NSA Community Gold Standard Technical Guidance:

MANAGEABLE NETWORK PLAN

Ethan Couch - Home Network

Manageable Network Plan

Version 3.1
4/24/23

VERSION HISTORY

The document will be updated with a new version on a bi-weekly basis.

Version #	Implemented By	Revision Date	Approved By	Approval Date	Reason
1.0	Ethan Couch	2/26/23	Ethan Couch	2/27/23	Document Creation
2.0	Ethan Couch	4/1/23	Ethan Couch	4/3/23	Milestone 3, 4, 5 Implementation
3.0	Ethan Couch	4/15/23	Ethan Couch	4/14/23	Milestone 6, 7, 8 Implementation
3.1	Ethan Couch	4/24/23	Ethan Couch	4/24/23	Final Revision

Table of Contents

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).

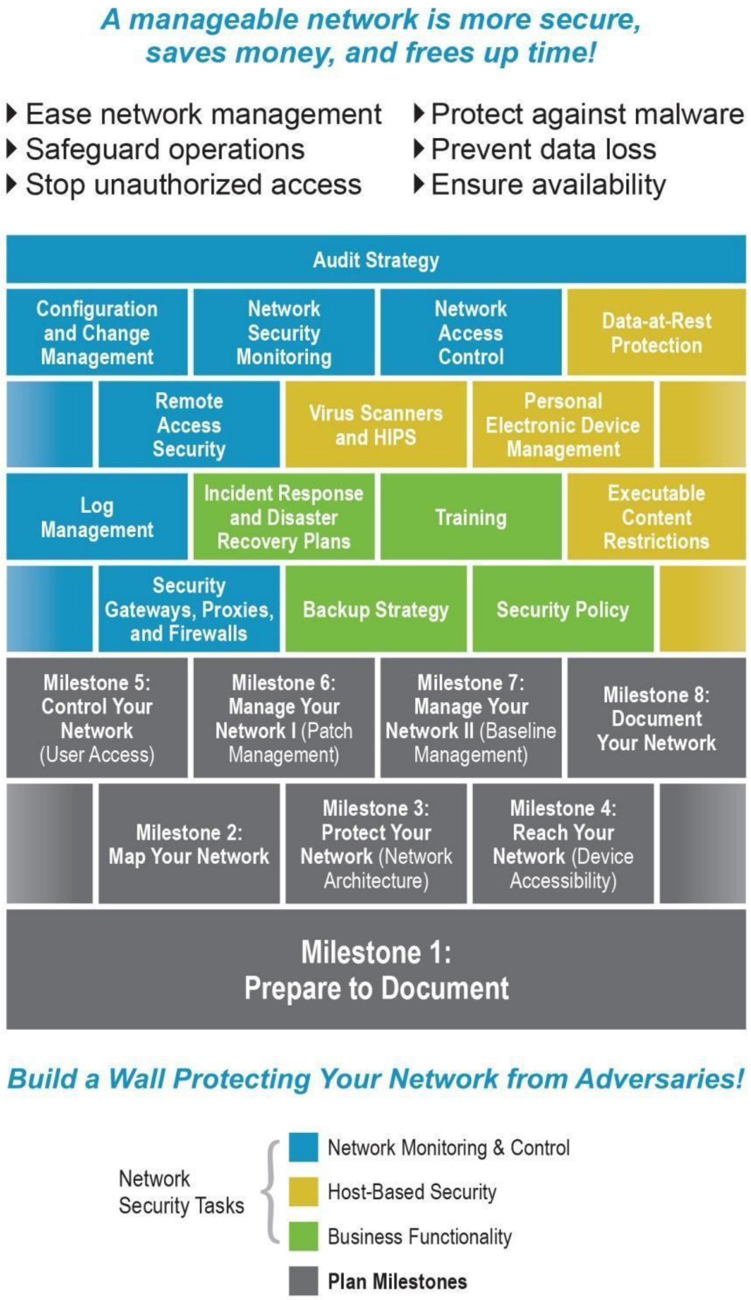

A manageable network is more secure, saves money, and frees up time!
Ease network management
Safeguard operations
Stop unauthorized access
Protect against malware
Prevent data loss
Ensure availability
Audit Strategy
Configuration and Change Management
Network Security Monitoring
Network Access Control
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 Frontier 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 Ethan Couch’s OneDrive or GoogleDrive 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 Monday 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 Ethan Couch, primarily for schoolwork, web browsing, gaming, streaming content, and cybersecurity research. There are three 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 Eero router utilizes WPA2 key with a trivial password generated by the family.

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

Operating systems being used by endpoints on the network are:

- Windows 10
- Apple iOS 15
- Apple iOS 16
- Android 5.0
- Windows 11
- Linux 3.2-4.9

The router being used for wireless and wired connections is the Eero Pro 6

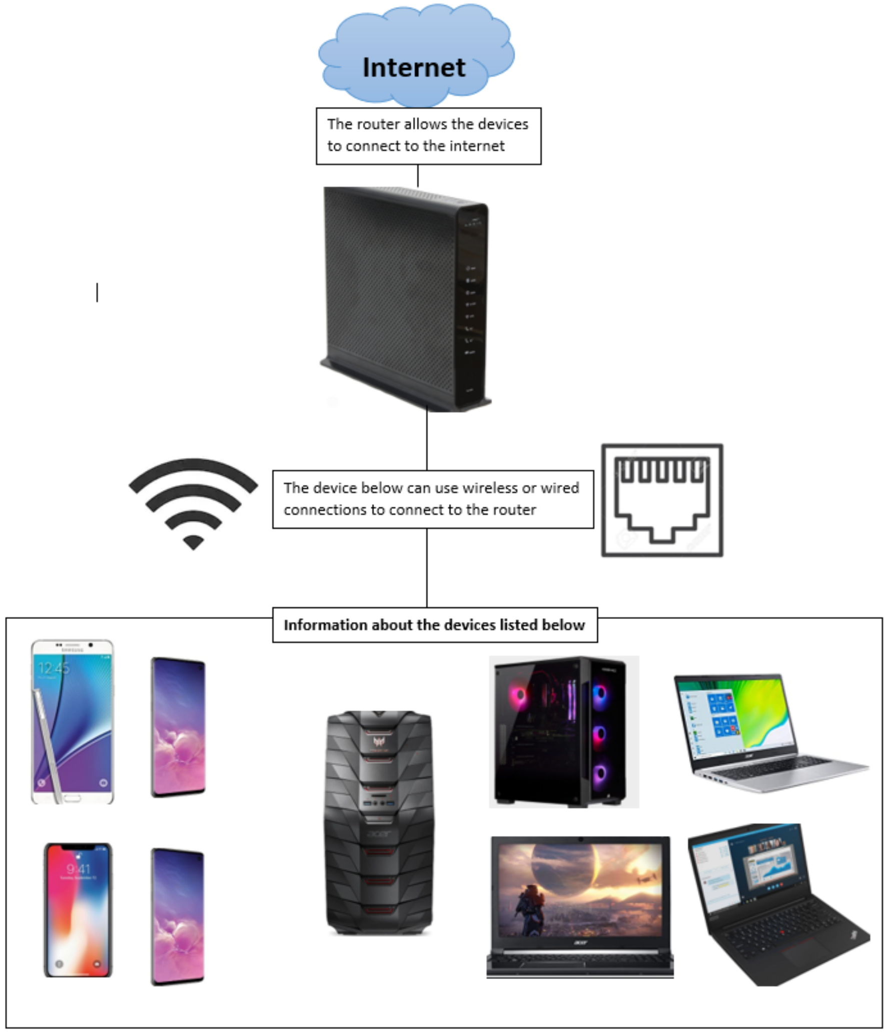
1.2.2 Assumptions and Constraints

- 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.
- 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 Ethan Couch has access to resources and skillset 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 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.



