Research Report

C00250995 – Matthew Kavanagh

Table of Contents

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 unsecured 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 that has been taken to help the planning, development and execution of the 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 to appliances like fridges and more. 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

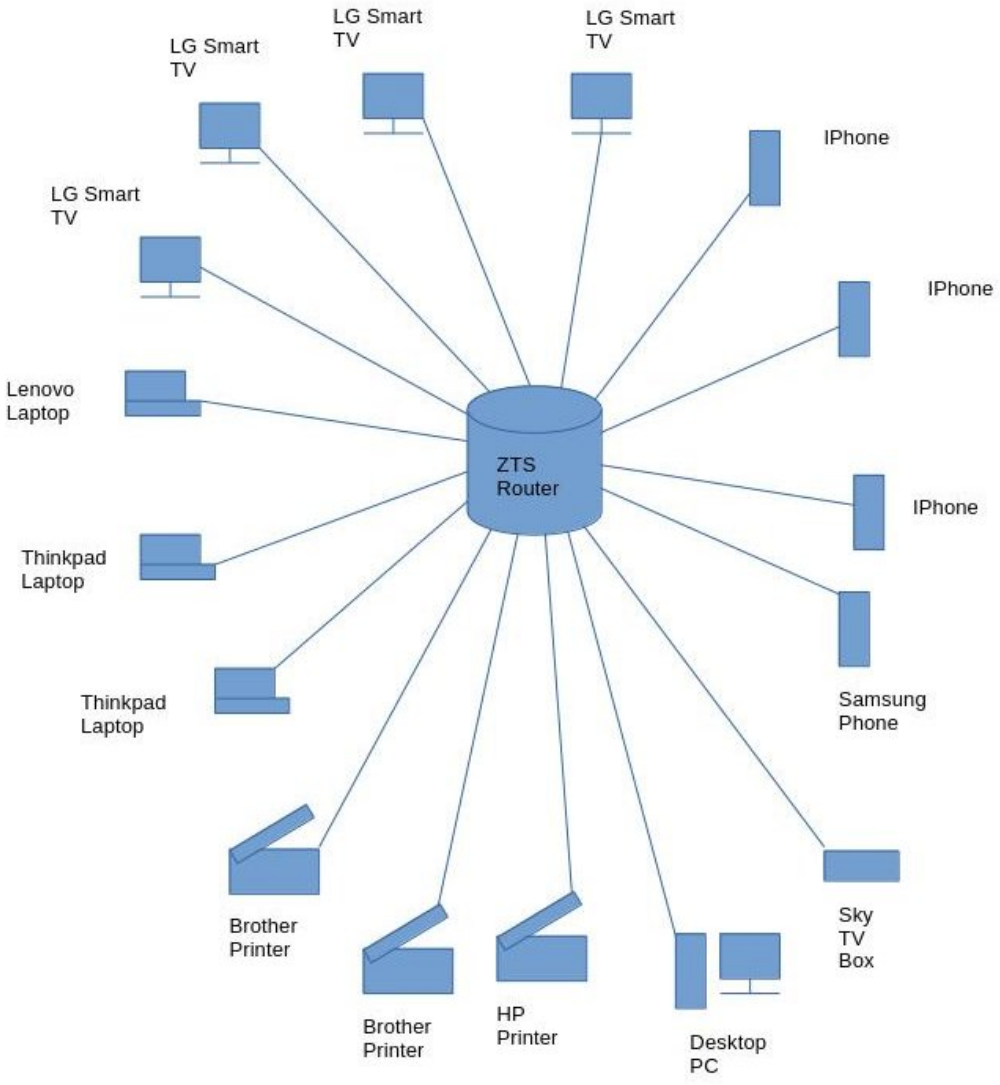

Figure 1 - Diagram of layout of Home Network A

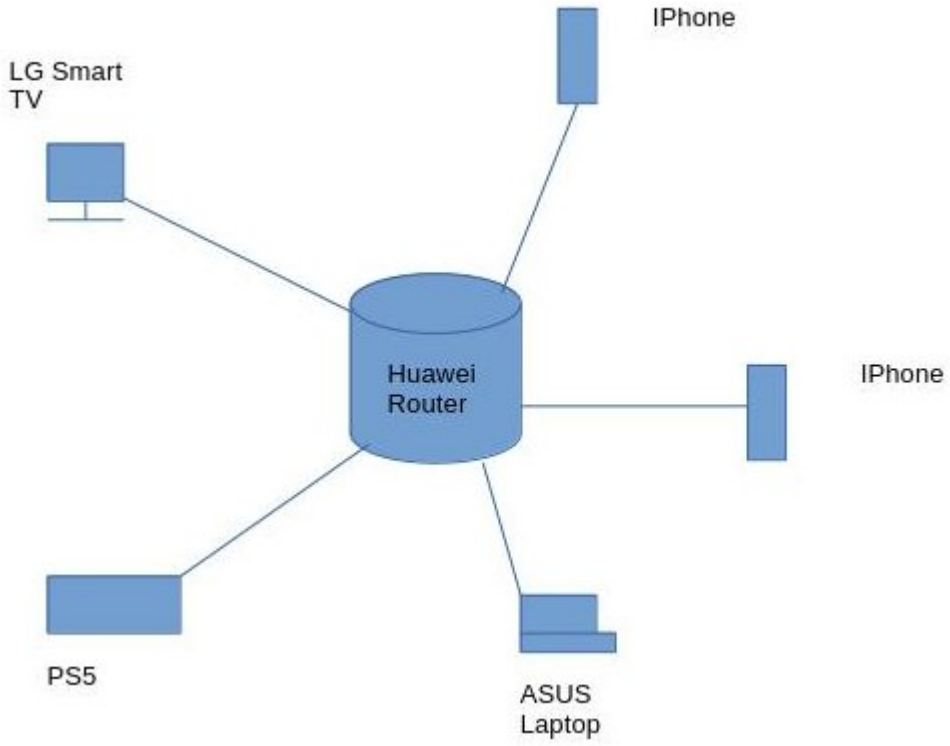

Figure 2 - Diagram of layout of Home Network B

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.”(Gordon Lyon,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 the project.

The first area of research into Nmap was the commands and arguments used in the CLI version that would be most pertinent to the projects intended use, during the course of the research the following list of commands and arguments of note has been compiled:

nmap -Oa <filename> <target>:

Output results as xml, grepable and a normal text file.

nmap –sn <target> :

Basic ping scan that reports active hosts.
Output:

 # Nmap 7.94 scan initiated Thu Dec 7 15:33:21 2023 as: nmap -sn -oA dec7ping 192.168.18.0/24

Nmap scan report for 192.168.18.1

Host is up (0.0029s latency).

Nmap scan report for 192.168.18.3

Host is up (0.075s latency).

Nmap scan report for 192.168.18.4

Host is up (0.086s latency).

Nmap scan report for 192.168.18.6

Host is up (0.0077s latency).

Nmap scan report for 192.168.18.9

