NSA Community Gold Standard Technical Guidance:
MANAGEABLE NETWORK PLAN

Milton Perez Home Network

Manageable Network Plan

Version 1.2
12/02/2022

This template is provided as-is, the materials gathered from the "NSA Manageable Network Plan"

VERSION HISTORY

Version #	Implemented By	Revision Date	Approved By	Approval Date	Reason
1.0	Milton Perez	10/10/2022	Milton Perez	10/10/2022	Document Creation
1.1	Milton Perez	11/07/2022	Milton Perez	11/07/2022	Addition to Document
1.2	Milton Perez	12/01/2022	Milton Perez	12/02/2022	Completion of Document

Table of Contents

1 **Overview** 5

2 **Introduction** 6

1.1 PURPOSE 6

1.2 PLANNING OVERVIEW (MILESTONE 1 DOCUMENTATION STRATEGY) 7

1.2.1 Network Description 7

1.2.2 Assumptions and Constraints 7

1.2.3 System Organization (Milestone 2 Network Map & Milestone 1 Network Documentation) 8

1.3 GLOSSARY 13

2 Management Overview 14

2.1 DESCRIPTION OF IMPLEMENTATION 14

2.2 POINTS-OF-CONTACT 14

2.3 MAJOR TASKS (MILESTONE 1 TASK CONSIDERATION DOCUMENTATION) 14

2.4 IMPLEMENTATION SCHEDULE (MILESTONE 1 TASK IMPLEMENTATION DOCUMENTATION) 18

2.5 SECURITY AND PRIVACY (ACCESS CONTROL PROTECTIONS) 18

2.5.1 System Security Features 18

2.5.2 Security Set Up During Implementation (Access Control Protections) 19

2.7 OPEN ISSUES 19

MILESTONE 3: PROTECT YOUR NETWORK (NETWORK ARCHITECTURE) 19

3.1 Overview 19

3.2 Facilities and Network Enclaves 19

3.5 High-Value Network Assets 22

3.6 Choke Points On This Network 23

3.7 Single Points of Failure 23

3.8 Legacy Systems 23

3.9 Plan Document Updates 23

MILESTONE 4: REACH YOU NETWORK (DEVICE ACCESSIBILITY) 24

4.1 Overview 24

4.2.1 Laptop Computers 24

4.2.3 Printers 24

4.2.4 Remote Administration 25

4.2.5 Physical Security 25

4.3 Automating Administration 25

4.4 Administrative Tools 25

4.5 Plan Document Updates 26

MILESTONE 5: CONTROL YOUR NETWORK(USER ACCESS) 26

5.1. User Accounts 26
5.2 Privileged accounts 26
5.3 Least privilege administrative model 26
5.4 Users Installing Software 26
5.5 Expiration Dates On Accounts 27
5.6 Plan Document Updates 27
MILESTONE 6: MANAGE YOUR NETWORK, PART I (PATCH MANAGEMENT) 28
MILESTONE 7: MANAGE YOUR NETWORK, PART II (BASELINE MANAGEMENT) 29
MILESTONE 8: DOCUMENT YOUR NETWORK 31
APPENDIX 32
APPENDIX A: MANAGEABLE NETWORK IMPLEMENTATION PLAN APPROVAL 32
APPENDIX B: REFERENCES 33
APPENDIX C: MILESTONE-1 CHECK-LIST 33
APPENDIX D: MILESTONE-2 CHECK-LIST 34
APPENDIX E: Milestone-3 Check-List 35
APPENDIX F: Milestone-4 Check-List 36
Appendix J: Milestone-5 Checklist.......... 38
Appendix H: Milestone-6 Checklist.......... ……..39
Appendix I: Milestone-7 Checklist.......... 40
Appendix J: Milestone-8 Checklist.......... 41

1 Overview

"The Manageable Network Plan is a series of milestones to take an unmanageable and insecure network and make it manageable, more defensible, and more secure. The Plan is intended to be a long-term solution; implementing the milestones may take a significant amount of resources and time (possibly months or even years). But consider: If your network is not manageable, or only barely manageable, it will be very difficult for you to fully implement *any* security measures. Once your network is manageable, you will be able to consider and implement security measures—and verify their implementation—much more efficiently and effectively. Admins may start shouting, "We have no free time! How can we do all this???" Having a manageable network *increases* your free time; it allows you to be *proactive* instead of *reactive*. And if you do have a huge network, don't take on the whole network at once: consider starting with individual subnets.
Each of the Plan's milestones contains a "To Do" list, and may also contain documentation requirements, points to consider, and ongoing tasks. Ideally, each milestone should be fully implemented before moving on to the next one, although some milestones can be implemented in parallel. If the earlier milestones are already implemented on your network, skip ahead to the first one that is not yet fully implemented. To determine this, each milestone has a checklist. For each question in a milestone's checklist, answer Yes or No; if "No" or only partially implemented, provide an explanation. If you consider the explanation acceptable from a risk management standpoint, check Accepts Risk.[1] If all the questions can be answered Yes or Accepts Risk, the milestone is complete. Document and date your answers to these milestone checklists. If a future network evaluation finds problems on your network, it may indicate that you should no longer accept the risks that you did in some areas, and that changes are needed. (Some checklist questions have suggested metrics that can be used to track progress.)
The Plan provides overall direction, offers suggestions, calls out crucial security tips,[2] and gives references to books, Web resources, and tools.[3] Every network is different, so use the Plan milestone "To Do" lists, documentation requirements, and ongoing tasks as a guide, and generate specific tasking for your network. The points to consider under each milestone may suggest additional tasks for your network. When developing these tasks, be mindful of any security assessment and authorization authorities that you must comply with. Use relevant standards (such as SCAP standards[4]) and community-vetted data models so that you can benefit from others' work, both immediately and in the long term. Be sure each task states *what* is to be done, *who* is to do it, and *when* the task must be completed. Also be sure that your specific tasking does not water down or miss the point of the Plan milestones—that won't help your network become more manageable! " (NSA).