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 Eero Pro 6 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.

PC Device Information:

Device	Form Factor	Manufacturer	Model	MAC Address	RAM	OS Version	Assignment	Service Tag
Ethans-PC *192.168.4.34*	Desktop	Custom-Prebuilt	ASUS ROG Strix x670E-E	C8:7F:54:00:D2:F4	64GB	22H2 Windows 10 Education	Ethan Couch	N/A
Addys-PC *192.168.4.23*	Desktop	Alienware	Alienware Aurora r7	90:CD:B6:41:13:21	16GB	22H2 Windows 10	Addison Couch	J6FRMD2

						Home		
Moms-Laptop *192.168.4.27*	Laptop	HP	HP Spectre x360 Convertible	1C:1B:B5:F4:77:02	16GB	22H2 Windows 10 Home	Lisa Couch	HP-2
Wes1961 *192.168.4.121*	Desktop	HP	Intel(R) Celeron(R) N5105	2C:0D:A7:D5:C9:C4	16GB	22H2 Windows 11 Pro	Wes Couch	HP-1

Phone/Tablet Device Information:

Device	Model	Manufacturer	MAC Address	OS Version	Assignment	Service Tag
Ethans Iphone *192.168.4.25*	iPhone 13 Pro Max	Apple	06:C2:34:16:F2:37	iOS 15.6.1	Ethan Couch	Apple-1
Addys Iphone *192.168.4.33*	iPhone 13 Pro Max	Apple	82:AC:38:43:8C:48	iOS 15.6.1	Addison Couch	Apple-2
Lisas Iphone *192.168.4.108*	iPhone 12 mini	Apple	8A:0A:49:52:F4:71	iOS 16.11	Lisa Couch	Apple-3

IoT Device Information:

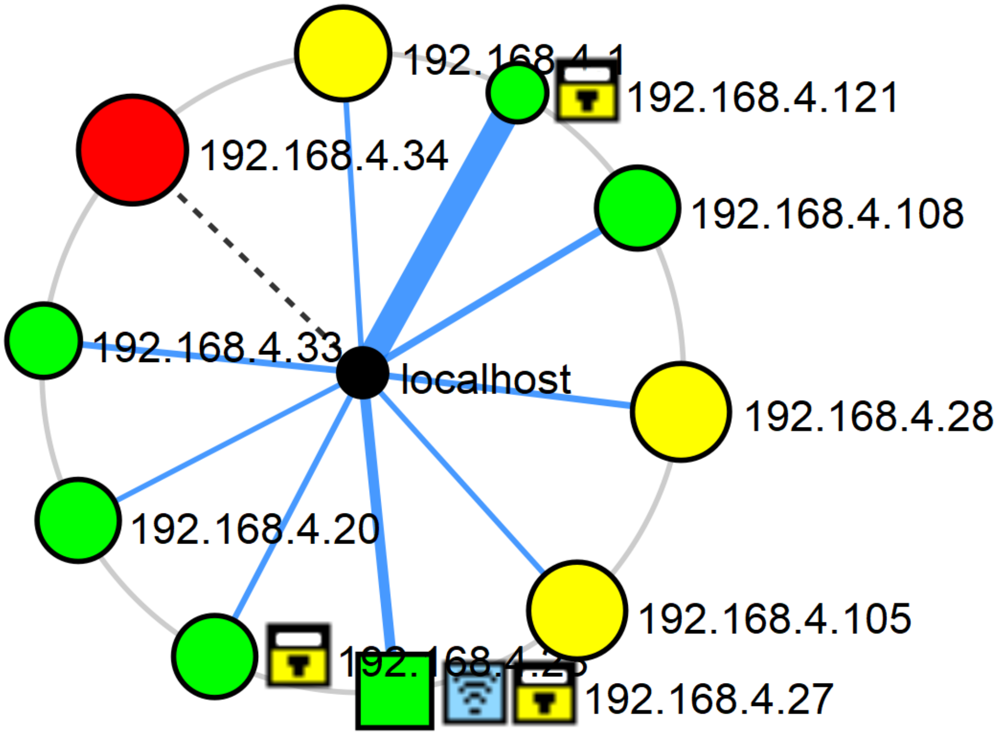
Device	Manufacturer	Model	Mac Address	OS Version
TV *192.168.4.105*	Sony	Sony X75CH-series Android TV	38:B8:00:8E:B4:FE	Android 5.0
Router **192.168.4.1**	Eeros	eero Pro 6	84:70:D7:A9:B6:12	Linux 3.2-4.9
Printer *192.168.4.28*	HP	HP6AA744 (HP ENVY Photo 7800 series)	48:BA:4E:6A:A7:45	Linux 3.2-4.9
Home Server *192.168.4.20*	Dell	PowerEdge R620 Server	84:70:D7:B3:CA:D2	Linux 3.2-4.9

