# CS 5153/5053 Network Security, Spring 2023

## Project 3: TCP Attacks

## Report

### **Student:** Austin Tyler Conn

Link to Source Code <https://github.com/austinc3030/tcp_m11809075>

## Host Environment Used

Operating System: Ubuntu 20.04 LTS



Hardware: Google Cloud E2 Instance

Links Used for Environment Setup:

* [seed-labs/seedvm-cloud.md at master · seed-labs/seed-labs (github.com)](https://github.com/seed-labs/seed-labs/blob/master/manuals/cloud/seedvm-cloud.md)
* [seed-labs/create\_vm\_gcp.md at master · seed-labs/seed-labs (github.com)](https://github.com/seed-labs/seed-labs/blob/master/manuals/cloud/create_vm_gcp.md)

## Docker Information

Text

Description automatically generated

Text

Description automatically generated

## Assumptions

1. Mapping between PDF document and docker containers provided:
   1. Client (10.0.2.5) = user1-10.9.0.6 (10.9.0.6)
   2. Server (10.0.2.6) = victim-10.9.0.5 (10.9.0.5)
   3. Attacker (10.0.2.7) = seed-attacker (10.9.0.1)

## Task 1

### How did you perform the attack in your VM

1. Write code for scapy.

<insert screenshot of code>

1. Check the size of net.ipv4.tcp\_max\_syn\_backlog on the victim/server.

<insert screenshot>

1. Check the usage of the queue on the victim/server.

<insert screenshot>

1. Initiate a telnet session from user1/client to the victim/server.

<insert screenshot>

1. Check netstat on the victim/server to see the new telnet connection.

<insert screenshot>

1. Disable SYN cookies on the victim/server per the assignment instructions (Note: the SEED Lab Docker Image for the victim/server already has SYN cookies disabled.)

<insert screenshot>

1. From the attacker, initiate a SYN attack using code from step 1.

<insert screenshot>

1. Exit telnet session from user1/client.

<insert screenshot>

1. Attempt to initiate a new telnet session from user1/client to the victim/server.

<insert screenshot>

1. Check netstat on the victim/server to see the telnet connections

<insert screenshot>

### Screenshots

### Was the attack successful

## Task 2

### How did you perform the attack in your VM

### Screenshots

### Was the attack successful

## Task 4

### How did you perform the attack in your VM

### Screenshots

### Was the attack successful

## Task 5

### How did you perform the attack in your VM

### Screenshots

### Was the attack successful