Research Report

C00250995 – Matthew Kavanagh

# Abstract

# Table of Contents

[Abstract 1](#_Toc1)

[Table of Contents 1](#_Toc2)

[Introduction 1](#_Toc3)

[Overview of Research 1](#_Toc4)

[Home Networks 1](#_Toc5)

[Nmap 1](#_Toc6)

[Python 1](#_Toc7)

[Summary 2](#_Toc8)

# Introduction

Over the past years there have been great strides made in improving Cybersecurity in multiple areas however the Home Network remains an often overlook aspect. With the rise of Working-From-Home the prospect of an unsecure home network being used to access sensitive corporate devices and information has become a major concern. My 4th Year Cyber Project hopes to improve the Home Network’s security.

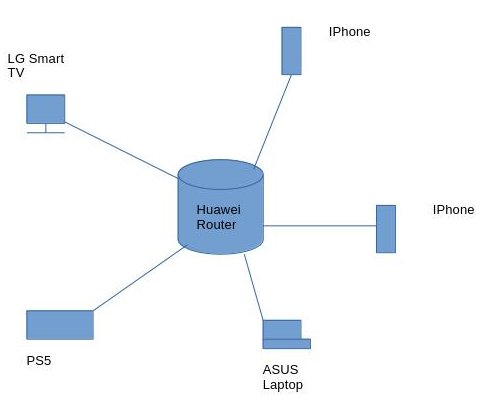
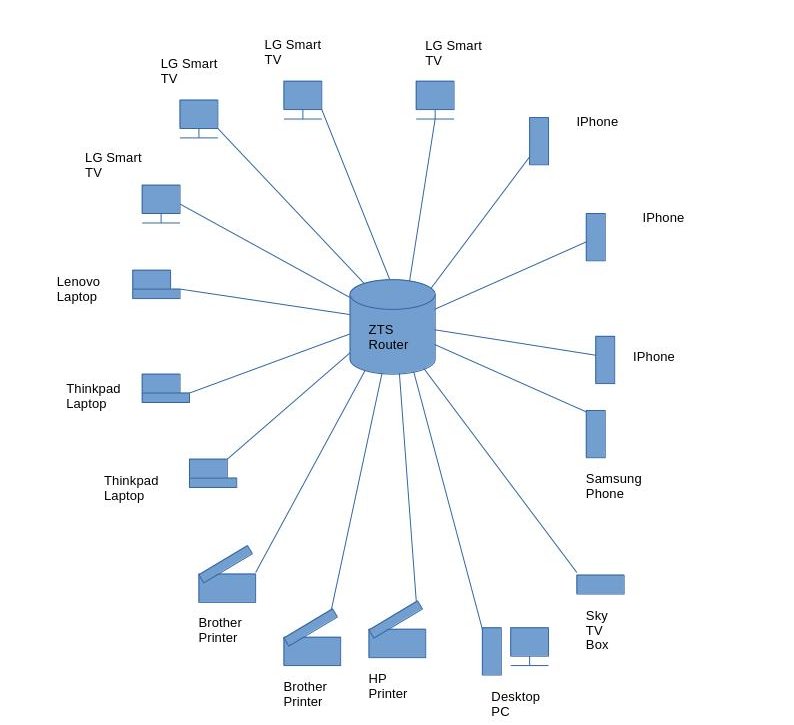
The purpose of this document is to present the research I have taken to help the planning and development of my project.

# Overview of Research

### Home Networks

The first topic of research to tackle is the Home Network. Home Networks can have a multitude of devices present that the Network owner could not even be aware of, this has been exasperated by the internet of things with everything from lights,heating,alarms,appliances like fridges, etc. All these devices present a possible weak link in the network.

To get an example of the average Home Network’s composition I conducted a survey of the devices connect to the network in various homes



### Nmap

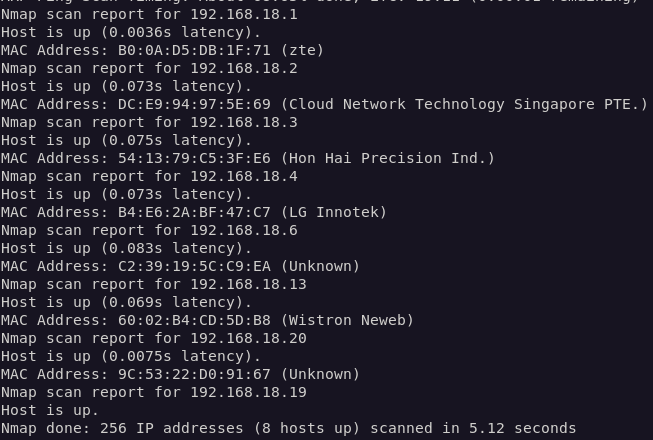
“Nmap (“Network Mapper”) is an open source tool for network exploration and security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. While Nmap is commonly used for security audits, many systems and network administrators find it useful for routine tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.”(Nmap,2023)

