9.6 Lab: Perform a DHCP Spoofing On-Path Attack

Candidate: COMPTIA COMPTIA ()
Time Spent: 01:18

Score: 0%

Task Summary

Required Actions and Questions

✗ On IT-Laptop, launch a DHCP on-path (MITM) attack using Ettercap

✗ On Support: Show Details

✗ *Q1*: What is the IP address of Support's current default gateway?

Your answer:

Correct answer: 192.168.0.5

✗ *Q2*: Which gateway addresses are provided in the DHCP ACK packets?

Your answer:

Correct answer: 192.168.0.5, 192.168.0.46

✗ *Q3*: Which packet contains the spoofed ACK packet?

Your answer:

Correct answer: Packet 4

✗ On Office1: Show Details

Explanation

Complete this lab as follows:

1. From IT-Laptop, start unified sniffing on the enp2s0 interface.
   a. From the Favorites bar, select **Ettercap**.
   b. Select **Sniff** > **Unified sniffing**.
   c. From the Network Interface drop-down list, select **enp2s0**.
   d. Select **OK**.
   e. Select **Mitm** > **DHCP spoofing** and then configure the Server Information as follows:
      - Netmask: **255.255.255.0**.
      - DNS: **192.168.0.11**.

   f. Select **OK**.
2. Find the current default gateway for Support.
   a. From the top left, select **Floor 1 Overview**.
   b. Under Support Office, select **Support**.
   c. From the Favorites bar, select **Terminal**.

   d. Type **route** and press **Enter**.
   e. From the top right, select **Questions**.
   f. Answer Question 1.
   g. Minimize the Lab Questions dialog.

3. Start a Wireshark capture that filters for bootp packets.
   a. From the Favorites bar, select **Wireshark**.
   b. Under Capture, select **enp2s0**.
   c. Select the ***blue fin*** to begin a Wireshark capture.
   d. In the *Apply a display filter* field, type **bootp** and press **Enter**.

4. Request a new IP address from the DHCP server for the enp2s0 interface.
   a. At the terminal prompt:
      - Type **ip link set enp2s0 down** and press **Enter** to bring the interface down.
      - Type **ip link set enp2s0 up** and press **Enter** to bring the interface back up.

   b. Maximize Wireshark for easier viewing.
      In Wireshark, under the *Info* column, notice there are two *DHCP ACK* packets. One is the legitimate acknowledgment (ACK) packet from the DHCP server and the other is the spoofed ACK packet.

5. Determine which DHCP ACK packet is the spoofed packet.
   a. Select one of the ***DHCP ACK*** packets received.
   b. In the middle panel, expand **Bootstrap Protocol (ACK)**.
   c. Expand **Option: (3) Router**.
      Make a note of the IP address used by the router.
   d. Repeat steps 5a-5c for the second ACK packet.
   e. From the top right, select **Questions**.
   f. Answer the Questions 2 and 3.
   g. Minimize Wireshark and the Lab Questions dialog so you can see the terminal window.
   h. At the terminal prompt, type **route** and press **Enter**.
      Notice that the current gateway is now 192.168.0.46.
      This is the address of the computer performing the on-path (man-in-the-middle) attack.

6. On Office1, view the current default gateway and the route to the rmksupplies.com site.
   a. From the top left, select **Floor 1 Overview**.
   b. Under Office 1, select **Office1**.
   c. Right-click **Start** and select **Terminal (Admin)**.
   d. At the PowerShell prompt, type **tracert rmksupplies.com** and press **Enter**.
      Notice that the first hop is 192.168.0.5.
   e. Type **ipconfig** and press **Enter** to view the IP address configuration for the computer.
      The configuration for Office1 is:
      - IP address: 192.168.0.33
      - Default Gateway: 192.168.0.5

   f. At the prompt, type **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).

7. Using Google Chrome, log into the rmksupplies.com Employee Portal.
   a. From the taskbar, select **Google 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** and login using the following:
      - Username: **bjackson**.
      - Password: **$uper$ecret1**.

   e. Select **Login**.
      You are logged in as Blake Jackson.

8. From IT-Laptop, find the captured username and password in Ettercap.
   a. From the top left, 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*.*