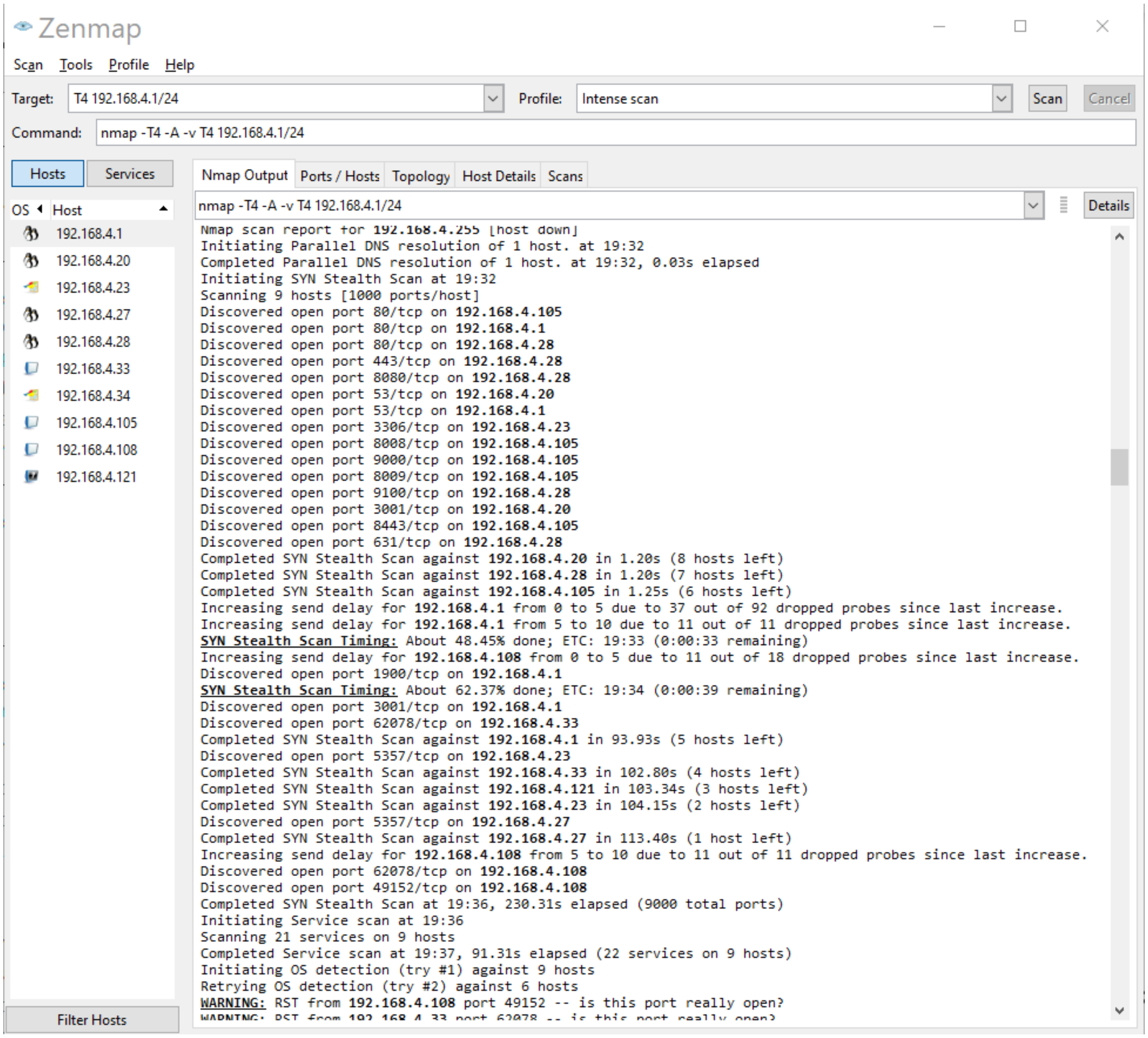
Total Device Count: 11

As can be seen, the naming convention of my devices is highly disorganized. All device’s possess varying naming conventions based on whether or not their user added a custom name or stuck with the default name of the device. 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. The following command was executed using Zenmap GUI:
Command: nmap -s0 192.168.4.1/24

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





Target: T4 192.168.4.1/24

Profile: Intense scan

Command: nmap -T4 -A -v T4 192.168.4.1/24

```
192.168.4.1
192.168.4.20
192.168.4.23
192.168.4.27
192.168.4.28
192.168.4.33
192.168.4.34
192.168.4.105
192.168.4.108
192.168.4.121
```

```
nmap -T4 -A -v T4 192.168.4.1/24
```

```
Nmap scan report for 192.168.4.255 [host down]
Initiating Parallel DNS resolution of 1 host. at 19:32
Completed Parallel DNS resolution of 1 host. at 19:32, 0.03s elapsed
Initiating SYN Stealth Scan at 19:32
Scanning 9 hosts [1000 ports/host]
Discovered open port 80/tcp on 192.168.4.105
Discovered open port 80/tcp on 192.168.4.1
Discovered open port 80/tcp on 192.168.4.28
Discovered open port 443/tcp on 192.168.4.28
Discovered open port 8080/tcp on 192.168.4.28
Discovered open port 53/tcp on 192.168.4.20
Discovered open port 53/tcp on 192.168.4.1
Discovered open port 3306/tcp on 192.168.4.23
Discovered open port 8008/tcp on 192.168.4.105
Discovered open port 9000/tcp on 192.168.4.105
Discovered open port 8009/tcp on 192.168.4.105
Discovered open port 9100/tcp on 192.168.4.28
Discovered open port 3001/tcp on 192.168.4.20
Discovered open port 8443/tcp on 192.168.4.105
Discovered open port 631/tcp on 192.168.4.28
Completed SYN Stealth Scan against 192.168.4.20 in 1.20s (8 hosts left)
Completed SYN Stealth Scan against 192.168.4.28 in 1.20s (7 hosts left)
Completed SYN Stealth Scan against 192.168.4.105 in 1.25s (6 hosts left)
Increasing send delay for 192.168.4.1 from 0 to 5 due to 37 out of 92 dropped probes since last increase.
Increasing send delay for 192.168.4.1 from 5 to 10 due to 11 out of 11 dropped probes since last increase.
SYN Stealth Scan Timing: About 48.45% done; ETC: 19:33 (0:00:33 remaining)
Increasing send delay for 192.168.4.108 from 0 to 5 due to 11 out of 18 dropped probes since last increase.
Discovered open port 1900/tcp on 192.168.4.1
SYN Stealth Scan Timing: About 62.37% done; ETC: 19:34 (0:00:39 remaining)
Discovered open port 3001/tcp on 192.168.4.1
Discovered open port 62078/tcp on 192.168.4.33
Completed SYN Stealth Scan against 192.168.4.1 in 93.93s (5 hosts left)
Discovered open port 5357/tcp on 192.168.4.23
Completed SYN Stealth Scan against 192.168.4.33 in 102.80s (4 hosts left)
Completed SYN Stealth Scan against 192.168.4.121 in 103.34s (3 hosts left)
Completed SYN Stealth Scan against 192.168.4.23 in 104.15s (2 hosts left)
Discovered open port 5357/tcp on 192.168.4.27
Completed SYN Stealth Scan against 192.168.4.27 in 113.40s (1 host left)
Increasing send delay for 192.168.4.108 from 5 to 10 due to 11 out of 11 dropped probes since last increase.
Discovered open port 62078/tcp on 192.168.4.108
Discovered open port 49152/tcp on 192.168.4.108
Completed SYN Stealth Scan at 19:36, 230.31s elapsed (9000 total ports)
Initiating Service scan at 19:36
Scanning 21 services on 9 hosts
Completed Service scan at 19:37, 91.31s elapsed (22 services on 9 hosts)
Initiating OS detection (try #1) against 9 hosts
Retrying OS detection (try #2) against 6 hosts
WARNING: RST from 192.168.4.108 port 49152 -- is this port really open?
WARNING: RST from 192.168.4.33 port 62078 -- is this port really open?
```