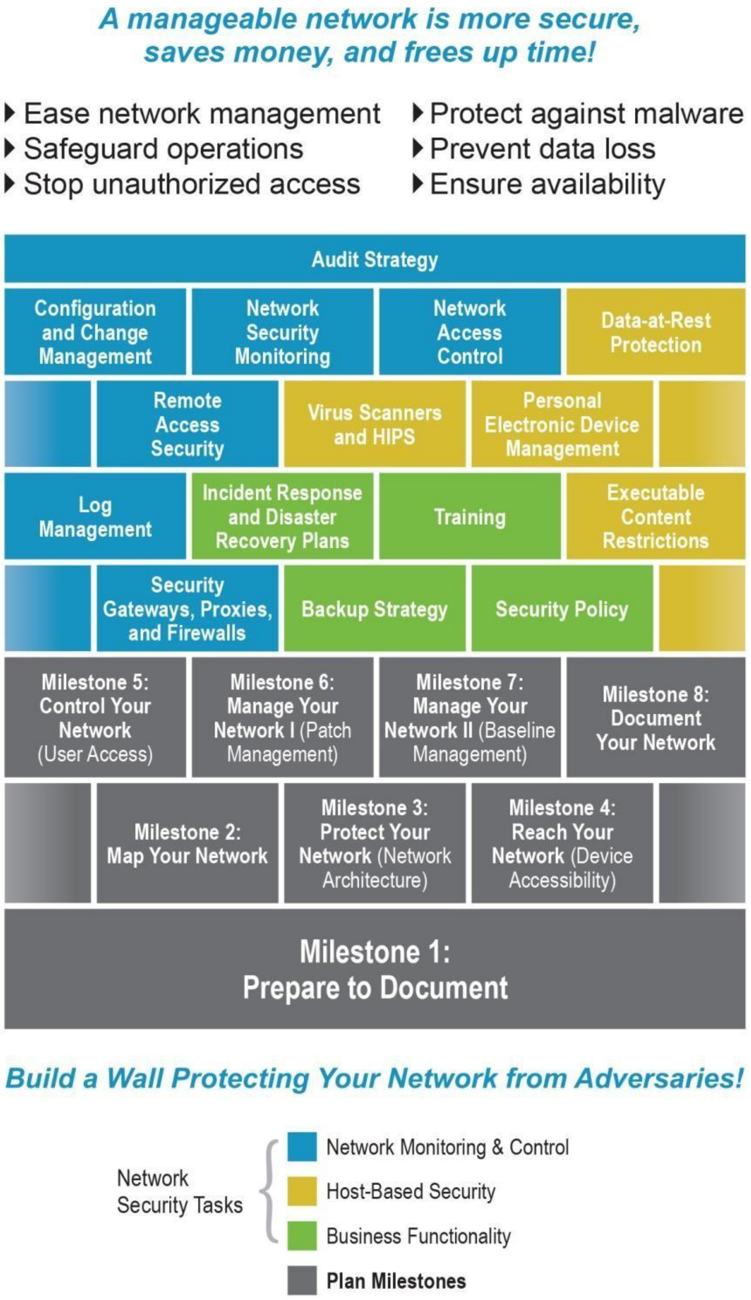

A manageable network is more secure, saves money, and frees up time!
Ease network management
Safeguard operations
Stop unauthorized access
Protect against malware
Prevent data loss
Ensure availability
Audit Strategy
Configuration and Change Management
Network Security Monitoring
Network Access Control
Data-at-Rest Protection
Remote Access Security
Virus Scanners and HIPS
Personal Electronic Device Management
Log Management
Incident Response and Disaster Recovery Plans
Training
Executable Content Restrictions
Security Gateways, Proxies, and Firewalls
Backup Strategy
Security Policy
Milestone 5: Control Your Network (User Access)
Milestone 6: Manage Your Network I (Patch Management)
Milestone 7: Manage Your Network II (Baseline Management)
Milestone 8: Document Your Network
Milestone 2: Map Your Network
Milestone 3: Protect Your Network (Network Architecture)
Milestone 4: Reach Your Network (Device Accessibility)
Milestone 1: Prepare to Document
Build a Wall Protecting Your Network from Adversaries!
Network Security Tasks
Network Monitoring & Control
Host-Based Security
Business Functionality
Plan Milestones

Figure 1: Milestones

2 Introduction

1.1 Purpose

The Purpose of the Home Network Manageable Network Implementation plan is to create documentation about the existing home network, the hardware and software that interacts with it, and understand how to manage, update, secure, and backup the home network.

1.2 Planning Overview (Milestone 1 Documentation Strategy)

This home network was installed by Spectrum and already in production at the time this plan was created. The network did not have any form of diagram or documentation, so this plan will create diagrams of the network and the devices interacting with it, as well as how to better implement the network, ensure security methodology, and install new devices on the network.

Documentation and changes to the network will be in this document, which will be automatically backed up to Milton Perez's OneDrive as revisions are made.
Changes will be documented through revision control listed in this plan. All tasks that are proposed and implemented will be tracked in section 2.4's Implementation Schedule. At the last Friday of each month this document will be hard copied and stored in the end user's safe under his closet for safe keeping.

1.2.1 Network Description

This home network is used by Milton Perez, primarily for schoolwork, web browsing, gaming, and streaming movies. There are two additional family members that use the network at its current state. There are no additional users at time of revision but might be occasional depending on if friends visit the network. The current Nighthawk router utilizes WPA2 key with a trivial password generated by the family.

The home network has endpoints that use wireless or wired ethernet cat6 connectivity.

Operating systems being used by endpoints on the network are:

- Windows 10
- Apple macOS Big Sur
- Apple iOS 15
- Apple iOS 16

The router being used for wireless and wired connections is the Nighthawk R8000.

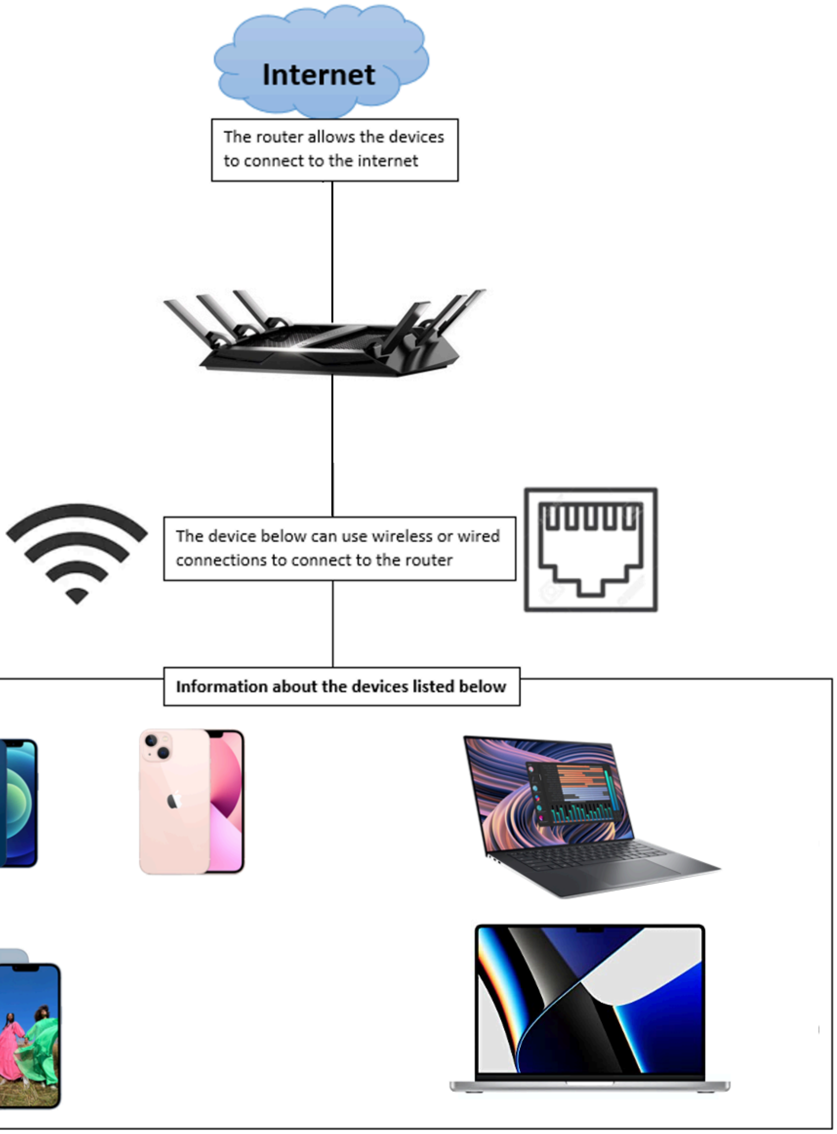
1.2.2 Assumptions and Constraints

- Schedule:
  - The schedule will not have dates of changes and events prior to the creation of this document since the network was created before this plan was
- Budget:
  - This network plan intends to implement and improve the network with the least number of additional purchases or money necessary. Free software will be prioritized in this plan for upgrades and maintenance. Cost/benefit analysis will be conducted on paid software and hardware.
- Resource Availability and manpower:
  - The administrator of the network Milton Perez has access to resources and skill set to operate on the network with general maintenance, network upgrades, and more.
- Software and technology to be used:
  - Software and technology might be reused on multiple devices.

- Limitations with certain interfaces
    - Operating Systems such as TV OS's, Alexa do not have an authentication method so guest access will be provided to all who use these devices.
    - Windows endpoints utilize the capability of logging in as separate users though family/friend's personal windows accounts. No guest accounts are implemented.
    - All mobile devices utilize facial recognition or PIN for unlocking.

1.2.3 System Organization (Milestone 2 Network Map & Milestone 1 Network Documentation)

All network mapping is conducted by utilizing the router's connected device list and verified utilizing NMAP as well as Advanced IP Scanner. This list and graph will be updated as new devices are added or removed from the network. This update will occur weekly every Friday. Plans to automate this update task are being processed.


Internet
The router allows the devices to connect to the internet
The device below can use wireless or wired connections to connect to the router
Information about the devices listed below

Routes to the Netgear R80000 are either Wi-Fi or ethernet.
As devices are end of life and removed from the network they will be removed from this document at the scheduled weekly update interval.