As Nmap provides a plethora of functionalities for discovering hosts and services running on a network it is a prime target for use in my project.

The first area of research into Nmap was the commands and arguments used in the CLI version that would be most pertinent to my intended use, in my research I have compiled the following list:

nmap -Oa <filename> : output results as xml, grep and normal file

nmap –sP <target> : Basic ping scan

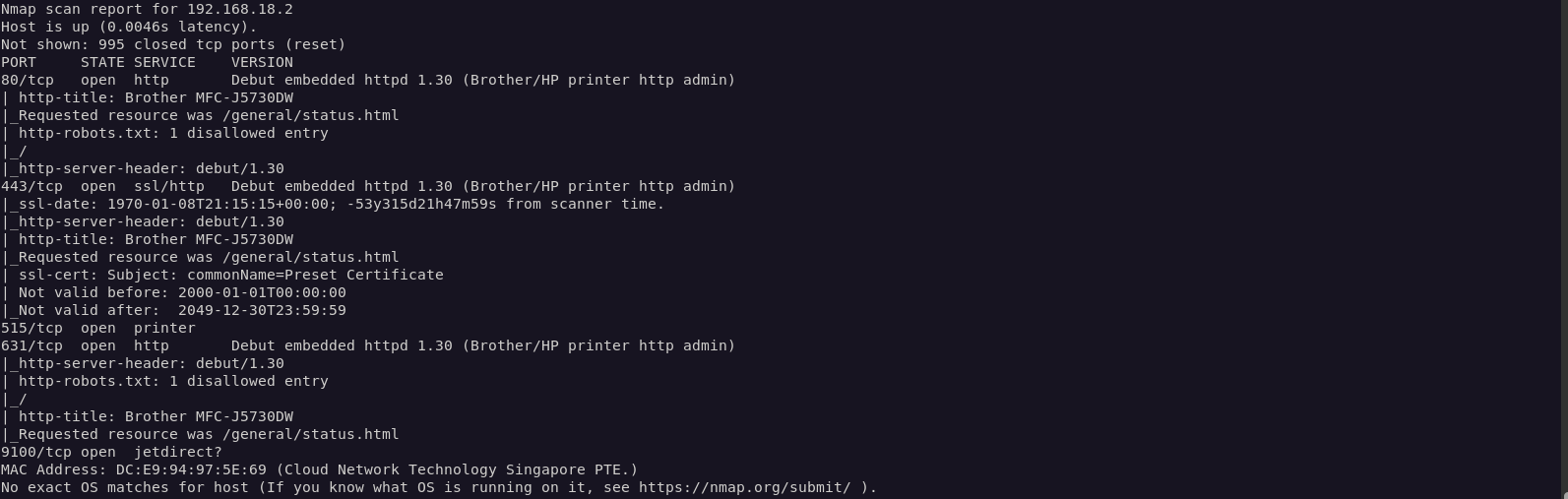


nmap -O -osscan-guess <target> : Scan aggresively for detailed OS info



Nmap —top-ports <number> <target> : Scans for the top <number> most used ports

Nmap –sV –A —version-all <target> : Scan for services, their versions and details



### Python

Due to it’s portability and plethora of third party libraries(including one for nmap integration) Python is a prime choice as a language to write the project software in.

A library that is of major use to the project is python3-nmap which is “A python 3 library which helps in using nmap port scanner. The way this tools works is by defining each nmap command into a python function making it very easy to use sophisticated nmap commands in other python scripts.” (nmapper,2022)

# Summary

# Reference List

Nmap (2023) Nmap Reference Guide, Chapter 15. Available at <https://nmap.org/book/man.html#man-description> (Accessed: 1 December 2023)

nmapper (2022) python3-nmap. Availabe at <https://pypi.org/project/python3-nmap/> (Accessed: 5 December 2023)