Protocols used: TCP, HTTP, UDP

Ports used: 53, 80, 1900, 3001, 135, 139, 445, 3306, 5357, 62078, 631, 8080, 9100, 902, 912, 1042, 1043, 6881, 8008, 8009, 8443, 9000 , 49152

Software:

This network uses the internet for educational and recreational purposes. All software listed is installed to Windows 10 and 11endpoints is listed as Bundle-A in the NMAP inventory Table:

- Free
  - Windows Defender
  - TeamViewer
  - Nmap
  - Discord
  - Google Chrome
  - Google Docs
  - Slack
  - Malwarebytes
- Licensed
  - Microsoft Office 2023
  - VMware Workstation Pro

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

- VMWare
- VirtualBox
- Wireshark
- Nmap
- Bitwarden
- Microsoft Teams
- Microsoft Office 2023
- Visual Studio Code
- Visual Studio
- Github Desktop

NMAP Inventory

Host	Device	Software	NMAP-Ports/Protocols	Description
192.168.4.34	Ethans-PC	Bundle-A & Bundle B	135, 139, 445, 902, 912, 1042, 1043, 5357, 6881	My main workstation for productivity.
192.168.4.23	Addys-PC	Bundle-A & Bundle B	135, 139, 445, 3306, 5357	Brother’s main workstation for productivity/gaming.
192.168.4.27	Moms-Laptop	Bundle A	5357	

192.168.4.121	Wes1961	Bundle A	80, 135, 445	
192.168.4.25	Ethans Iphone	N/A	62078	All mobile devices used mainly for texting, audio streaming, and web browsing.
192.168.4.33	Addys Iphone	N/A	62078	
192.168.4.108	Lisas Iphone	N/A	49152, 62078	
192.168.4.105	TV	N/A	80, 8008, 8009, 8443, 9000	
192.168.4.1	Router	N/A	53, 80, 1900, 3001	
192.168.4.28	Printer	N/A	80, 443, 631, 8080, 9100	
192.168.4.20	Home Server	N/A	53, 3001	Currently offline and misconfigured. Serves as a would-be hosting grounds for multiple VMs and a DNS Sinkhole

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
DMZ - Demilitarized Zone - a perimeter network that protects an organization’s internal LAN from untrusted traffic.
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 Ethan Couch. The implementations and operations presented will be done by Ethan Couch. 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. Additionally, certain ports need to be examined for security vulnerabilities, and should be disabled if deemed nonessential for the device's operation.

2.2 Points-of-Contact

Role	Name	Contact Number
Business Sponsor	Ethan Couch	813-997-1234
Project/Program Manager	Ethan Couch	813-997-1234
Government Project Officer	Ethan Couch	813-997-1234
System Developer or System Maintainer	Ethan Couch	813-997-1234
Quality Assurance Manager	Ethan Couch	813-997-1234
Configuration Management Manager	Ethan Couch	813-997-1234
Security Officer	Ethan Couch	813-997-1234
Database Administrator	Ethan Couch	813-997-1234
Site Implementation Representative	Ethan Couch	813-997-1234
IV&V Representative	Ethan Couch	813-997-1234

Table 2.2 – Points-of-Contact

2.3 Major Tasks (Milestone 1 Task Consideration Documentation)

Firewall:

Currently, there is no robust firewall solution that is implemented on all devices. I am unable to login to my current router interface, where I will ideally limit outbound access to DHCP, DNS, IMAP, SMTP, POP3, HTTP, HTTPS, FTP, and Telnet. This situation will be changed as soon as possible, and my home server will be setup on the network with its respective firewall through Proxmox VE. This will allow adequate protection of the virtual machines it hosts.

To better improve network monitoring we can 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.

Specifically, I intend to use Nessus to scan my network for vulnerabilities periodically, where I will then take hardening/remediating action based on the scan results of each Nessus scan. The Nessus interface will be set up on my homelab/home server. Ports need to be managed on a basis to prioritize both security and functionality of all devices.

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

Resources: Free, 60-minutes
Key Person: Ethan Couch
Successful Criteria: Stricter firewall settings implemented, Proxmox VE firewall implemented

Anti-Virus + VPN Implementation:

All windows endpoints on the network are already running Windows Defender, a free windows proprietary antivirus software. Additionally, I will need to ensure that all windows systems are up to date, and that Windows Defender is correctly enabled on each machine. For my mobile devices, I may opt to use a mobile firewall app or VPN such as Nord VPN to offer increased security with mobile traffic.

As a backup to Windows Defender, I will ensure installation of Malwarebytes's free home version to provide stronger protections against malware infections with no noticeable performance impact compared to Windows Defender. This product will allow for free improvements to endpoint security and enables routine scanning and web filtering based off their malicious URL database. Risks included with installing a new antivirus is it missing definitions, and ensuring it is up to date. All users will be taught to update the antivirus when the popup occurs.

Resources: Free, 20-minute install per endpoint
Key Person: Ethan Couch

Successful Criteria: Antivirus is active and securing each endpoint (Optional: VPN app installed on mobile devices)

OS upgrades:

Currently, there are 2 mobile devices (iPhones) that are not updated to the latest version. These devices will be updated, and updates will be monitored for all devices at the start of every week on Monday. The owners of respective devices will be reminded of this process every week to ensure safety of personal data.

Resources: Free, ~15-minute install per endpoint
Key Person: Ethan Couch
Successful Criteria: All endpoints are running the latest respective Operating System version.

Specifically, all endpoints with Apple iOS 15 will need to be upgraded to version 16. This upgrade will take about 20 minutes but can be conducted in parallel.

Resources: Free, 20 minute install per endpoint
Key Person: Ethan Couch
Successful Criteria: iOS is updated to newest version. All Windows OS Current.

Data backup:

For the most part, the current network lacks a centralized data backup solution. This holds true for all devices except my desktop, which is backed up to a 2 TB external drive. As a starting point, all desktops and laptops will be backed up to an external drive of at least 1 TB. Referencing the current brand of external drive I use (G-Drive) it is expected that connecting all respective devices to an external drive will cost roughly $400.

If time and budget remains flexible, a cloud-based storage solution such as OneDrive and ICloud will be implemented across all devices to allow for at least 1 TB of cloud storage. At a minimum, this will cost $9.99/month for 1TB of ICloud storage. The assumption is that a universal implementation of Icloud (for all 3 Iphone devices) will cost upwards of $29.99/month.

Resources: 400 dollars + $29.99/month (optional), 10 minute install per endpoint
Key Person: Ethan Couch, Apple Support
Successful Criteria: Physical backups are enabled
(Optional: Cloud backups are implemented for mobile devices)

Physical/Logical Security:

Currently the router/modem is not located in a safe and central location. The router should be kept in a secure room away 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 router will be moved to a more central location to allow easy configuration and optimal wireless performance. Proper controls will also need to be implemented on the router-side in order to accommodate for a DNS Sinkhole (Pihole- hosted on Dell R620 Server) and inbound/outbound traffic rules.