Windows 10 Device Information:

Device	Form Factor	Manufacturer	Model	MAC Address	RAM	OS Version	Assignment	Service Tag
LAPTOP-1	Laptop	Dell	XPS	<MacAddress>*	32 GB	20H2	Milton Perez	XPS-1
Macbook-1	Laptop	Apple	Macbook Pro	<MACAddress>*	128 GB	20H2	Milton Perez	Mac-1

Macbook-2	Laptop	Apple	Macbook Pro	<MACAddress>*	128 GB	20H2	Sister	Mac-1

Phone/Tablet Device Information:

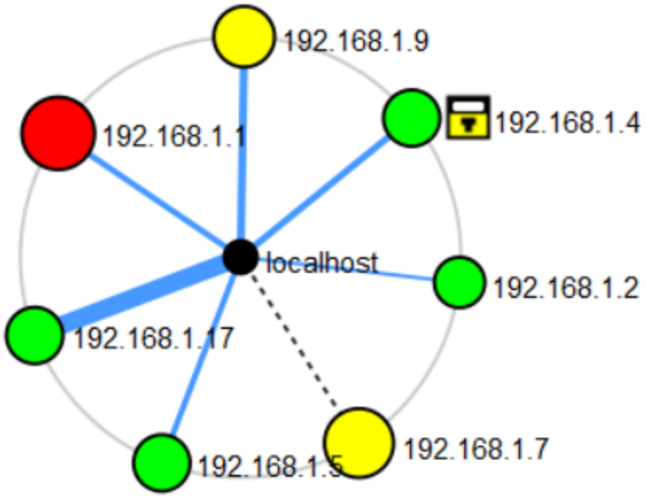
Device	Model	Manufacturer	MAC Address	OS Version	Assignment	Service Tag
iPhone-1	iPhone 12 mini	Apple	<MAC Address>*	iOS 16	Milton Perez	Apple-2
iPhone-3	iPhone 14	Apple	<MAC Address>*	iOS 16	Sister	Apple-3
iPhone-2	Iphone 13	Apple	<MAC Address>*	iOS 15	Mom	Apple-4

*Kept confidential for security purposes

Total Device Count: 7 (including router)

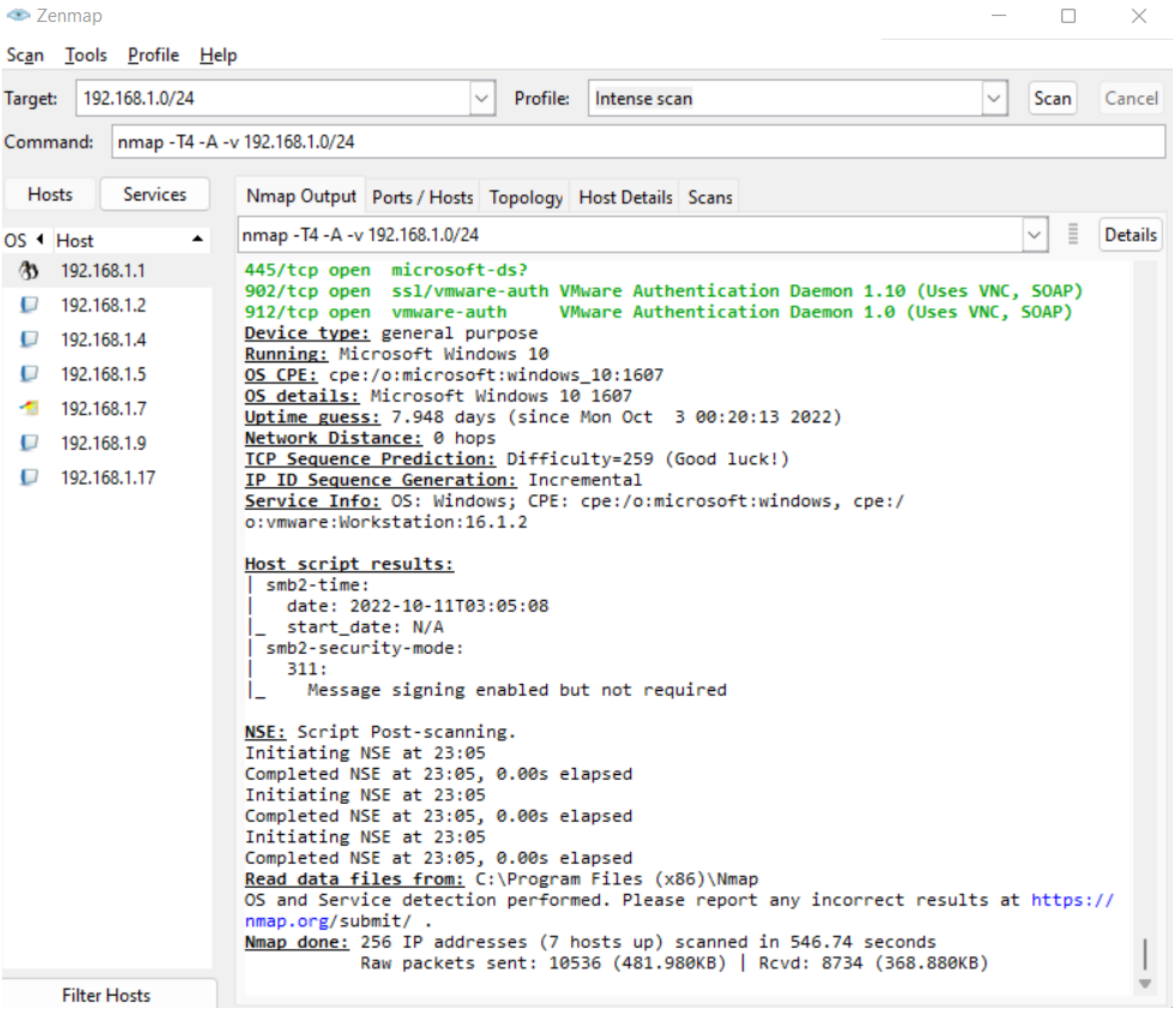
One thing to note is the naming convention of the devices, they are not uniform, and an attacker could simply name their device something similar and it would be hard to recognize. In the future a naming convention scheme will be considered for organizational purposes.

Utilizing an nmap network protocol scan a quick service investigation can be conducted.



Command: nmap -s0 192.168.0.0/24

A summary of the complexity of the network is displayed below:



Target: 192.168.1.0/24 Profile: Intense scan

Command: nmap -T4 -A -v 192.168.1.0/24

192.168.1.1
192.168.1.2
192.168.1.4
192.168.1.5
192.168.1.7
192.168.1.9
192.168.1.17

```
nmap -T4 -A -v 192.168.1.0/24
445/tcp open  microsoft-ds?
902/tcp open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp open  vmware-auth     VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10:1607
OS details: Microsoft Windows 10 1607
Uptime guess: 7.948 days (since Mon Oct  3 00:20:13 2022)
Network Distance: 0 hops
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows, cpe:/
o:vmware:Workstation:16.1.2

Host script results:
| smb2-time:
|   date: 2022-10-11T03:05:08
|_  start_date: N/A
| smb2-security-mode:
|   311:
|_    Message signing enabled but not required

NSE: Script Post-scanning.
Initiating NSE at 23:05
Completed NSE at 23:05, 0.00s elapsed
Initiating NSE at 23:05
Completed NSE at 23:05, 0.00s elapsed
Initiating NSE at 23:05
Completed NSE at 23:05, 0.00s elapsed
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://
nmap.org/submit/ .
Nmap done: 256 IP addresses (7 hosts up) scanned in 546.74 seconds
           Raw packets sent: 10536 (481.980KB) | Rcvd: 8734 (368.880KB)
```

Protocols used: HTTP/HTTPS, TCP/UDP, SMTP, FTP.

