ACIT 4630 – Assignment 4 – TCP RST and Session Hijacking Attacks

Please download and unzip assignment4-setup.zip in your SEED VM. Enter the Lab setup folder, and use the docker-compose.yml file to set up the lab environment.

To simplify this assignment, we assume that the attacker and the victim are on the same LAN, i.e., the attacker can observe the TCP traffic between other containers.

Take screenshots of your code snippets and important results and explain what you see.

TCP RST Attack on a telnet Connection

In this attack, you (as the attacker) are going to spoof a RST packet to break an established telnet connection (TCP) between two machines.

Open Wireshark on the VM and select the container network interface.

- telnet from the victim machine to HostB.
- Update the `sniff-spoof-rst.py` code to sniff any telnet packet sent from the victim machine to hostB and immediately send a spoofed RST packet from hostB back to the victim machine to break the connection.
    - **Note:** Don't hard-code any value for the spoofed packet. You should set them all based on the info in the sniffed packet
    - These are the available flag values corresponding to the flag bits on the TCP header: F, S, R, P, A, U
- Run the code on the attacker's machine.
- Type something in the telnet terminal on the victim machine to trigger the sniff-spoof code.

The telnet connection should be reset. Provide screenshots of the RST packet sent in Wireshark as well as changes you made in the code and the commands you ran.

- If you leave the reset code running, can you make a new telnet connection from the victim machine to hostB? Why?
- Which element in the CIA triad is jeopardized in this attack?
- Explain if we will be able to do a Reset attack against an SSH connection
    - Hint: Think about at what layer SSH does encryption

TCP Session Hijacking

In this attack, you are going to hijack a telnet session between hostB and the victim machine and inject some commands into this session.

Open Wireshark on the VM and select the container network interface.

- telnet from the victim machine to hostB.
- Update the `sniff-spoof-hijack.py` code to sniff any telnet packet sent from the victim machine to hostB and send a spoofed packet from the victim machine to hostB to get the telnet server to run an arbitrary command e.g. touch /tmp/success
    - **Note:** Don't hard-code any value for the spoofed packet. You should set them all based on the info in the sniffed packet
    - The ACK bit has to be set in the spoofed packet
- Run the code on the attacker's machine.
- Type a character (without pressing enter) in the telnet terminal on the victim machine to trigger the sniff-spoof code.

Find the spoofed packet in Wireshark.

Verify that the command has been run on hostB and a new file is created.

Note: After a successful attack the telnet session between the victim and hostB freezes because the injected data by the attacker messes up the sequence number.

- Which element in the CIA triad is jeopardized in this attack?

Note: Instead of running a simple command like "touch /tmp/success" on the victim's machine, attackers prefer to have a back door on that machine so they could run multiple commands. Creating a reverse shell (a shell that runs on the victim's machine but gets input from the attacker and shows the output to the attacker) through session hijacking gives hackers such access.

Submission:

Submit your report, with the answers to the questions above, to the Assignment 4 dropbox on the Learning Hub before the Week 11 class.