Resources: 120 minute install
Key Person: Ethan Couch
Successful Criteria: Router is properly configured; DNS Sinkhole is introduced to the network via Home Server.

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.

- *Download and install Malwarebytes on other unprotected devices*
- Consolidate Manuals and other related tools/equipment
- *Purchase G-Drive external 1TB hard drive*
- Download and install all relevant updates for Windows and IOS devices
- Set inbound/outbound traffic rules through router
- Implement firewall rules through Promox VE

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

Task	Start Date	End Date	Implementor	Rollback Plan	Status
Enable Firewall rules and implement Proxmox VE Firewall	2/26/23	TBD	Ethan Couch	Set back Firewall rules to default	Pending
Implement Cloud Data Backup solution for all devices	2/26/23	TBD	Ethan Couch	Buy low-cost external drives for all desktops/laptops.	Pending

Ensure Updated Systems	2/26/23	TBD	Ethan Couch	None. Updates are time-efficient and priority.	Half-Completed
Strengthen Router Security	2/26/23	TBD	Ethan Couch	Router configuration is restored to default. DNS Sinkhole plan is scrapped.	Pending
Install AV on Respective Devices	2/26/23	TBD	Ethan Couch	Windows Defender is enabled and used as the sole antivirus solution across devices.	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 configured properly within the next two weeks.

The endpoints themselves however have windows implemented accounts with passwords and/or 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. Even further, Bitwarden will be properly implemented on all systems as a browser-based extension.

2.5.1 System Security Features

- Passwords
- Operating System Updates
- Nessus Vulnerability Scans
- Pihole DNS Sinkhole
- Malwarebytes antivirus
- Proxmox VE and Eero Firewalls

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. This will likely be implemented through powershell on Windows devices.
- All drives must be securely erased or destroyed if they are being sold or removed.

2.6 Open Issues

A few issues that need to be addressed later are:

1. Ensure MFA across all devices, and ensure updated AV presence
2. Naming conventions of endpoints
3. Lack of data backup solutions for 80% of devices
4. Implement configurable firewall solution across VMs

Milestone 3: Protect Your Network (Network Architecture)

3.1 Overview

As previously referenced in Milestone 2 (section 2.1), the network will undergo adjustments in the form of OS upgrades, physical security measures, and the installment of secure remote access tools and firewalls. Additionally, the outstanding issues of lacking backup solutions and MFA implementation will be examined and mitigated within Milestone 3 of this document.

Much of the software existing on the devices within the network, especially within the cluster of mobile devices, is outdated. Host-based software will be updated, and physical security measures will be addressed by heightened authentication procedures and superior placement of network devices.

3.2 Facilities and Network Enclaves

For the purpose of this network plan, the facility can be considered as residential- within a 2-story home. Most of the network endpoints are contained within the living room and Study Room-1 (belonging to Ethan Couch). There are no enclaves or subnets that resemble that of a DMZ within this network. The facility lacks physical security measures; this will be mitigated by placing routers in locations that are out of plain-sight, and placing unused network devices within a locked filing cabinet. Additionally, a digital PIN-based lock will be utilized at the front door of the residence to limit physical access to the facility.

3.3 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, and/or the sensitivity of the data they contain:

Eero Pro 6 router (Provides external Internet connection for all devices on the LAN. Redundancy is provided for through the existence of a second duplicate of the router that is currently being used as an extension of wireless coverage. If need be, this device will act as a backup.)

Homelab/PowerEdge Server (This server demarcates the administrator's (Ethan Couch) consistent access to various virtual machines used for testing and productivity within the realm of cybersecurity research and academic work. For this reason, if this asset were compromised in terms of availability or integrity, the functionality of the network would be drastically compromised).

Desktop-1 (The custom-built computer belonging to Ethan Couch contains critical information in the form of projects, documents awaiting completion for employment, as well as many virtual machines used to complete academic projects).

In the event of compromise, all PC's and Laptops have been backed up to an independent 1TB hard drive. For mobile counterparts, Apple's ICloud storage solution is utilized.

3.4 Choke Points On This Network

Within the scope of the network plan, a choke point will be defined as an entity presenting the greatest risk to critical network assets/devices and the effectiveness of data transmission within the network as a whole.

With this in mind, the choke points of this network are the Eeros Pro 6 Router, along with the Dell PowerEdge Server. To remediate these threats, a redundant router is utilized and placed in an inaccessible location. Additionally, the Proxmox VE firewall will be implemented on the home server in order to consolidate and protect traffic between Host and VM nodes. Physical access of the server will require a complex password, along with requiring the user to supply a security key in order to gain access to the server through its garage location.

3.4.1 Single Points of Failure

To reiterate, the choke points and single points of failure within this network are largely the same. The router is the prime candidate for a single point of failure, and this will be protected against through the steps addressed above.

3.5 Legacy Systems

The sole legacy system within this network is Desktop-3; the outdated HP Pavilion desktop was upgraded to a secure version of the Windows 10 operating system, in which Windows Defender and Malwarebytes was installed to enhance security.

3.6 Plan Document Updates

In the case of architectural changes to the current network enclaves or choke points for this network, it will be the responsibility of Ethan Couch to update this milestone to reflect such changes. This will be performed at the identified weekly cadence (every Monday).

Milestone 4: Reach You Network (Device Accessibility)

4.1 Overview

This section details the measures that have been enacted to ensure authoritative access and administration of devices on this network. These changes apply to all PCs, laptops, routers, mobile devices, and server(s) within the network.

4.2 Accessibility and Administration

4.2.1 Personal Computers

All personal computers are scattered between the first and second floors of the residence, with most of the PCs existing within Study Room-1 and the Living Room. In this sense, Study Room-1 can otherwise be considered the home office in which access to all of the PCs on the network will be enabled. Desktop-1, the most critical PC asset within the home office runs an updated version of Windows 10 with malwarebytes and Windows Defender installed. The same is true for Desktop-2 and Desktop-3, and there is only one administrative account on each of these PCs that is protected by a complex password on each machine. Further, these passwords are stored using the Bitwarden service across all desktops, which uses an equally complex master password to provide its password managing services. Modification/viewing this password requires the presentation of a security key which the administrator (Ethan Couch) of the network has access to, along with a duplicate backup. Passwords will be changed monthly, and password history will be notated in the locked filing cabinet that lies in the Garage.

Furthermore, all default and user accounts on these PCs will be hardened with Windows Advanced Firewall protection and Malwarebytes. Password policy is configured on a user-group basis such that passwords must be changed on a monthly basis, and require the usage of special characters, and alphanumeric characters of varying case sensitivity. Windows automatic updates are enabled on each computer and MalwareBytes is configured such that a user is unable to disable it without administrative rights.

Guest access to a PC is constrained to one guest account that is available on Desktop-3; this desktop is at an isolated physical location at Study Room-2, which is away from the home office, and the majority of network devices that contain more critical information. In this sense, accessibility and availability has been provided for, while maintaining concepts of least privileges and separation of duties within the network.

