Homework 3: Attacks on TCP/IP

- This is an individual assignment and worth 20 points.
- The due date is Saturday, October 1, midnight.
- Please zoom in on the outputs.
- Use the accompanying output document to report your results.
- Follow the naming convention.
- YOU ARE NOT ALLOWED TO DO THIS DURING THE CLASS.

1. Overview

- The objective of this assignment is to perform nmap scans, TCP SYN flooding and reset attacks on a server. Students will complete the assignment on the Labtainer VM environment.
- This learning objective is evaluated by examining the outputs captured in screenshots after performing the tasks.

2. Background

- Install Labtainer VM: https://nps.edu/web/c3o/labtainers
- Labtainer student guide: https://nps.edu/web/c3o/labtainers
- Labtainer overview: https://www.youtube.com/watch?v=24vmrltDasE&t=1021s&ab_channel=CAEinCybersecurityCommunity

3. Tasks

This assignment is based on the **Labtainer tcpip** lab manual.

Task 1. Performing a Ping Sweeping

- Perform a ping sweeping of your network segment using Nmap from the **Attacker**. That is, you are to scan *the entire subnet*. To scan the entire subnet, you need to provide the IP address of the network segment and the subnet mask using CIDR notation. When you scan, *do not use any options*.
- Take a screenshot of the Nmap scan report. The screenshot must include the command you used.

Task 2. Performing a Port Scanning

- Port scanning is an attempt to figure out whether any ports on a host are open and listening.

- Scan open ports on the **Server** from the **Attacker** using nmap.
    - Probe open ports to determine service/version info
    - Enable OS detection
- Add **sudo** before you enter the command whenever the command requires a superuser privilege.
- Take a screenshot of the scan report. The screenshot must include the command you used.

Task 3. Complete Task 1 of the Labtainer tcpip (SYN flooding attack)

- Refer to the following sites to learn how to use **nping** and **netstat**.

  https://nmap.org/book/nping-man.html

  https://linuxhint.com/install-netstat-command-linux/
- For "--source-ip rand", use "--source-ip 192.168.10.10" instead. This is to prevent the use of a public IP address by chance.
- Send the SYN packet *20 times*.
- Add **sudo** before you enter the command whenever the command requires a superuser privilege.
- Display a screenshot of the attacker. You must include the command you used for the attack.
- Display a screenshot of the Wireshark that shows the captured packets.

Task 4. Complete Task 2 of Labtainer tcpip (TCP RST attacks on telnet connections)

- *Skip the ssh part* because the attack is similar.
- There are YouTube videos that explain how to do this.
- Add **sudo** before you enter the command whenever the command requires a superuser privilege.
- The credentials of the server for telnet are: **admin**/**admin**, not ubuntu/ubuntu.
- Display a screenshot of the attacker. You must include the command you used for the attack.
- After the attack, press **enter** on the *client* terminal to get the message "connection close by foreign host".
- Display a screenshot of the client. The screenshot must include the entire screen of the telnet session on the client.

Task 5. Complete Task 3 (TCP session hijacking)—Optional

- The Latainer admin changed the setting of the server. So, some instructions do not work on the new image.
    a. "delete-this.txt" file does not exist. This means you need to create a text file somewhere on the server.
    b. Removed ubuntu account. So, use admin/admin instead.

c. Usage of hexify.py: **sudo python hexify.py "your target text"**

- I have spent several hours to figure out the solution but could not make it work. I found a few Youtube videos that explain how to do this. But the videos are based on the old images and the details do not work.
- If you do this, I'll give you an extra credit of 5 points.
- Display a screenshot of the attacker. You must include the command you used for the attack.
- Display a screenshot of the server. Show that the text file is deleted after the attack.