Ports used: 21,22,23,53,80,111,135,139, 443, 631,902, 912, 1040,1069, 1166, 1259, 1322, 1500,1700, 1914, 2002, 2065, 2910,3306, 3689, 3878, 5000, 5555, 5718, 5678, 5952, 5959, 5987, 6789, 8011, 8086, 8090, 8093,9103, 10009, 10010,10215, 20005, 24444, 24800, 28201, 44501,49153, 49154, 49159, 62078

Software:

This network uses the internet for educational and recreational purposes. All software listed is installed to windows 10 endpoints and is listed as Bundle-A in the NMAP inventory Table:

- Free
  - Windows Defender
  - Virtual Box
  - Nmap
  - Discord
  - Google Chrome
  - Firefox
  - Safari
- Licensed
  - Microsoft Office 2019
  - VMware Workstation
  - IntelliJ
  - VMWare

In addition to the above software, a development software, Bundle-B is the following: routinely used:

- VMWare
- Wireshark
- Virtual Box
- Nmap
- Microsoft Teams
- Microsoft Office 2019
- Visual Studio Code
- IntelliJ
- Discord

NMAP Inventory

Host	Device	Software	NMAP-Details	NMAP-Ports/Protocols	Description
192.168.1.2	iPhone-1	Bundle A	1 open port	http	Personal Phone
192.168.1.4	Macbook-1	Bundle A	31 open ports	Numerous Unknown TCP ports	Sister’s Macbook
192.168.1.5	iPhone-2	Bundle A	2 open ports	TCP	Sister’s Phone

192.168.1.7	Laptop-1	Bundle A	6 open ports	TCP	Personal Laptop
192.168.1.9	Macbook-2	Bundle A	3 open ports	TCP	Personal Macbook
192.168.1.17	iPhone3	Bundle A	2 open Ports	TCP	Mom's Phone

1.3 Glossary

AP – Access Point: Device that allowed wireless devices to connect to a wired network using Wi-Fi, or related standards. The AP normally connects to a router (via a wired network) as a standalone device.
DHCP - Dynamic Host Configuration Protocol - a network management protocol used on Internet Protocol
GB – Gigabyte – 1000 megabytes IP – Internet Protocol Address – an address of a computer or other network device using TCP/IP.
IDS –Intrusion Detection System–a device or software application that monitors network or system activities for malicious activities.
IP –Internet Protocol Address –an address of a computer or other network device using TCP/IP.
LAN - Local area network
MB – Megabyte – 1000 kilobytes
NMAP – A network device and port scanner
MFA – Multi Factored Authentication, typically an email code, or a text message.
RAM – Random Access Memory.
KB – Windows OS Patches that generally contain fixes, improvements, or security updates.
TB – Terabyte – 1000 gigabytes
USB – Universal Serial Bus
WAN – Wide-area network
WEP – Wired Equivalent Privacy: Security algorithm for IEEE 802.11 wireless networks. Introduced in 1997.
WPA – Wi-Fi Protected Access: WiFi standard that provides greater service than WEP.
WPA2 – Wi-Fi Protected Access 2: Latest WiFi standard that provides greater service than WPA.
VPN –Virtual Private Network: A method employing encryption to provide secure access to a remote computer over the Internet.VM –Virtual Machine: An operating system OS or application environment that is installed on software which imitates dedicated hardware.
WPA2 –Wi-Fi Protected Access 2: Latest Wi-Fi standard that provides greater service than WPA.

2 Management Overview

This home network was configured by another organization but is now being managed by Milton Perez. The implementations and operations presented will be done by Milton Perez. The improvements and management suggested will be carried out within the next two months.

2.1 Description of Implementation

This network and the components that function with the network were established before the plan was created. It has been running fine for months, but there are aspects of the network that need to be improved or re implemented including high protection firewalls, OS upgrades, physical and software security implementations, as well as remote VPN access.

2.2 Points-of-Contact

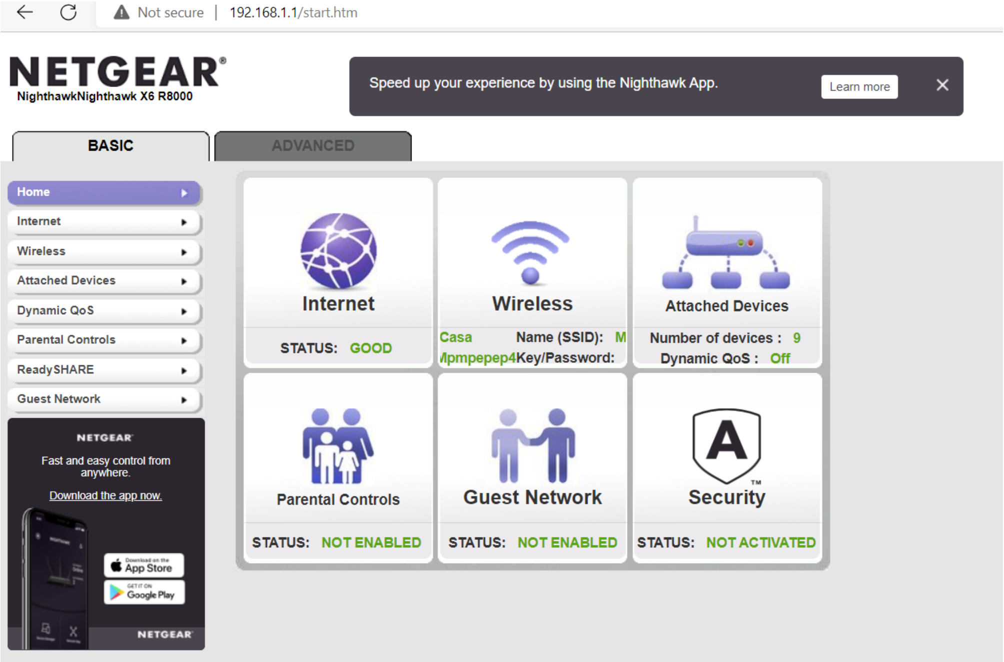
Role	Name	Contact Number
Business Sponsor	Milton Perez	239-898-0400
Project/Program Manager	Milton Perez	239-898-0400
Government Project Officer	Milton Perez	239-898-0400
System Developer or System Maintainer	Milton Perez	239-898-0400
Quality Assurance Manager	Milton Perez	239-898-0400
Configuration Management Manager	Milton Perez	239-898-0400
Security Officer	Milton Perez	239-898-0400
Database Administrator	Milton Perez	239-898-0400
Site Implementation Representative	Milton Perez	239-898-0400
IV&V Representative	Milton Perez	239-898-0400

Table 2.2 – Points-of-Contact

2.3 Major Tasks (Milestone 1 Task Consideration Documentation)

Firewall:

Currently there are no firewall settings on the spectrum home network.



Speed up your experience by using the Nighthawk App.

Fast and easy control from anywhere.

Internet

STATUS: GOOD

Wireless

Name (SSID): Casa M

Key/Password: Mpmpepep4

Attached Devices

Number of devices : 9

Dynamic QoS : Off

Parental Controls

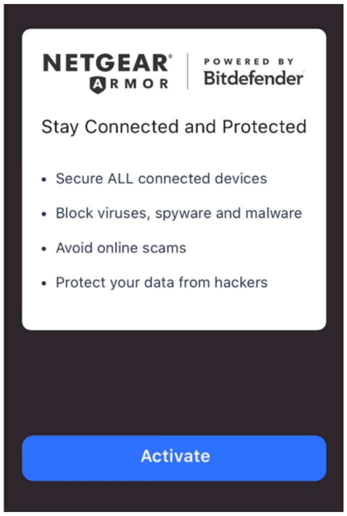
STATUS: NOT ENABLED

Guest Network

STATUS: NOT ENABLED

Security

STATUS: NOT ACTIVATED

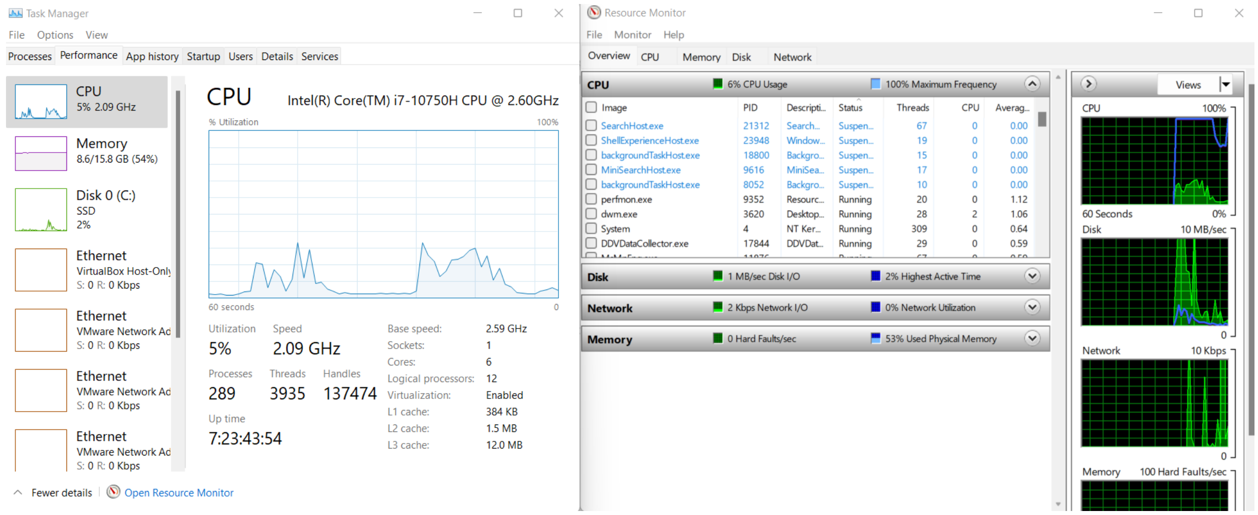


Stay Connected and Protected

- Secure ALL connected devices
- Block viruses, spyware and malware
- Avoid online scams
- Protect your data from hackers