4.2.2 Laptop Computers

Following the administration procedures that apply to personal computers, all laptops are covered by Windows Defender and MalwareBytes AV systems. Additionally, the same account-based constraints and password policy applies to laptop devices that are located in the home office and living room. Guest account access is not permitted through any laptop device.

Furthermore, all laptops and personal computers are coupled with hard drive backups. which are stored in the Garage filing cabinet when not in use due to active backup. The hard drive backups are expected to be utilized every week to perform consistent data backup for each endpoint. Due to it's frequent travel outside of the residence, access to Laptop-1 requires the presentation of the aforementioned security key device (Yubico Authenticator App & Security key) whenever attempting logon to the laptop. To allow for access of the home network while outside the LAN, a GlobalProtect VPN will be installed and configured on this system to allow access to the protected subnet.

4.2.3 Mobile Devices

For all of the 3 IPhone mobile devices, the MalwareBytes mobile application has been used to act as an antivirus solution. Additionally, all mobile devices have been updated from requiring PIN based authentication, to instead require a complex password that is known to the user. As of the revision and implementation of Milestone 4, a VPN solution has not been configured for any mobile device; this will likely not change, due to the volatile nature of these devices, and their frequent travel outside of the residence. Because compromise of these devices is most likely, it would be unwise to have a ready-to-go VPN option which allows the user to connect back to the home network.

4.2.4 Homelab/Server

The Dell PowerEdge R620 Server has its access limited through its placement in a garage location that is well-lit, with the garage door never being left open. The server rests on a server rack that houses a MicroTek Switch and monitor for terminal access. Terminal access to the server is protected by a password and the aforementioned security key. Through the home server, one can access the firewall-protected node of VMs which are hosted by the server. The desktop/laptop/mobile endpoints are not accessible through this server. VPN access to this server will be accounted for using an OpenVPN container that will be setup by following Proxmox VE documentation.

4.3 Remote Administration

Remote administration is important given the scale and segmentation of the network. Remote administration for all laptop and desktop devices is provided free through the TeamViewer and Remote Desktop services. TeamViewer provides for remote administration at a heightened level of security; it utilizes the RSA algorithm as a form of end-to-end access encryption. Remote desktop allows remote access to all respective Windows devices, although this form of access is limited to a web account which requires user authentication in order to proliferate to any one remote computer.

As stated above, remote administration is not currently possible through mobile devices, and there are no immediate plans to alter this.

4.4 Physical Security

As described in Milestone 3, physical security is provided for by limiting administrative actions to the home office (Study Room-1). Standalone devices are generally placed out of sight or easy access, and confidential information is stored in a filing system. Additionally, routers are out of common sight, and the main entry point to the residence (front-door) is protected by a PIN-based digital lock. The router choke point is provided redundancy by the existence of a clone.

4.5 Automating Administration

Automated administration has not been fully implemented within the network, although this feature would greatly benefit the enforcement of password and update policies across respective devices.

To name a few implementations of this process, automated updating of Windows devices will be put in place, along with automatic updates for Windows Defender and MalwareBytes applications. For the home server, cronjobs may be utilized in order to provide for consistent uptime of servers that are executed upon login to respective VMs hosted by the Proxmox VE.

4.6 Administrative Tools

Password policy configuration has been specified using the Windows 'Local Security Policy' interface. Additionally, the Yubico USB-C security key has been used to access critical/administrative assets within the network. Two of these security keys are in the administrator's possession, one of which serves as a redundant backup. This key is coupled with the Yubico Authenticaion App to provide further security to cloud accounts such as Google and Amazon. A web account serves as an administrative account from which Windows machines can be remotely accessed through the Remote Desktop Service.

4.7 Plan Document Updates

In the case of policy or configuration changes regarding administration and remote access for this network, it will be the responsibility of Ethan Couch to update this document to reflect such changes. This will be performed at the identified weekly cadence (every Monday).

Milestone 5: Control Your Network (User Access)

5.1 Overview

This Milestone serves as clarification and specification of access control procedures that have been implemented to secure user behavior within the network. As a result, this Milestone reiterates much of what was detailed in Milestone 4 of the network plan.

5.2 User Accounts

As previously stated, the user access model resembles that of a least-privilege model.

Regular user activity will encompass using productivity tools and suites, browsing the internet, playing games, using communication platforms, etc..

The local admin accounts contained on each device will be owned and maintained by Ethan Couch (administrator), and used only when necessary. They will not be used for everyday use, and Internet access through these accounts will be limited, wherever possible.

In the case an end-user needs to perform a privileged action, the administrator will review the request, and use administrative privileges to satisfy the request if it will not cause risk within the network.

Each machine is provided will approximately 3 user accounts, which allows easy temperance of user permissions and review of user behavior.

5.3 Privileged accounts

Privileged administrator accounts on the network will be used strictly for network and computer administration. The admin account is not to be used for general purpose computing, specifically web browsing and email access, unless this is necessary to enact configurations of certain services. This is to help prevent phishing attacks that can result from accessing email attachments or the download/execution of malicious code on mobile or static systems. As an example, Powershell access will be limited to administrator accounts.

5.4 Least privilege administrative model

Growth of the network plays into the PowerEdge Server that will likely be used to perform automated management of resources on the network. Access to this server is highly limited; only those with the respective security key are able to access this critical device.

To further the implementation of the least privilege model, default groups and users will only have the functionality to perform activities along the line of everyday use. Policy adjustments, the addition of user accounts, accessing network devices, and changing passwords is limited to users with administrative privileges.

5.5 Users Installing Software

There are currently no users on this network that have elevated/privileged accounts with the exception of the designated admin account. This prevents all users from having the ability to install software without the approval and assistance of the administrator. Mobile devices will restrict the download of malicious software at the discretion of the user; with the approval of the device owner, restrictive controls will be set up on the IPhones to ensure certain types of software is not downloaded.

5.6 Expiration Dates On Accounts

While passwords are set to expire for accounts, the accounts themselves will not be set to expire. Allowing accounts to expire will cause unnecessary overhead in terms of retaining configurations of user accounts on each device. Instead, creation or deletion of accounts will be supervised manually at the discretion of the administrator.

5.7 Plan Document Updates

If there are any changes or additions to the users of the network, it will be the responsibility of Ethan Couch to update this milestone to reflect such changes. This is to be performed within a week of the changes, ideally on a Monday.

Milestone 6: Manage Your Network (Patch Management)

6.1 Mode of Patch Delivery

One of the most promising options for patch management would be to have a central patch management solution that automatically rolls out distributed patches across the network. Though this idea received ample consideration, it has been concluded that patches across all devices will be conducted manually. Given the different operating systems across network devices, the configuration overhead of such a solution, and the likelihood of failure with a central patch management solution, it will not be optimal for for the long-time operation services, virtual machines, and host machines within the network.