Host is up (0.0099s latency).

Nmap scan report for 192.168.18.10

Host is up (0.044s latency).

Nmap scan report for 192.168.18.20

Host is up (0.00011s latency).

 # Nmap done at Thu Dec 7 15:33:26 2023 -- 256 IP addresses (7 hosts up) scanned in 4.17 seconds

As we can see from the output this scan simply pings the target(in this case the entire 192.168.18.0/24 network) and reports if the target is active. While this is a fast and simple scan that can detect most hosts if for whatever reason a host fails to respond to the ping the host will be marked as down.

nmap –sn –PU <target> :

Scan that uses UDP packets to determine if a host is active

Output:

 # Nmap 7.94 scan initiated Thu Dec 7 16:12:45 2023 as: nmap -sn -PU -oA dec7ping 192.168.18.0/24

Nmap scan report for 192.168.18.1

Host is up (0.0018s latency).

MAC Address: B0:0A:D5:DB:1F:71 (zte)

Nmap scan report for 192.168.18.3

Host is up (0.090s latency).

MAC Address: DC:E9:94:97:5E:69 (Cloud Network Technology Singapore PTE.)

Nmap scan report for 192.168.18.5

Host is up (0.090s latency).

MAC Address: 84:3A:4B:8C:01:9C (Intel Corporate)

Nmap scan report for 192.168.18.6

Host is up (0.090s latency).

MAC Address: B4:E6:2A:BF:47:C7 (LG Innotek)

Nmap scan report for 192.168.18.7

Host is up (0.096s latency).

MAC Address: 8A:FB:BF:7F:AB:2A (Unknown)

Nmap scan report for 192.168.18.9

Host is up (0.19s latency).

MAC Address: C2:39:19:5C:C9:EA (Unknown)

Nmap scan report for 192.168.18.13

Host is up (0.086s latency).