After careful inspection, it was realized that the security features and firewall were not even activated yet on the router.

To better improve network monitoring we can activate the firewall and security features periodically check the network usage, open TCP connections, listening ports, and open processes by using the task manager setting and the resource manager tool. If something suspicious occurs, then the process can be suspended and blocked.



CPU
5% 2.09 GHz

Memory
8.6/15.8 GB (54%)

Disk 0 (C:)
SSD
2%

Ethernet
VirtualBox Host-Only
S: 0 R: 0 Kbps

Ethernet
VMware Network Ad
S: 0 R: 0 Kbps

Ethernet
VMware Network Ad
S: 0 R: 0 Kbps

Ethernet
VMware Network Ad
S: 0 R: 0 Kbps

CPU Intel(R) Core(TM) i7-10750H CPU @ 2.60GHz

Utilization: 5%
Speed: 2.09 GHz
Processes: 289
Threads: 3935
Handles: 137474
Up time: 7:23:43:54

Base speed: 2.59 GHz
Sockets: 1
Cores: 6
Logical processors: 12
Virtualization: Enabled
L1 cache: 384 KB
L2 cache: 1.5 MB
L3 cache: 12.0 MB

CPU — 6% CPU Usage — 100% Maximum Frequency

Image	PID	Descripti...	Status	Threads	CPU	Averag...
SearchHost.exe	21312	Search...	Suspen...	67	0	0.00
ShellExperienceHost.exe	23948	Window...	Suspen...	19	0	0.00
backgroundTaskHost.exe	18800	Backgro...	Suspen...	15	0	0.00
MiniSearchHost.exe	9616	MiniSea...	Suspen...	17	0	0.00
backgroundTaskHost.exe	8052	Backgro...	Suspen...	10	0	0.00
perfmon.exe	9352	Resourc...	Running	20	0	1.12
dwm.exe	3620	Desktop...	Running	28	2	1.06
System	4	NT Ker...	Running	309	0	0.64
DDVDataCollector.exe	17844	DDVDat...	Running	29	0	0.59

Disk — 1 MB/sec Disk I/O — 2% Highest Active Time

Network — 2 Kbps Network I/O — 0% Network Utilization

Memory — 0 Hard Faults/sec — 53% Used Physical Memory

Whitelisting MAC addresses of approved devices will also be conducted to further increase security and remove unapproved devices off the network.

Resources: Free, 10-minute
Key Person: Milton Perez
Successful Criteria: Stricter firewall settings implemented

Anti-Virus:

All windows endpoints on the network are already running Windows Defender, a free windows proprietary antivirus software. Both of the MacBooks are not currently running any type of antivirus software.
All users will be taught how to update the antivirus when the popup occurs.

Resources: Free, 10-minute install per endpoint
Key Person: Milton Perez
Successful Criteria: Antivirus is active and securing each endpoint

Equipment:

There are various amounts of instruction manuals and supplemental equipment for the devices in this network. They should all be consolidated and stored safely. If an incident were to arise the equipment and manuals will be easily accessible.

OS upgrades:

There is 1 mobile device that does not currently use the latest OS update. The laptop runs the current version of Windows 10. The other phones are up to date and both the MacBooks are running the latest OS system.

Resources: Free, 30 minute install per endpoint
Key Person: Milton Perez
Successful Criteria: iOS is updated to newest version

Data backup:

The existing network currently has no form of data backup at all since I have never considered it up until this moment. The Netgear plan includes 2TB of cloud storage that can be used as a backup for data such as, pictures, documents, and various other types of data that is important to the users.

Additionally, an external 2TB hard drive can be purchase to store other sensitive/personal data in house. https://www.bestbuy.com/site/seagate-one-touch-2tb-external-usb-3-0-portable-hard-drive-with-rescue-data-recovery-services-black/6439172.p?skuId=6439172

A device like Seagate OneTouch Backup 2TB External hard drives however would cost 67 dollars and would work for 5 users as well, being portable, physical and locally contained. The con is physical drives are likely to be stolen or break.

Both the local and remote back policies will be implemented

Resources: 67 dollars, 5 minute install per endpoint
Key Person: Milton Perez
Successful Criteria: Physical backups are enabled

Physical/Logistical security:

Currently the router/modem is located in a safe and central location. The router is kept in a separate room but not completely secured from potential adversaries. It is important for the router to be in a centralized location so that wireless traffic can reach the router across the premises. The room with the router is a small den and can be locked in order to prevent access.

Resources: 0 dollars, 1 minute install per endpoint
Key Person: Milton Perez
Successful Criteria: Securing/locking the router room.

2.4 Implementation Schedule (Milestone 1 Task implementation Documentation)

All changes will be logged and monitored once completed. This allows for a smooth transition to the new equipment and software.

- *Install Firewall and security settings on router*
- *Download and install Norton Anti-Virus Security on other unprotected devices*
- Consolidate Manuals and other related tools/equipment
- *Purchase an external 2TB hard drive*
- Update mobile devices with latest software/firmware
- Lock room to secure Router/Modem

All changes and their statuses will be maintained and updated in the implementation schedule. Any tasks that are canceled, rolled back, complete, or pending will be listed here.

Task	Start Date	End Date	Implementor	Rollback Plan	Status
Install and enable Firewall security rules	10/11/2022	10/18/2022	Milton Perez	Setup firewall and security devices for router	Pending
Update iOS	10/12/2022	10/12/2022	Milton Perez	Simple Update	Pending

2.5 Security and Privacy (Access Control Protections)

While the current network has a low-level firewall security implementation that allows users to access the internet, it is not strong enough and will be changed on 10/10/2022.
The endpoints themselves however have windows implemented accounts with passwords and pin enablement. The iOS devices have PIN or facial recognition. This aspect of the network can be improved and will be continuously investigated and visited as security threats evolve. One potential implementation is mandatory MFA on all devices.

2.5.1 System Security Features

- Passwords
- Operating System Updates
- Windows Defender Firewall
- Netgear Armor
- Physical Security

2.5.2 Security Set Up During Implementation (Access Control Protections)

This home network has no more than 5 concurrent end users, so the security implementation is as follows:

- All devices with sensitive information must have an encrypted drive, with username password authentication. External drives must also be encrypted.
- Devices that have no ability to use user authentication must be locked down to “guest” functionality. Meaning, it should have no access to sensitive data.
- Passwords must be strong (undecided) and changed periodically.
- All drives must be securely erased or destroyed if they are being sold or removed.

