9.9 Lab: Poison DNS

Candidate: COMPTIA COMPTIA ()
Time Spent: 01:07

Score: 0%

Task Summary

Required Actions

- ✕ Scan for hosts in Ettercap
- ✕ Set Exec as the target machine and initiate DNS spoofing
- ✕ Confirm the redirection to Exec

Explanation

Complete this lab as follows:

1. From the Support computer, use Ettercap to begin sniffing and scanning for hosts.
   a. From the Favorites bar, select **Ettercap**.
   b. Select **Sniff** > **Unified sniffing**.
   c. From the Network Interface drop-down menu, select **enp2s0**.
   d. Select **OK**.
   e. Select **Hosts** >**Scan for hosts**.
2. Configure the Exec computer (192.168.0.30) as the target 1 machine.
   a. Select **Hosts** > **Host list**.
   b. Under IP Address, select **192.168.0.30**.
   c. Select **Add to Target 1** to assign it as the target.
3. Initiate DNS spoofing.
   a. Select **Plugins** > **Manage the plugins**.
   b. Select the **Plugins** tab.
   c. Double-click **dns_spoof** to activate it.
   d. Select **Mitm** > **ARP poisoning**.
   e. Select **Sniff remote connections** and then select **OK**.
4. From the Exec computer, access **rmksupplies.com**.
   a. From the top left, 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 then press **Enter**.
   Notice that the page was redirected to RUS Office Supplies despite the web address staying the same.