6.2 Patch System Implementation

In any case, it would certainly be favorible if the network administrator were able to receive automated notifications of pending updates across machines. An implementation of this feature will be attempted using a mail server on the Dell PowerEdge home server as a collection point. As the network administrator becomes notified of important updates, it will be at the administrator's discretion that manual update installation will occur. For future Linux devices and existing UNIX-based virtual machines, patches will be applied using the standard package management CLI tool. This tool varies between distributions (Yum, Snap, APT, etc.) On the other hand, the standard Windows Update Service will be used for all Windows 10 and 11 devices. Regarding Windows devices not within the administrator's direct ownership, automatic updates will be preferred so as to protect against user negligence. Applications that have the potential for misuse or exploitation will be updated independently within a virtual environment or sandbox. This detail will prevent the exploitation of custom scripts or vulnerable plugins that could lead an attacker to proliferate across host machines or the network as a whole.

6.3 Patch Policy

To provide integrity to the patch management process in place of a central patch management solution, patch processes/policies will be documented and explained by the network administrator (Ethan Couch). This will ensure that all users within the network are aware of the importance of patch management and version control across applications. In general, updates will be conducted during a period of low activity every Sunday. This policy will be exceeded depending on the severity of updates (a critical operating system update would need to be installed as soon as possible). If Nessus is able to identify misconfigurations across devices with a CVSS score of 7 or higher, administration attention is immediately required to the offending device.

6.4 Order of Priority

The priority of application updates will fall second to operating system updates, and will be conducted during a period of device downtime, one day after release. In the case that updates to network devices such as the routers are needed, updates will be staggered so as to ensure no downtime is incurred. The redundant Eero router will be used when the primary router is being updated, and so on. Updates to routers or switches will rank third in priority when the administrator is tasked with performing a multitude of patches within a limited amount of time.

Milestone 7: Manage Your Network (Baseline Management)

7.1 Virus Scanning/Intrusion Detection

In order for the network to be secure up front, proper baselines need to be established for each type of device within the network. Proper baselines within the network enable an administrator to more quickly detect abnormalities in traffic or endpoint behavior within the network. To this effect, vulnerable/virus scanning is an important facet of a secure network, as it allows an administrator to proactively evaluate anomalous traffic or application execution within a network.

To account for virus scanning and intrusion detection, Tenable's Nessus Vulnerability Scanner is installed on the Dell PowerEdge home server. Using Nessus, the administrator (Ethan Couch) is able to manually engage in vulnerability scans or virus sweeps across all endpoints within the network. On the other hand, the network administrator will configure Nessus to execute daily vulnerability scans to report the status of the network and it's executable content. Nessus condenses all of these functions into a web application interface; the Nessus web application interface is accessible through a dedicated virtual machine within the homelab's Proxmox VE.

7.2 PED Management

Not to be forgotten, is the importance of considering PEDs (portable electronic devices) as vulnerable devices in any data-bearing network. To inform the approach to securing the use of these devices and their appropriate permissions within the network, the network administrator followed the recommendations contained with a Department of Homeland Security document titled '*The Risks of Using Portable Devices.'*

In short, the Department of Homeland Security article discusses the risks associated with using portable devices ranging from smartphones, tablets, and laptops, to portable audio players and thumb drives. Due to the frequency at which data contained in these devices is in-transit, these devices are culprit in increasing the risk of data loss, data exposure, and network-based attacks. To raise an example, if an attacker is able to infect a smart device when it's user leaves the device at work for just a few minutes, that device can easily be taken home to a secure network in which it can perform reconnaissance at the discretion of the infiltrator on otherwise secure endpoints. Even further, if a compromised device is allowed to infect a single node within the network, the whole network can fall victim to an attacker via privilege escalation and lateral movement strategies.

Ultimately, in order to counter the dangers imminent with the smartphones and laptops existing within this document's network, Malwarebytes has been installed on all PEDs, confidential data has been limited on PEDs, and the AutoPlay and AutoRun Windows features have been disabled on respective hosts.

As previously noted, all mobile devices are accompanied by a mobile version of Malwarebytes in order to strengthen the PED's defense against viruses. Additionally, in the sense of remote administration/VPN configuration, smartphones have been severed from the home network; implementing a way for these devices to connect to the home network (and especially the home server) using a VPN or remote administration service would pose too much of a security risk to the internal network. Even further, the storage of passwords or confidential information regarding the makeup of the home network on mobile devices has been discouraged amongst all owners of these devices.

For laptops, the AutoRun and AutoPlay components have been disabled. The reasoning for this action stems from the nature of these components in deciding what actions a system will take when a drive is mounted to the Windows device. In the case that a laptop within the network was gained temporary access by an attacker, the attacker should not be able to upload malicious media to cause unwarranted system calls or command execution.

7.3 Executable Content Restrictions

In order to establish an effective network baseline, all applications must be met with a baselining process which denotes the intended behavior and status of all installed software/applications. Of course, all installed applications must minimize the attack surface of a network, and must be defended against trivial exploits.

Seeing as the network administrator frequently downloads/uploads content to the internet, and will often execute scripts when testing projects related to independent research or academic work, content execution must be monitored. To ensure that downloaded content is not of malicious nature, sandboxing using the ANY.RUN tool will be utilized for untrusted software/applications. Additionally, across all devices that the network administrator has ownership of, execution restrictions will be administered so that only administrator accounts are allowed to launch executables. In other words,a ll files of executable content types (.BAT, .EXE, .COM, .ps1, .APK, .JAR, .XLM, etc.) will be required to 'run as Administrator.'

In order to establish a prospective baseline of the network software, the following approved applications are recognized across potential network devices:

- Microsoft Office Suite (provided via academic subscription, necessary for collaboration on school assignments).
- Slack (used as an academic and professional communication platform).
- Microsoft Teams (used for interviews, communication with classmates).
- MalwareBytes free trial
- Windows Defender
- Nessus
- TeamViewer (enables secure remote administration for appropriate hosts).
- Wireshark (used for analyzing network traffic captures, diagnosing network issues, and confirming network switch/router functionality).
- Remote Desktop
- OpenVPN (required for access to homelab nodes)
- Visual Studio Code (preferred IDE for software projects)
- VMware Workstation (preferred virtualization environment for cybersecurity research and exploit testing)
- Google Chrome (preferred browser)
- Steam
- Yubico Authenticator (used for security key authentication for XPS 9510 laptop)

7.4 Baseline Considerations

In order to properly complete the baseline management process for the network, problem scenarios across the following subjects have been identified and met with prospective responses:

7.4.1 Password Compromise

All passwords related to web applications will be stored within Bitwarden, a secure and open-source password manager. This will be secured by a master password or security key per the discretion of the network administrator. Additionally, system passwords will be required to be changed on a basis outlined within the local policy editor of all Windows machines.

7.4.2 Device Integrity

To ensure that none of the devices are compromised, modified, or repeatedly breached, weekly AV scans are scheduled by the administrator every Friday, so as to not disrupt regular network proceedings.