MAC Address: 60:02:B4:CD:5D:B8 (Wistron Neweb)

Nmap scan report for 192.168.18.17

Host is up (0.091s latency).

MAC Address: C0:3E:0F:4A:89:BF (SKY UK Limited)

Nmap scan report for 192.168.18.20

Host is up.

 # Nmap done at Thu Dec 7 16:12:49 2023 -- 256 IP addresses (9 hosts up) scanned in 4.03 seconds

Despite being run on the same network the results show that the UDP scan is capable of detecting more hosts than the ping scan alone. The scan attempts to send a UDP packet to a port that is unlikey to be open on a target(by default it targets ports 40 and 125) which results in a port unreachable being sent back, indicating that the host is up.

nmap -O -osscan-guess <target> :

Scan aggresively for detailed OS info
Output:

 # Nmap 7.94 scan initiated Thu Dec 7 14:26:03 2023 as: nmap -O -osscan-guess -oA dec7ping 192.168.18.1

Nmap scan report for 192.168.18.1

Host is up (0.0020s latency).

Not shown: 997 closed tcp ports (reset)

PORT   STATE SERVICE

53/tcp open domain

80/tcp open http

443/tcp open https

MAC Address: B0:0A:D5:DB:1F:71 (zte)

Device type: WAP

Running: Linux 3.X|4.X

OS CPE: cpe:/o:linux:linux_kernel:3.18 cpe:/o:linux:linux_kernel:4.1

OS details: OpenWrt Chaos Calmer 15.05 (Linux 3.18) or Designated Driver (Linux 4.1 or 4.4)

Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .

 # Nmap done at Thu Dec 7 14:26:43 2023 -- 1 IP address (1 host up) scanned in 39.70 seconds

As the results show this option attempts a set of scans to gather information on the targeted device's operating system. While this scan is usually accurate it can sometimes give false positives or have to guess the OS running on the device.

nmap —top-ports <number> <target> :

Scans for the top <number> most used ports
Output:

 # Nmap 7.94 scan initiated Thu Dec 7 14:42:34 2023 as: nmap --top-ports 5 -oA dec7ping 192.168.18.6

Nmap scan report for 192.168.18.6

Host is up (0.078s latency).

PORT   STATE SERVICE

21/tcp closed ftp

22/tcp closed ssh

23/tcp closed telnet

80/tcp closed http

443/tcp closed https

MAC Address: B4:E6:2A:BF:47:C7 (LG Innotek)

 # Nmap done at Thu Dec 7 14:42:34 2023 -- 1 IP address (1 host up) scanned in 0.32 seconds

The —top-ports argument can be used for a quick scan to find if popular services such as SSH or HTTP are running on a device.

nmap –sV –A —version-all <target> :

Scan for services, their versions and details
Output:

 # Nmap 7.94 scan initiated Thu Dec 7 16:46:49 2023 as: nmap -sV -A --version-all -oA dec7ping 192.168.18.3

Nmap scan report for 192.168.18.3

Host is up (0.0035s latency).

Not shown: 995 closed tcp ports (conn-refused)

PORT STATE SERVICE VERSION

80/tcp open http Debut embedded httpd 1.30 (Brother/HP printer http admin)

| http-robots.txt: 1 disallowed entry

|_/

| http-title: Brother MFC-J5730DW

|_Requested resource was /general/status.html

|_http-server-header: debut/1.30

443/tcp open ssl/http Debut embedded httpd 1.30 (Brother/HP printer http admin)

|_http-server-header: debut/1.30

| ssl-cert: Subject: commonName=Preset Certificate

| Not valid before: 2000-01-01T00:00:00

|_Not valid after: 2049-12-30T23:59:59

|_ssl-date: 1970-01-01T09:17:01+00:00; -53y340d07h30m28s from scanner time.

515/tcp open printer

631/tcp open http Debut embedded httpd 1.30 (Brother/HP printer http admin)

| http-title: Brother MFC-J5730DW

|_Requested resource was /general/status.html

| http-robots.txt: 1 disallowed entry

|_/

|_http-server-header: debut/1.30

9100/tcp open jetdirect?

Service Info: Device: printer

Host script results:

|_clock-skew: -19698d07h30m28s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

 # Nmap done at Thu Dec 7 16:47:29 2023 -- 1 IP address (1 host up) scanned in 40.28 seconds

The “–sV –A —version-all” argument conducts a series of scans to determine what services are running on a target before attempting to determine the versions and additional information about them.