2.7 Open Issues

A few issues that need to be addressed later are:

1. Multi Factor authentication
2. Approving/Removing devices to the network (Process creation)
3. Naming conventions of endpoints
4. No Firewall or security features enabled
5. Figuring out unknown ports on devices
6. Expanding guest access and controls
    a. What can guests do and not do
    b. How to control and share network resources like printers

Milestone 3: Protect Your Network (Network Architecture)

3.1 Overview

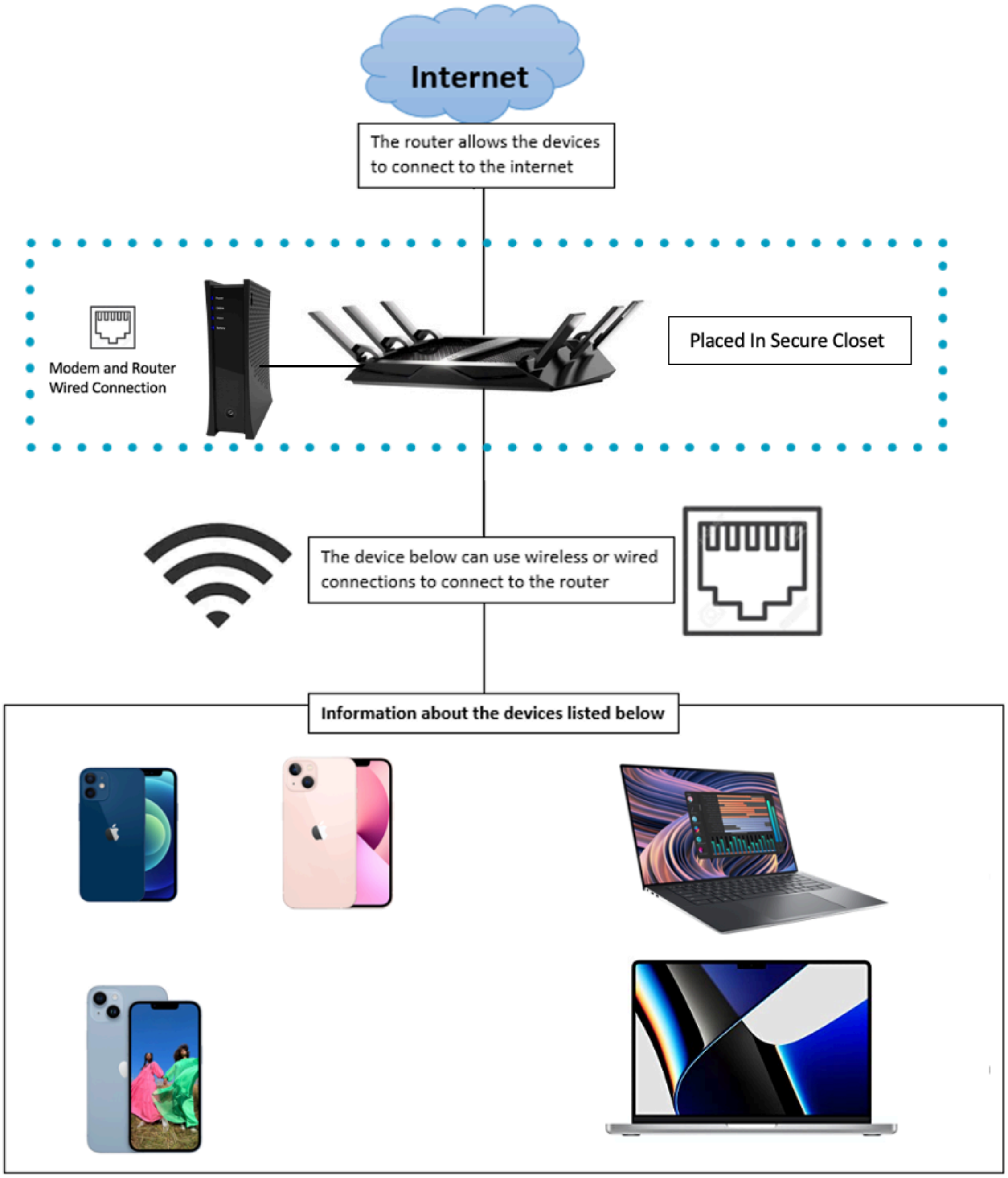
As previously described in section 2, the goal is to significantly increase the security of this home network to meet NSA guidelines and milestones outlined within this project. This will be done by adding both new hardware and software. This entails installing a new wireless router, a dedicated firewall, and software updates.

Previously, the host Windows PC were protected with the Windows firewall, the Apple Macbooks had no firewall, and the router had no security features turned on. One of h Macbooks was running outdated software. Also, the router was in an unsecure location. In this milestone assignment, I sought to enhance these security weakness by implementing security features to the router and updating the Macbooks.

3.2 Facilities and Network Enclaves

My private residence is the facility that houses this network. In order to move the Netgear router and Spectrum modem to a closet that is big enough for network equipment, new CAT5e cabling have been installed in the closet of the room. The closet door does not currently have a lock installed, but as part of this new implementation, a new keyed lock assembly will be fitted. This will give the network's modem, router, and infrastructure the necessary protection to guard against any illegal access.

3.3 New System Organization



The router allows the devices to connect to the internet

Placed In Secure Closet

The device below can use wireless or wired connections to connect to the router

Information about the devices listed below

3.5 High-Value Network Assets

The following items are considered the high-value network assets for this home network due to their importance to the users and functionality of the network:

- Netgear Nighthawk Router
- Spectrum Modem
- Dell XPS PC
- Apple Macbooks

The Netgear Nighthawk Router and spectrum modem are the most crucial and valuable elements on this list in terms of network connectivity because these are required for an internet connection. This is why it's crucial that they stay in a secure and safe location.

The new Nighthawk netgear and firewall, are considered high-value network assets as well since they provide the additional and much needed security to the infrastructure. The Netgear router also functions as a wireless access point for wireless clients such as laptops, tablets, and smartphones.

All of the Macbooks and the PC are backed up monthly to an external hard drive. Macbook-1 and PC-1 are the most critical machines at this point for me personally in time as it is utilized for my college courses and contains the data associated with the courseworks. Macbook-2, my sister's device is also important because she uses on the network for college courses as well so it is imperative to secure that device with the rest. Macbook-3 is my mom's device and is rarely used and if it is in use, it mostly is just used for browsing videos or personal use. Currently the network only has a 5.643 mbps upload speed, 174.16 mbps download speed, and 13.64 ms ping speed connections to the internet. This connection to the internet and these speeds are extremely important as this is currently the only high speed network service in place for the current infrastructure.

3.6 Choke Points On This Network

The choke points for this network are the Spectrum modem and the Netgear Nighthawk router. These both will be physically guarded against access by a key locked door in the closet of a room. The key to this closet will remain in a secure undisclosed location within the home.

3.7 Single Points of Failure

Single points of failure for this infrastructure are determined to be the Spectrum modem, Nighthawk Router, the devices as well as the spectrum Internet serviced provided. The security for the Nighthawk Router has been enhanced by adding a security layer to it called Netgear Armour that was previously disabled. The Spectrum modem software has been upgraded by contacting Spectrum and having them upgrade the software. In the future this will be done every 6 months to ensure that the modem is running the latest software.

It is worth noting that the internet service is out of my control. If the internet ever fails with the service provider there is no backup internet. In this case the only option is to use Verizon hotspots from our iPhones but that will quickly have its limitations due to bandwidth and costs.

3.8 Legacy Systems

There are no old hardware or software systems to maintain right now. Any current systems or software that ceases to be supported will be listed in this area and assessed to see if it should still be a part of the network or if it can be removed.

3.9 Plan Document Updates

If there are any architectural changes to the current network enclaves or choke points for this network, it will be the responsibility of Milton Perez to update this milestone to reflect such changes. This is to be performed within the five days of the such changes.

Milestone 4: Reach You Network (Device Accessibility)

4.1 Overview

This section describes the accessibility and administration of devices on this network including all PCs, routers, firewalls, and mobile devices.

4.2 Accessibility and Administration

4.2.1 Laptop Computers

The located throughout the home and spread across different rooms because of the different owners. All three macbooks have MacOS Big Sur installed, and the PC has Windows 10. There is only one administrative account and password on each of these devices. These passwords will have to be screened for complexity and it is recommended that they are updated every 6 months for security purposes.

All accounts on Macbooks utilize MacOS built in firewall features. These firewalls will be checked to ensure that they are set up and working correctly. Additionally firewall implementation for the Apple macbooks will be considered in this plan for the future. The PC currently runs Windows Firewall, and Windows automatic updates are enabled on it. Automatic updates are also set up for the Macbooks as well.

No current guest accounts are enabled on the PC or macbooks will be added in the to do section of this document to add another layer of security when outsiders utilize these devices on the current network.

