Lab Report

Your Performance

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

Elapsed Time: 30 minutes 59 seconds Required Score: 100%

Task Summary

Required Actions

- ✓ Use ssh -X to connect to the remote computer
- ✓ Launch an MITM attack
- ✓ On Exec, release and renew the IP address
- ✓ Inject the session ID into a cookie
- ✓ Hijack the session
- ✓ Login to the rmksupplies Employee Portal

Explanation

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

- On Consult-Lap2, use **ssh -X** to connect to your rogue computer using the following paramenters:
  - IP address: **192.168.0.251**
  - Password: **$uper$neaky**
- Use Ettercap and the following parameters to launch a DHCP spoofing man-in-the-middle attack on your rogue computer and attempt to capture any unsecure passwords:
  - Network Interface: **enp2s0**
  - Netmask: **255.255.255.0**
  - DNS Server IP address: **192.168.0.11**
- On Exec, release and renew the IP address assigned by DHCP.
- Log in to the rmksupplies.com employee portal using the following credentials:
  - Username: **bjackson**
  - Password: **$uper$ecret1**
- On Consult-Lap2, copy the session ID detected in Ettercap.
- On Consult-Lap, go to rmksupplies.com and use the cookie editor plug-in to inject the session ID cookie.
- Verify that you have hijacked the session.

Complete this lab as follows:

1. From Conult-Lap2, connect to your rogue computer as follows:
   a. From the Favorites bar, open Terminal.
   b. At the prompt, type **ssh -X 192.168.0.251** and press **Enter**.
   c. For the password, type **$uper$neaky** and press **Enter**.
   You are now connected to Rogue1.
2. Use Ettercap to launch a DHCP spoofing man-in-the-middle attack as follows:
   a. At the prompt, type **ettercap** and press **Enter** to launch Ettercap remotely.
   Ettercap is running on the remote computer, but you see the screen locally.
   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**.

3. On Exec, release and renew the IP address as follows:
    a. From top navigation tabs, select **Buildings**.
    b. Under Building A, select **Floor 1**.
    c. Under Executive Office, select **Exec**.
    d. Right-click **Start** and select **Windows PowerShell (Admin)**.
    e. Type **ipconfig /release** and press **Enter** to release the currently assigned addresses.
    f. Type **ipconfig /renew** and press **Enter** to request a new IP address from the DHCP server.
4. 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 **$uper$ecret1**.
    g. Select **Login**.
       You are logged in as Blake Jackson.
5. On Consult-Lap2, copy the session ID detected in Ettercap as follows:
    a. From the top navigation tabs, select **Building A**.
    b. Under Red Cell, select **Consult-Lap2**.
    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.
6. On Consult-Lap, 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 **Building A**.
    b. Under Red Cell, select **Consult-Lap**.
    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** appears in the Domain field.
    l. Select the **green check mark** to save the cookie.
    m. Click outside the cookie editor to close the editor.
    n. At the bottom of the rkmsupplies page, select **Employee Portal**.
       You are now on Blake Jackson's web session on your external computer.