# 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: macOS Ventura 13.0.1

Hardware: Apple M1 Mac Mini (ARM Architecture)

Hypervisor: UTM

## Additional Notes

Due to the current state of virtualization on M1 Macs (ARM based), the pre-built virtualbox image provided by SEED Labs was not used. Instead, the instructions to build the virtual machine for the lab provided by SEED Labs were followed and used for the project.

Further, the current state of virtualization on M1 Macs makes running multiple virtual machines in parallel to each other prone to crashing and lockups. All attempts were made to mitigate this, but this is a known limitation of the underlying technology due to the proprietary nature of Apple Silicon and the infancy of support for this processor.

Due to a limitation in the UTM hypervisor, each virtual machine has 2 network interfaces, one is used for outbound internet connectivity and the second interface is used for inter-virtual machine communication.

## Task 1

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

### 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