4.2.2 Mobile Devices

All mobile devices are iPhones and come with a built in firewall. This firewall will be checked to ensure that it is up to date and running correctly.

4.2.3 Printers

There are currently no active printers on this network. Since most documents can be sent electronically, there is no need for us to have a printer. If any user needs to print something then offsite printing is commonly utilized.

4.2.4 Remote Administration

Remote administration for this network is currently not enabled at the moment for any devices or to manage this network.

Remote administration will be considered in the final plan of this document to see if it is viable since it could add another security layer to the infrastructure.

4.2.5 Physical Security

As mentioned in Milestone 3, this network is installed on my current home infrastructure. The devices which mainly include, laptops and mobile devices, are used by three users both in and out of the home.

The primary network components are the Spectrum modem and Netgear router which are now located in the closet of the room in which they previously resided in. A lock will be placed on this closet door in the future with a key. The key to this closet is stored in a safe place within the home so that family members may have access to it if needed.

4.3 Automating Administration

As of right now, this network lacks a server, which may restrict the automation of various administrative duties that may be done by a centralized management system like that found in Macbooks and Microsoft Windows Server. The following policies will be present on this network despite the absence of centralized server to automate administrative activities whenever possible.

- Enable Windows Update service on the PC and prevent users from disabling without administrative privileges.
- Enable Apple update services on the Macbooks and prevent users from disabling without administrative privileges.
- Enable automatic updating for the Negear Router and prevent users from disabling without administrative privileges.
- Check in with spectrum to ensure the modem is up to date.

4.4 Administrative Tools

The management of each type of device will follow the same procedures as described previously. To ensure a uniform, standard procedure, the security tools and password will be set up in the same way.

4.5 Plan Document Updates

If there are any accessibility changes to the current network enclaves or changes to the security configurations for any device on this network, it will be the responsibility of Milton Perez to update this milestone to reflect such changes. This is to be performed within the five days of the such changes.

Milestone 5: Control Your Network(User Access)

5.1. User Accounts

It is policy for this network that no user accounts will have admin access to router or modem unless needed other than Milton Perez.

Admin accounts are allowed on current devices but will be supervised with the help of Milton Perez. This is to ensure that each user has full access to their devices since each user has their own use times and tasks that they need to accomplish with their devices.

Each computer will have a guest account installed so that visitors can use the internet, but these accounts only give non-elevated access to the network and Internet.

5.2 Privileged accounts

Each computer will come with their own privileged account run by their administrator. Milton Perez will just oversee the network and check in with current users to ensure that all security protocols are being followed.

5.3 Least privilege administrative model

There is currently no server on this network but it will be looked into.

5.4 Users Installing Software

There are currently no elevated/privileged accounts. This will be looked into more detail in future milestones plans.

5.5 Expiration Dates On Accounts

There are not currently an expiration dates on accounts. It will be standard procedure to evaluate accounts at least every six months to see if any need to be terminated.

5.6 Plan Document Updates

If there are any changes or additions to the users of the network, it will be the responsibility of Milton Perez to update this milestone to reflect such changes. This is to be performed within the five days of the changes.

Milestone 6: Manage Your Network, Part I (Patch Management)

Vulnerable devices on a network are often used as entry points for dangerous network attacks. Actively managing your network devices in a few areas can dramatically improve your security; this milestone and the next are focused on setting up these management areas. Note that specific implementations will differ for different device roles and operating systems. Note also that truly *effective* management of these areas relies on the previous milestones being completed.

Patch management process.
NOTE Also documented it in the device list from Milestone 2 for each device (or group of identical devices), include:

- Patches will be applied every 6 months or as necessary.
- Patches will be downloaded by the sysadmin or users, verified by sysadmin, and tested by the sysadmin.
- Patches will be done automatically unless they become absolutely necessary to be done manually.
- If any patches need to be applied manually then they it will be up the sysadmin to determine a course of action.
- Patch application will verified by the sysadmin using online metrics to ensure hashes match.
- Any specific system that warrants an exception from the patch management process, or reasons for the exception, and how this vulnerability of an unpatched system is being mitigated will be addressed accordingly when that moment occurs.

Non Microsoft Updates:

To inform administrators of new updates and patches for non-Microsoft applications, third-party apps, device drivers, and Web browser plug-ins, management tools and processes must be put in place.

No-End of Life Software/Hardware:

Devices with End-of-Life (EOL) software or hardware should be taken off the network as they provide a significant security risk and cannot be patched. Administrators will make sure that no EOL software or hardware is installed on any networked devices. The free EOL Lookup web service from SolarWinds

Using Virtualization:

In some environments, patching and controlling centrally stored pictures is more effective than patching widely dispersed individual workstations. If using virtualization is required, more research and preparation are needed. VMware or VirtualBox are two potential virtualization tools.

Using Administrative Tools:

Administrators must update administrative tools like Nmap, Wireshark, PuTTY, Puppet, network access control, etc. during the patch management process. In addition, security tools will be updated to prevent them from developing weaknesses that might make the network less secure.

Milestone 7: Manage Your Network, Part II (Baseline Management)

Application List:

Application Name	**Version**
Discord	2021 or newer
VMWare or VMware fusion (for Mac OS devices)	17
Microsoft Office	2021
Virtual Box	6.1.26
Microsoft Teams	2022.39.01.3
Google Chrome	108.0.5359.71
Firefox	107.0
Wireshark	4.0.1
IntelliJ 2022	2022
PyCharm	2022
Code::Blocks	2022

These application have been approved for specific reasons as the are necessary for users to accomplish everyday activities. More details on each program below:

- Discord and Microsoft teams are used to communicate with classmates and friends.
- VMware and VirtualBox are used for virtualization.
- Microsoft office is used for school or work purposes to generate, read, and write documents.
- Google Chrome and Firefox are approved web browsers to browse the internet.
- Wireshark is used as a packet sniffer for home labs.
- IntelliJ, Code::Blocks, and PyCharm are IDEs used to create, write, and read different programs.

Application Approval Criteria:

- Is this the application needed to accomplish a goal?
- Is it being downloaded from a trusted source?
- Are there any known security issues/flaws?
- Is the application critical for daily operations or use?

If the answer to all these questions are met and any admin or sysadmin approves of the application then it will be alright to download onto a device that utilizes this network.

Device Baseline:

All devices will be hardened by downloading routine patches and following recommended security guidance. All applications will be checked every 6 months to ensure that they are up to date and meet this criteria.

Offline Backup:

The data and files for these applications will be backed up and saved on the SSD that was purchased within the scope of this milestone project. It is password encrypted. If there is any point of failure, data or files can be restored from there while the applications can just be redownloaded.

Same Password Problem:

There will be local admin accounts for each device and users are encouraged to not use the same passwords. This is to ensure that they can make changes without the sysadmin present. Also, guest accounts will be mandatory on all laptops to ensure that no one is sharing passwords.

Device Integrity:

System integrity checking tools to verify the integrity of the baseline installs on your devices. This is very important to discover any unauthorized changes. If possible, these integrity checks will be automated. They will also be routinely inspected every 6 months.

Automatic Reboots:

It will be recommended for all laptops to reboot their laptops at least once a day when they are done using it. Mobile devices can be rebooted bi-weekly since they are not believed to be a huge security concern.

Hardware Configurations:

All hardware configurations are done by the admins and to be checked by the sysadmin as needed. All of our devices are laptops, MacBook’s, or iPhones. They will be routinely inspected to ensure that proper and necessary hardware configurations are enabled.

Supply Chain:

We are not concerned with the supply chained risks because this a small private home network running limited devices.

Milestone 8: Document Your Network

As time permits, your processes and procedures for your network should be documented. This helps keep your network manageable. Even if you only have time to document one process per week, that's still better than nothing! Be sure to give priority to documenting those things that are most important to keeping your organization doing business.

In Case of Rebuild:

Contact the sysadmin of this network. All devices will be dealt with in accordance with the law and their user guidelines. The router and modem are owned by spectrum so if something this serious happens that warrants a rebuild, spectrum will need to be contacted. The sysadmin will work with the network provider.

How to add a new user:

Adding any new user to any account would be a very special case that will only be done if someone moves into the house or network that requires their own login credentials and set of devices. For most cases, guest users can be utilized.

