Lab Report

Your Performance

Your Score: 6 of 6 (100%) Pass Status: Pass

Elapsed Time: 8 minutes 18 seconds Required Score: 100%

Task Summary

Required Actions

- ✓ Select the enp2s0 interface
- ✓ Set Office1 as a target
- ✓ Set the gateway as a target
- ✓ Launch the MITM Arp poison attack with Sniff Remote Connections
- ✓ Login to RMKSupplies on Office1
- ✓ Hijack the session on Office2

Explanation

In this lab, your task is to hijack a web session as follows:

- On IT-Laptop, use Ettercap to sniff traffic between the employee's computer in Office1 and the gateway.
- Initiate a man-in-the-middle attack to capture the session ID for the employee portal logon.
- On Office1, log in to the employee portal on rmksupplies.com using the following credentials:
  - Username: **bjackson**
  - Password: **$uper$ecret1**
- On IT-Laptop, copy the session ID detected in Ettercap.
- On Office2, navigate to rmksupplies.com and use the cookie editor plug-in in Chrome to inject the session ID cookie.
- Verify that you hijacked the session.

Complete this lab as follows:

1. On IT-Laptop, open Terminal from the sidebar.
2. At the prompt, type **host office1** and press **Enter** to get the IP address of Office1.
3. Type **route** and press **Enter** to get the gateway address.
4. Use Ettercap to sniff traffic between Office1 and the gateway as follows:
   a. From the Favorites bar, open Ettercap.
   b. Maximize the window for easier viewing.
   c. Select **Sniff** > **Unified sniffing**.
   d. From the Network Interface drop-down list, select **enp2s0**.
   e. Click **OK**.
   f. Select **Hosts** > **Scan for hosts**.
   g. Select **Hosts** > **Host list**.
   We want to target information between Office1 (192.168.0.33) and the gateway (192.168.0.5).
   h. Under IP Address, select **192.168.0.5**.
   i. Select **Add to Target 1**.
   j. Select **192.168.0.33**.
   k. Select **Add to Target 2**.
5. Initiate a man-in-the-middle attack as follows:
   a. Select **Mitm** > **ARP poisoning**.
   b. Select **Sniff remote connections**.
   c. Click **OK**. You are ready to capture traffic.
6. On Office1, log in to the employee portal on rmksupplies.com as follows:
   a. From the top navigation tabs, select **Floor 1 Overview**.
   b. Under Office 1, select **Office1**.
   c. From the taskbar, open Chrome.
   d. Maximize the window for easier viewing.

   e. In the URL field, enter **rmksupplies.com**.
   f. Press **Enter**.
   g. At the bottom of the page, select **Employee Portal**.
   h. In the Username field, enter **bjackson**.
   i. In the Password field, enter **$uper$ecret1**.
   j. Click **Login**.
      You are logged into the portal as Blake Jackson.

7. On IT-Laptop, copy the session ID detected in Ettercap as follows:
   a. From the top navigation tabs, select **Floor 1 Overview**.
   b. Under IT Administration, select **IT-Laptop**.
   c. In the Ettercap console, find bjackson's ***username***, ***password***, and ***session cookie*** (.login) captured in Ettercap.
   d. Highlight the **session ID**.
   e. Press **Ctrl** + **C** to copy.

8. On Office2, go to rmksupplies.com and use the cookie editor plug-in to inject the session ID cookie as follows:
   a. From the top navigation tabs, select **Floor 1 Overview**.
   b. Under Office 2, select **Office2**.
   c. From the taskbar, open Chrome.
   d. Maximize the window for easier viewing.
   e. In Chrome's URL field, enter **rmksupplies.com**.
   f. Press **Enter**.
   g. In the top right corner, select **cookie** to open the cookie editor.
   h. At the top, select the plus **+** sign to add a new session cookie.
   i. In the Name field, enter **.login**
   j. In the Value field, press **Ctrl** + **V** to paste in the session cookie you copied from Ettercap.
   k. Make sure **rmksupplies.com** is in the Domain field.
   l. Select the **green check mark** to save the cookie.
   m. Click outside the cookie editor to close the editor.

9. At the bottom of the rkmsupplies page, select **Employee Portal**.
   You are now on Blake Jackson's web session.