CS 5153/6053 Network Security, Spring 2023
Project 3: TCP Attacks

Instructor: Dr. Boyang Wang

Due Date: 3/24/2023 (Friday), 11:59pm.
Format: Please submit a zip file of your code in Canvas.
Total Points: 12 points
Note: This is an individual project. The instructor would like to thank Dr. Wenliang Du from Syracuse University for making the project materials of SEED Labs public and free for students to use.

1 Project Description

In this project, you will need to demonstrate several attacks on TCP, including SYN Flooding Attack, TCP Reset Attack and TCP Session Hijacking Attacks by using the project materials offered by SEED Labs [3]. The description of the TCP project offered by SEED Labs can be found at [4]. A copy of the description can also be found in Canvas.

There are several tasks described in the description. **You need to complete Task 1, Task 2 and Task 4** by following the example we discussed in class. The details of each task have been simplified/changed as below.

- For **Task 1**: please use **netwox** to perform SYN flooding on a telnet connection from a user to a server, where SYN cookies is off on the server; You do not need to test the case when SYN cookies is on.
- For **Task 2**: please use **scapy** to perform TCP Reset on a telnet connection from a user to a server. Please use both manual and automated methods to decide the sequence number of a spoofed RST packet as we mentioned in our lectures. You do not need to perform the TCP Reset with netwox or test the case with a ssh connection.
- For **Task 4**: please use **scapy** to perform TCP Hijacking on a telnet connection from a user to a server such that an attacker can print out the content of a secret file (`/home/seed/secret.txt`) from the server; please include your ucid and a fake password as the content of this secret file. You do not need to perform TCP Hijacking with netwox.
- **(Additional Task for CS 6053)**: please complete **Task 5** about reverse shell as well using **scapy**.

As in Project 2, You do not need to write the code from scratch. Most of the code you will need have been discussed during the class and can be found in our slides. Additional information about this project can be found at [4].

To complete the project, you will need to create multiple VMs with Linux (Ubuntu 16.04-32bit) and ensure they are on the same Local Area Networks. You can find the instruction regarding how to install VMs and download a copy of the Linux at this webpage [1]. **Please read this document** [2] from Seed Labs regarding how to setup multiple VMs. You can also find the account name and password for telnet connection on the first page of this document. A copy of this document will be provided in Canvas as well.

Please demonstrate all the attacks on your own VMs only and do not perform these attacks on other people's devices on your Local Area Networks.

2 Basic Requirements

Program Directory: Please name your project folder in the form of `tcp_m123456`, where `tcp` is the name of this project and `m123456` is your UCID. The recommended directories of your program should be organized as follows:

```
./tcp_m123456/src
./tcp_m123456/report.pdf
```

Folder `src` should include all the source files that you have completed. In `report.pdf` file, you should describe

- How do you perform each attack in your VM;
- Please provide a screenshot of each step in each attack similar as the ones we have in our lectures.
- Whether your attack is successful.

References

1. Lab enviroment setup, `https://seedsecuritylabs.org/lab_env.html`
2. Run seed vm on virtualbox, `https://seedsecuritylabs.org/Labs_16.04/Documents/SEEDVM_VirtualBoxManual.pdf`
3. Seed labs (hands-on labs for security education), `https://seedsecuritylabs.org/`
4. Tcp lab, `https://seedsecuritylabs.org/Labs_16.04/Networking/TCP_Attacks/`