Lab 6: TCP/IP Network Attacks

SYN Flooding, TCP Reset, and TCP Session Hijack

Due **Sunday** April 2nd

Overview

The learning objective of this lab is for students to gain first-hand experience on vulnerabilities, as well as on attacks against these vulnerabilities. Wise people learn from mistakes. In security education, we study mistakes that lead to software vulnerabilities. Studying mistakes from the past not only help students understand why systems are vulnerable, why a “seemly-benign” mistake can turn into a disaster, and why many security mechanisms are needed. More importantly, it also helps students learn the common patterns of vulnerabilities, so they can avoid making similar mistakes in the future. Moreover, using vulnerabilities as case studies, students can learn the principles of secure design, secure programming, and security testing. The vulnerabilities in the TCP/IP protocols represent a special genre of vulnerabilities in protocol designs and implementations; they provide an invaluable lesson as to why security should be designed in from the beginning, rather than being added as an afterthought. Moreover, studying these vulnerabilities help students understand the challenges of network security and why many network security measures are needed.

Setup

You will utilize docker to emulate users communicating over a network. You will need to `git pull` to pull the most recent changes from the course github. Within the `TCP_attacks` folder, you can find the docker-compose file and the python files for this lab.

Instructions

Lab 6 instructions: https://www.cs.montana.edu/pearsall/classes/spring2023/476/labs/Lab6.pdf

Follow the instructions above and complete the tasks in your SEED Labs VM. Your solutions/output/observations will all be put into a lab report. See the next sections for the lab report.