How and when to remove a user:

Users will be removed when the move out of the house or away from the current network to eliminate clutter and unused accounts.

How to add a new system:

For the PC, right-click the "Computers" icon listed under the server's domain. Select "New" and then "Computer" from the menu. A configuration window opens to add the new computer. For the Mac, the single digits will be utilized by logging onto the network and selecting add a device.

How to remove a system:

For the PC, right-click the "Computers" icon listed under the server's domain. Select “Remove” & then the system which you wish to remove. For the Mac, the single digits will be utilized by logging onto the network and selecting remove device.

APPENDIX

APPENDIX A: Manageable Network Implementation Plan Approval

The undersigned acknowledge that they have reviewed the Milton Perez Home Network **Implementation Plan** and agree with the information presented within this document. Changes to this **Manageable Network Implementation Plan** will be coordinated with, and approved by, the undersigned, or their designated representatives.

Signature: Milton Perez Date: 12/02/2022

Print Name: Milton Perez

Title: Network Administrator

Role: Project Manager

APPENDIX B: REFERENCES

The following table summarizes the documents referenced in this document.

Document Name	Description	Location
AV-TEST.org -1.0	AV-test conducts antivirus evaluations on a point-based system including protection, performance, and usability	Test Malwarebytes Premium 4.4.2 &amp; 4.4.4 for Windows 10 (211414) | AV-TEST
Microsoft OS Builds	Lists Windows 1	https://support.microsoft.com/en-us/topic/windows-10-update-history-8127c2c6-6edf-4fdf-8b9f-0f7be1ef3562
Mac OS Builds		https://support.apple.com/en-us/HT211896

APPENDIX C: Milestone-1 Check-List

Yes	No	Explanation	Accepts Risk	Milestone 1: Prepare to Document
Yes		1.2		Do you have a way to document information about your network?
Yes		Weekly, updated Fridays 1.2		Are you currently documenting all changes to your network?
Yes		1.2		Have you gone over the points to consider for this Milestone?

Checklist date: 10/10/2022

APPENDIX D: Milestone-2 Check-List

Yes	No	Explanation	Accepts Risk	Milestone 2: Map Your Network
Yes		Section 1.2.3		Do you have a current, accurate network map?
Yes		Section 1.2.3 Checked every Friday		Do you have a current, accurate list of ALL devices on your network (or that ever connect to your network), that records host name, role, MAC address, service tag, physical location, OS/firmware, and responsible person/group? - Total number of devices on your network, broken down by category (workstation/server/supporting/infrastructure/mobile/removable media)? - How often is this list checked for accuracy by using discovery tools?
Yes		Section 1.2.3		Do you have a current, accurate list of ALL protocols that are running on your network?
Yes		Section Every Friday 7 Days		Are you updating your network map and lists of devices and protocols whenever a change is made to your network? - When there is a change, how long before this documentation is updated?
Yes		Section 1.2.3, 2.5.2		Have you gone over the points to consider for this Milestone?

Checklist date: 10/10/2022

APPENDIX E: Milestone-3 Check-List

Yes	No	Explanation	Accepts Risk	Milestone 3: Protect Your Network (Network Architecture)
X		Yes. Detailed in the milestone		Have you identified and documented your current network enclaves?
X		Yes. Detailed in the milestone		Have you identified and documented the current highvalue assets and choke points on your network?
X		This is the initial creation of this network plan. All future changes to the network shall be documented per the milestone details		Are you updating your documentation whenever your network enclaves, high-value assets, or choke points change? - When there is a change, how long before this documentation is updated?
X		This is the initial creation of this network plan. Items are described in the milestone.		Are you periodically re-evaluating your network architecture to make sure it most effectively protects your high-value assets, limits access to sensitive information, and keeps damage contained? - How often are these re-evaluations done? - How often do you review your network trust relationships? - If a trust relationship is found that can be eliminated or limited, how long before this elimination/limiting is actually done?
X				Have you gone over the points to consider for this Milestone?

Checklist date: 11/07/2022

APPENDIX F: Milestone-4 Check-List

Yes	No	Explanation	Accepts Risk	Milestone 4: Reach Your Network (Device Accessibility)
X		Detailed in Milestone 4		Have you established and documented a process to properly, easily, and securely access and administer EVERY device on your network (workstations, servers, supporting devices, infrastructure devices, and mobile devices)?
X		Detailed in Milestone 4		Are you updating your device access/administration process and documentation as necessary?
X		Detailed in Milestone 4		Have you gone over the points to consider for this Milestone?

Checklist date: 11/07/2022

APPENDIX G: Milestone-5 Check-List

Yes	No	Explanation	Accepts Risk	Milestone 5: Control Your Network (User Access)
X		Detailed in Milestone 5		Have you established non-privileged user accounts for all users on your network?
				- % of *total* users on your network that are allowed to use *only* non-privileged accounts? (Higher % is more secure)
X		Detailed in Milestone 5		For all users with elevated privileges, have you documented the privileges given and the reasons for giving those privileges, and are those reasons regularly reviewed? - How often are the reasons for giving those privileges reviewed? - If the reasons are no longer valid or no longer justifiable, how long before the privileges are actually removed? - % of elevated privilege accounts that do NOT have access to Internet or e-mail? (Higher % is more secure)
X		Detailed in Milestone 5		Are you periodically verifying that all accounts on your network are tied to specific, current, authorized users? - How often are these verifications done? - If an account is found that cannot be so verified, how long before this account is disabled? - If a user becomes unauthorized (terminated, etc.), how long before his account(s) are actually disabled?
X		Detailed in Milestone 5		Have you gone over the points to consider for this Milestone?

Checklist date: 11/07/2022

APPENDIX H: Milestone-6 Check-List

Yes	No	Explanation	Accepts Risk	Milestone 6: Manage Your Network, Part I (Patch Management)
X		All devices have been looked into, patched, ensure to be up to date.		Have you established and documented a patch management process for ALL the OS and application software on EVERY device on your network (workstations, servers, supporting devices, infrastructure devices, and mobile devices)? - Within each device category, % of devices actually patched via this process? - Within each device category, % of devices that are assessed by an automated capability that they are adequately free of vulnerabilities?
X		Patch management is being done by me periodically.		Are you updating your patch management processand documentation as necessary?
X		Yes.		Have you gone over the points to consider for this Milestone?

Checklist date: 12/02/2022

APPENDIX I: Milestone-7 Check-List

Yes	No	Explanation	Accepts Risk	Milestone 7: Manage Your Network, Part II (Baseline Management)
X		Yes, they were documented and will be kept up to date.		Have you created and documented a list of all the applications that are approved for use on your network? - Within each device category, % of devices that have an automated capability to prevent or restrict execution of unapproved applications and other unapproved executable content? (Higher % is more secure)
X		Yes, they were documented and will be kept up to date.		Have you established and documented the criteria and process for getting an application on the approved list?
X		Yes, they were documented and will be kept up to date.		Have you created and documented device baselines (including for infrastructure devices and mobile devices)? - Within each device category, % of devices actually covered by a documented baseline? - Within each device category, % of devices that are compliant with their documented baseline (no changes or additions)? - Within each device category, % of devices that have an automated capability to verify compliance (detect changes and additions)?
X		Yes, they were documented and will be kept up to date.		Are you updating your device baselines on a regular basis?
X		Yes, they were approved and will be kept up to date.		Are you updating your approved application list, criteria and process for getting an application on the approved list, and baselines documentation whenever there is a change?
X		Yes, they were documented and will be kept up to date.		Have you gone over the points to consider for this Milestone?

Checklist date: 12/02/2022

APPENDIX I: Milestone-8 Check-List

Yes	No	Explanation	Accepts Risk	Milestone 8: Document Your Network
x		Yes, they were documented and will be kept up to date.		Are the procedures to rebuild servers and other important devices on your network fully documented and kept up to date?
x		Yes, they were documented and will be kept up to date.		Are the procedures for adding and removing users and systems from your network fully documented and kept up to date?
x		Yes, they were documented and will be kept up to date.		As time permits, are you documenting all other administrative processes and procedures, and keeping them up to date?
x		Yes, they were documented and will be kept up to date.		Have you gone over the points to consider for this Milestone?

Checklist date:12/02/2022

[Insert appropriate disclaimer(s)]