# CS 5153/5053 Network Security, Spring 2023

## Project 2: Buffer Overflow Attack

## Report

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

Link to Source Code <https://github.com/austinc3030/buffer_m11809075>

## Host Environment Used

Operating System: macOS Ventura 13.0.1

Hardware: Apple M1 Mac Mini (ARM Architecture)

Hypervisor: UTM

## Virtual Machine Environment Used

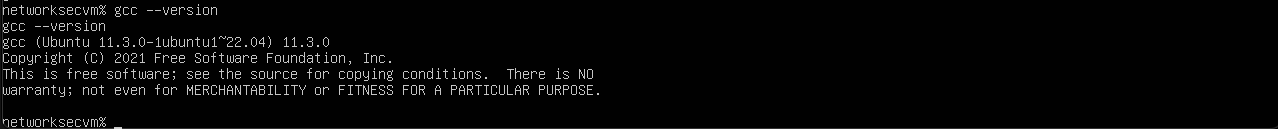
Operating System: Ubuntu Desktop 22.03.2



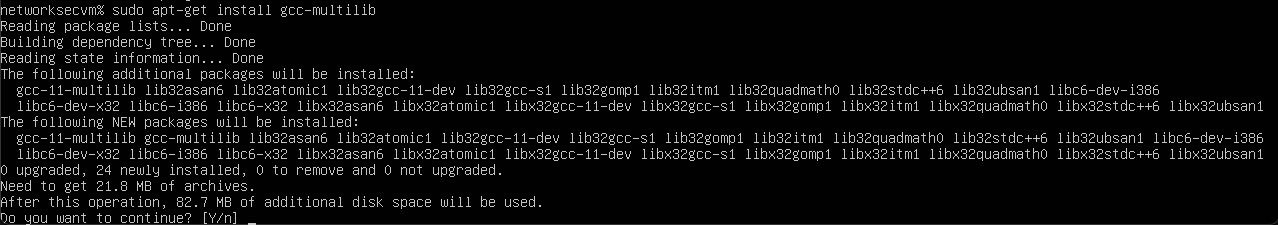
Shell: zsh v5.8.1A black screen with white text

Description automatically generated with low confidence

Gcc:



Caveats:

1. Due to differences between 32/64-bit assembly, the `gcc-multilib` package is required. 
   1. Further, when compiling c code in this environment, the gcc flag `-m32` is required to instruct gcc to compile for a 32-bit architecture.

## How do you perform the attack in your VM

1. Disable address space randomization





## How do you find the value of ebp

1. Compile stack.c with the flags:
   1. `-g` debug flag
   2. `-z execstack` make the stack executable
   3. `-fno-stack-protector` disabled Stack-Guard Protection Scheme

## How do you decide the content of badfile

## Whether your attack is successful