9.10 Lab: Analyze DNS Spoofing

Candidate: COMPTIA COMPTIA ()
Time Spent: 00:59

Score: 0%

Task Summary

Required Actions and Questions

✗ Begin unified sniffing on the enp2s0 interface.

✗ Set Exec as the target machine.

✗ Enable DNS spoofing and initiate ARP poisoning

✗ Confirm the redirection to Exec

✗ *Q1*: Which of the following was a result of the DNS spoofing attack?

Your answer:

Correct answer: Queries to the rmksupplies.com site were redirected to the RUS Office Supplies site.

Explanation

Complete this lab as follows:

1. View normal access to the RMK Office Supplies website.
   a. From the Favorites bar of the Linux computer named Support, select **Google Chrome**.
   b. In the URL field, type **rmksupplies.com** and press **Enter**.
   Notice that you are taken to the RMK Office Supplies site.
   c. Close Google Chrome.
2. Use Ettercap to begin 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**.
3. Set Exec (192.168.0.30) as the target machine.
   a. Select **Hosts** > **Scan for hosts**.
   b. Select **Hosts** > **Host list**.
   c. Under IP Address, select **192.168.0.30**.
   d. Select **Add to Target 1** to assign it as the target.
4. Initiate DNS spoofing using an Ettercap plugin.
   a. Select **Plugins** > **Manage the plugins**.
   b. Select the **Plugins** tab.
   c. Double-click **dns_spoof** to activate it.

5. Initiate ARP poisoning on remote connections.
    a. Select **Mitm** > **ARP poisoning**.
    b. Select **Sniff remote connections**.
    c. Select **OK**.
6. From Exec, access rmksupplies.com.
    a. From the top navigation tabs, select **Floor 1 Overview**.
    b. Under Executive Office, select **Exec**.
    c. From the taskbar, select **Google Chrome**.
    d. In the URL field, type **rmksupplies.com** and press **Enter**.
    e. Answer the question.