Python

“Python is an interpreted, interactive, object-oriented programming language. It incorporates modules, exceptions, dynamic typing, very high level dynamic data types, and classes. It supports multiple programming paradigms beyond object-oriented programming, such as procedural and functional programming. Python combines remarkable power with very clear syntax. It has interfaces to many system calls and libraries, as well as to various window systems, and is extensible in C or C++. It is also usable as an extension language for applications that need a programmable interface. Finally, Python is portable: it runs on many Unix variants including Linux and macOS, and on Windows.”(Python Software Foundation,2023)

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.

Jupyter Notebook

The Jupyter Notebook format is “a shareable document that combines computer code, plain language descriptions, data, rich visualizations like 3D models, charts, graphs and figures, and interactive controls. A notebook, along with an editor like Jupyter Notebook, provides a fast interactive environment for prototyping and explaining code, exploring and visualizing data, and sharing ideas with others.”(Jupyter Team,2015)

As the format allows for code to be written and tested in small segmented parts, known as cells, it has been used in this project for sandboxing python code before its use in the finished codebase.

python3-nmap

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)

The library allows full use of nmaps capabilities with dedicated functions for the most used commands e.g to carry out the ping scan shown in the previous section the following code may be used:

```
import nmap3,json
nmap = nmap3.NmapScanTechniques()
target = "192.168.18.0/24"
result = nmap.nmap_ping_scan(target)
removeEmptyResult(result)
result = parsePing(result)
result = json.dumps(result,indent=4)
print(result)
```

Note the use of python json library as the python3-nmap library returns its results in the json format for ease of readability and manipulation.

Flask

“Flask is a lightweight WSGI web application framework. It is designed to make getting started quick and easy, with the ability to scale up to complex applications. It began as a simple wrapper around Werkzeug and Jinja and has become one of the most popular Python web application frameworks.”(Pallets Projects,2023)

The flask library will help in the creation of the graphical front end of my project. It provides the necessary framework to create a fully featured and modern web application with the simplicity and ease of use associated with the Python language. A web app frontend for the application is a good consideration as most users will be familiar with the use of webpages.

NVDLib

“NVDlib is a Python library that allows you to interface with the NIST National Vulnerability Database (NVD), pull vulnerabilities (CVEs), and Common Platform Enumeration (CPEs) into easily accessible objects.” (Vehemont,2023)

NVDLib presents the opportunity to automate the checking of vulnerabilities as the CPEs obtained from the scans performed by python3-nmap can be fed into the library to search the database. An important caveat to remember is that the NVD API has rate limit of 5 requests in 30 seconds with the ability to request an API key to increase this to 50 requests.

National Vulnerability Database (NVD)

“The NVD is the U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. The NVD includes databases of security checklist references, security-related software flaws, product names, and impact metrics.” (National Institute of Standards and Technology,2024)

The NVD allows for a the searching of vulnerabilities associated with a Common Platform Enumeration (CPE) which is a scheme for identifying the software running on a systems. This functionality can be useful to my project as if the CPEs of a system can be determined then the NVD can be used to search for vulnerabilities of the software the device is running.

Summary

Altogether the research conducted as described by this document will be a great aid in achieving the end goal of an Home Network Analyzer with a simplistic user interface that can be easy to use and understand. Nmap’s functionalities are second to none in discovering hosts in a network and gathering information on their running software and services which can be analyzed to find any security concerns. Python’s portability will allow the Home Network Analyzser to be run on almost any device in a network. The python3-nmap library can be used for the creation of a python program that can fully implement all of Nmap’s features while the PyQt6 toolkit can provide an uncluttered easy to use interface for the program.

Reference List

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

Python Software Foundation (2023) General Python FAQ. Available at https://docs.python.org/3/faq/general.html#what-is-python (Accessed: 7 December 2023)

Jupyter Team (2015) Jupyter Notebook Documentation. Available at https://jupyter-notebook.readthedocs.io/en/latest/ (Accessed: 7 December 2023)

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

Pallets Projects (2023) Flask. Available at https://pypi.org/project/Flask/ (Accessed 27 February 2024)

Vehemont (2023) NVDLib. Available at https://pypi.org/project/nvdlib/ (Accessed 28 February 2024)

National Institute of Standards and Technology (2024) National Vulnerability Database. Available at https://nvd.nist.gov/ (Accessed 28 February 2024)