Lab Report

Your Performance

Your Score: 5 of 5 (100%) Pass Status: Pass
Elapsed Time: 10 minutes 27 seconds Required Score: 100%

Task Summary

Required Actions & Questions

- ✓ Use Zenmap/nmap to scan ports
- ✓ Started syn flood using Metasploit
- ✓ Filtered for SYN attach using Wireshark
- ✓ Q1What is the source IP address of the SYN flood attack?
  Your answer: 192.168.0.33
  Correct answer: 192.168.0.33
- ✓ Q2Which of the following MAC addresses is initiating the SYN flood attack?
  Your answer: 00:60:98:7F:41:E0 (IT-Laptop)
  Correct answer: 00:60:98:7F:41:E0 (IT-Laptop)

Explanation

In this lab, your task is to perform and monitor a SYN flood attack using the following information:

- Use Zenmap to find the FTP port on CorpServer (192.168.0.10).
- Use Metasploit to send a SYN flood attack as follows:
  - Remote host: **192.168.0.10**
  - Source host: **192.168.0.33**
  - Set the FTP port to match the FTP port used by CorpServer.
- Use Wireshark to capture the SYN flood on the enp2s0 network interface.
- Filter to show only TCP SYN packets.
- Find the MAC address of the computer causing the SYN flood.
- Answer the questions.

Complete this lab as follows:

1. From Zenmap, use nmap to find the FTP port used on CorpServer as follows:
   a. From the Favorites bar, open Zenmap.
   b. In the Command field, type **nmap -p 0-100 192.168.0.10**
   c. Select **Scan**.
   CorpServer is using port 21 for FTP.
   d. Close Zenmap.
2. Use Metasploit to send a SYN flood as follows:
   a. From the Favorites bar, open Metasploit Framework.
   b. At the prompt, type **search synflood** and press **Enter** to find a SYN flood Metasploit module.
   c. Type **use auxiliary/dos/tcp/synflood** and press **Enter** to select the SYN flood module.
   d. Type **show options** and press **Enter** to view the current options for the SYN flood module.
   Notice that RHOST and SHOST are unassigned and RPORT is set to port 80.
   e. Type **set rhost 192.168.0.10** and press **Enter** to set the RHOST address.
   f. Type **set shost 192.168.0.33** and press **Enter** to set the SHOST address.
   g. Type **set rport 21** and press **Enter** to set the FTP port.
   h. Type **show options** and press **Enter** to view the new options for the SYN flood module.
   Notice that RHOST and SHOST have IP addresses assigned and RPORT is set to port 21 matching CorpServer.
3. Capture SYN flood attacks on the CorpServer machine as follows:
   a. From the Favorites bar, open Wireshark.
   b. Under Capture, select **enp2s0**.

c. In the Apply a display filter field, type **host 192.168.0.10 and tcp.flags.syn==1**
d. Press **Enter**.
e. Select the **blue fin** to begin a Wireshark capture.
Notice that no packets are being captured.

4. In Metasploit, type **exploit** and press **Enter** to start a SYN flood.
5. Capture packets for a few seconds.
6. In Wireshark, select the **red box** to stop the Wireshark capture.
Notice the time between each packet sent to host 192.168.1.10. Notice that only SYN packets were captured.
7. In the top right, select **Answer Questions**.
8. Answer question 1.
9. In the middle pane, expand **Ethernet II**.
Notice the source MAC address of the computer sending the SYN flood.
10. Answer question 2.
11. Select **Score Lab**.