Ettercap.
   b. Select **Sniff**.
   c. Select **Unified sniffing**.
   d. From the Network Interface drop-down list, select **enp2s0**.
   e. Click **OK**.
   f. Select **Mitm**.
   g. Select **DHCP spoofing**.
   h. In the Netmask field, enter **255.255.255.0**.

   i. In the DNS Server IP field, enter **192.168.0.11**.
   j. Click **OK**.

2. On Support, start a capture that filters for bootp packets as follows:
   a. From top navigation tabs, select **Floor 1 Overview**.
   b. Under Support Office, select **Support**.
   c. From the Favorites bar, open Wireshark.
   d. Under Capture, select **enp2s0**.
   e. Select the **blue fin** to begin a Wireshark capture.
   f. In the Apply a display filter field, type **bootp** and press **Enter**.

3. Request a new IP address as follows:
   a. From the Favorites bar, open Terminal.
   b. At the prompt, type **ip addr show** and press **Enter**.
      The IP address for enp2s0 is 192.168.0.45.
   c. Type **route** and press **Enter**.
      The gateway is 192.168.0.5.
   d. Type **ip link set enp2s0 down** and press **Enter**.
   e. Type **ip link set enp2s0 up** and press **Enter** to bring the interface back up.
   f. Maximize Wireshark for easier viewing.
      In Wireshark, under the Info column, notice that there are two DHCP ACK packets. One is the real acknowledgment (ACK) packet from the DHCP server, and the other is the spoofed ACK packet.
   g. Select the first **DHCP ACK packet** received.
   h. In the middle panel, expand **Bootstrap Protocol (ACK)**.
   i. Expand **Option: (3) Router**.
      Notice the IP address for the router.
   j. Repeat steps 3g-3i for the second ACK packet.
   k. In the top right, select **Answer Questions**.
   l. Answer the questions.
   m. Minimize Wireshark.

4. View the current IP addresses as follows:
   a. In Terminal at the prompt, type **ip addr show** and press **Enter**.
      The IP address is 192.168.0.45.
   b. Type **route** and press **Enter**.
      The current gateway is 192.168.0.46. This is the address of the computer performing the man-in-the-middle attack.

5. On Office1, view the current route and IP address as follows:
   a. From top navigation tabs, select **Floor 1 Overview**.
   b. Under Office 1, select **Office1**.
   c. Right-click **Start** and select **Windows PowerShell (Admin)**.
   d. Type **tracert rmksupplies.com** and press **Enter**.
      Notice that the first hop is 192.168.0.5.
   e. Type **ipconfig /all** and press **Enter** to view the IP address configuration for the computer.
      The configuration for Office1 is as follows:

      - IP address: 192.168.0.33
      - Gateway: 192.168.0.5
      - DHCP server: 192.168.0.14

   f. At the prompt, **ipconfig /release** and press **Enter** to release the currently assigned addresses.
   g. Type **ipconfig /renew** and press **Enter** to request a new IP address from the DHCP server.
      Notice that the default gateway has changed to the attacker's computer which has an IP address of 192.168.0.46.
   h. Type **tracert rmksupplies.com** and press **Enter**.
      Notice that the first hop is now 192.168.0.46 (the address of the attacker's computer).

6. In Chrome, log into the rmksupplies.com employee portal as follows:
   a. From the taskbar, open Chrome.
   b. Maximize the window for easier viewing.
   c. In the URL field, enter **rmksupplies.com** and press **Enter**.
   d. At the bottom of the page, select **Employee Portal**.
   e. In the Username field, enter **bjackson**.
   f. In the Password field, enter **$super$ecret1**.
   g. Select **Login**. You are logged in as Blake Jackson.

7. From IT-Laptop, find the captured username and password in Ettercap as follows:
    a. From top navigation tabs, select **Floor 1 Overview**.
    b. Under IT Administration, select **IT-Laptop**.
    c. Maximize Ettercap.
    d. In Ettercap's bottom pane, find the ***username*** and ***password*** used to log in to the employee portal.
8. In the top right, select **Answer Questions** to end the lab.
9. Select **Score Lab**.