Name: Thomas Hamilton

Major: Cybersecurity

Minor: Criminal Justice

Project Advisor Name: Sean Hayes

Expected Graduation Date: 5/2025

**Problem Statement:**

Ideally, network communications would be completely secure and private. Data would be submitted confidentially and without being altered. However, this is not the case. Individuals attempt to intercept your data to exploit it for personal gain and/or others' detriment. This issue is of utmost importance as it directly affects your personal life. Consider the potential consequences if your bank account details, tax information, or personal messages were compromised. This is the reality we face.

My project is to show people how connecting to an unknown and possibly unsecured network risks them to a MitM (man-in-the-middle) attack. The benefit of this project is that it informs people to be cautious when connecting to unknown WIFI and never enter sensitive information while on those connections. By informing people of the risks of public and unsecured WIFI, they can limit their chances of having sensitive information stolen or changed.

**Project Description:**

My project will be a fake WIFI set up in the Buc stop that will not be password protected and will be left open. The WIFI will be made using pfsense, and it will be just a man in the middle using CSU wireless to connect to the internet. It will scan for people using non-encrypted websites or trying to see if it can store the hash to bypass login and log in without storing any data given to the site. It will show how many people are connected to the WIFI and how many use non-encrypted websites. I will then create a small personal WIFI to make an account on a website, log in while using the MitM router, and attempt to get the username and password from the packet.

**Proposed Implementation Languages**

Python will be the primary coding language used in implementing the MitM attacker due to its versatility and extensive libraries regarding networking.

**Libraries, Packages, Development Kits, etc.**

* Scapy
* PyShark
* Netifaces
* Requests
* OpenSSL

**Additional Software/ Equipment Needed**

* Pfsense Virtual Machine
* Kali Virtual Machine
* Virtualization Software

**Personal Motivations**

I want to do this project because I found my phone trying to connect to open WIFIs in the past before I turned it off. I never realized how dangerous that was until after going to college and studying cybersecurity. If I can show people how dangerous it is for them to allow their phones to do that, then I can help reduce the number of people who have sensitive information leaked online. Also, the best way to learn to stop and detect certain things is to do them yourself. This project will be for both other's benefit and for my learning.

**Outline of Future Research Efforts**

* Launching of both the router and attached machine
* Development of programming scripts
* Integration of Pfsense router Kali machine and Python scripts
* Testing and validation
* Documentation and reporting

**Schedule**

* Summer (2024)
  + Take courses on Python
  + Take courses on Pfsense
* Fall (2024)
  + Week 1-2:
    - Set up virtual machines
    - Download all necessary items in virtual machines
  + Week 3-6:
    - Writing all necessary Python scripts
  + Week 7-8:
    - Implement all code into Pfsense and Kali machines
    - Testing all code in those machines
  + Week 9-10:
    - Run a private network and use fake accounts to show it can grab login information and other data
  + Week 11-12:
    - Setting up WIFI in the Buc stop to see if anyone connects (will try multiple days)
    - Go over collected data
  + Week 13-15:
    - Construct a report and gather all information into a small and concise format
* Spring (2025)
  + Create presentation
  + Practice presentation
  + Prepare for questions
  + Present