If any device is suspected of a breach, the device will be wiped, and will be restored using its respective external drive. Of course, these external drives will be reviewed to ensure the incoming backup is free of malware.

For detailed information regarding this process, see section 8.2 of the network plan.

7.4.3 Automatic Reboots

In order to minimize disruptions across devices, automatic reboots will not be enacted. In general, devices will be turned off when not expected usage for more than 4 hours, and will be manually rebooted as needed.

Milestone 8: Document Your Network (Network Expansion, Incident Response, & Disaster Recovery)

8.1 Incident Response

This milestone proactively designates strategies and guidelines that must be followed in the event of a security misconfiguration, user behavior anomaly, or network breach.

The administrator will spearhead their incident response efforts with a determination of how the network incident occurred. This involves assessing and tracing the exploitation vector, level of damage, and motives behind the incident.

After this step is completed, the network administrator will determine an isolation strategy for the affected machine or user entity. If the attack is likely to proliferate to other network devices or accounts, the affected entity will be disconnected/eradicated from the network until the threat is purged.

Consequently, a compromised device must undergo a disaster recovery procedure (see section 8.2), and recovered using it's accompanying external hard drive. It should be noted, this is only feasible if the external hard drive is found to be free from the compromising data.

Once an affected device is deemed to be clean and hardened against the possibility of a related infection in the future, the device will be reintroduced to the network with heightened vulnerability scanning and constricted user permissions (account disabling, if applicable) on the device.

8.2 Disaster Recovery

Given that an anomalous incident is deemed to be a true positive occurrence, the following procedure will be adhered to in order to quickly regain control of the affected asset:

1. First, the administrator will assess whether data can can be extracted or recovered from the device. This involves the administrator determining what drive(s) were affected by the incident, and what kind of memory acquisition tool can be used to examine the state of intact data.
2. Recoverable data should be extracted to an unaffected storage device. This will be useful in rebuilding the affected device to it's previous baseline.
3. In the event that no recoverable data is found on the device, and/or a physical failure of the storage media has occurred, a replacement drive must be issued as soon as possible.
4. The affected device will be restored using it's respective backup device. This will be an external hard drive or cloud storage solution.
5. Missing applications or services should be installed to promote the device to it's baseline level of security and productivity.

Overall, the presence of various forms of redundant drives and media backups will prove crucial in the event of a network incident. It is the main objective of the network administrator to have the affected device restored to a secure baseline under an RTO of 48 hours. This recovery time objective has been evaluated to be the most appropriate metric for stating how long a network of this caliber should remain inoperative.

8.3 Network Expansion

A key component of the network's documentation is network expansion. This section details the general procedures that will be followed in the event that the administrator intends to introduce new users, devices, or policies to the network.

8.3.1 User Addition

For the most part, the addition of new users is a scenario that is already accounted for in Milestone 5 of this document. To reiterate, new users will be added to host machines at the discretion of the administrator and the valid request of a resident or guest. Before a new user account can be introduced to an endpoint, the user responsible for the account must have specific privileges and storage partitions assigned for them on the respective device, and they must also be informed of all policies that govern the use cases of this network.

8.3.2 Hardware Addition

First of all, the addition of a new laptop, computer, or related IoT device to the network will require the network administrator to setup the device in an appropriate location. This location must have reasonable proximity to a router so as to promote connectivity, yet must not intrude upon the administrator office that houses Laptop-1, Desktop-1, and other high priority devices. The new device must comply with the DHCP process to be assigned an IP address within the network. Additionally, the device must be scanned for malicious media, and must have its applications/services cross-examined with the list of approved applications (see section 7.3). Upon determining that the new device has connectivity within the network, the administrator will document the system details of the device, and add the device as a target node of the Nessus vulnerability scanner. This will ensure the newly-introduced device is monitored.

8.3.3 Policy Addition

The efforts of the administrator to secure the network will be ongoing and proactive. It will be the responsibility of the administrator to modify existing policy or add new policies governing the usage of devices or accounts within the network depending on the evolving cybersecurity landscape and threat environment. The difficulty of this task comes with designing a selection of policies that are robust and protective of the network, yet lax enough so as to not suffocate the effectiveness and functionality of the network.

APPENDIX

APPENDIX A: Manageable Network Implementation Plan Approval

The undersigned acknowledge that they have reviewed the Ethan Couch 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: Ethan Couch Date: 2/26/23
Print Name: Ethan Couch

Title: Network Administrator
Role: Project Manager

APPENDIX B: REFERENCES

The following table summarizes the documents referenced in this document.

Document Name	Description	Location
Apple ICloud Documentation	Provides information about pricing plans for purchasing ICloud storage.	https://support.apple.com/en-us/HT201238
Microsoft OS Builds	Lists OS builds and fixes to new windows updates	September 30, 2021—KB5005611 (OS Builds 19041.1266, 19042.1266, and 19043.1266) Preview (microsoft.com)
Proxmox VE Firewall	Proxmox VE Firewall provides an easy way to protect your IT infrastructure. Here is documentation pertaining to the implementation of firewall rules and other features included with the Proxmox hypervisor solution.	https://pve.proxmox.com/wiki/Firewall
G-Drive 1TB Drives	Amazon page displaying relative pricing for 1TB of storage on an external drive.	https://www.amazon.com/G-Technology-0G10264-G-Drive-Mobile-Portable/dp/B07DK2LPDD
Nessus Vulnerability Scanner	Web-based vulnerability scanner that allows identification of vulnerabilities based on a variety of preset scans. GUI-based.	https://www.tenable.com/lp/campaigns/22/try-nessus-multiprdct/free-trial/?utm_campaign=gs-{1877131155}-{69726218533}-{537515897960}_00026641_fy23&utm_promoter=tenable-hv-brand-00026641&utm_source=google&utm_term=nessus&utm_medium=cpc&utm_geo=amer&gclid=CjwKCAiAxvGfBhB-EiwAMPakqn7N1Ku-tEAkb2s-okSKS3xKpPAkJRB8ZgvSWTKkHjsfm--4faV-0hoCiNoQAvD_BwE
Proxmox VE VPN Implementation	Provides information regarding the setup of an OpenVPN container using the Proxmox virtual environment	https://pve.proxmox.com/wiki/OpenVPN_in_LXC
MalwarebBytes AV	Provides pricing/device coverage information on MalwareBytes, a premier antivirus solution for mobile and desktop devices.	https://www.malwarebytes.com/business/pricing?gclid=Cj0KCQjw8qmhBhCIARIsANAtbofrkMcwruOtwKgmNIBPqzI7OyPmQ9VE9z-EqOyuxDibdMNmN6N-ItwaAhiFEALw_wcB
Yubico Authenticator App	Allows a physical security key to be used to provide heightened authentication security to compatible devices.	https://www.yubico.com/products/yubico-authenticator/

PED Informational Article	This document composed by the CISA informs one of the dangers of neglecting security mechanisms and policies surrounding portable electronic devices. This document was used to shape my perspective on how to handle data contained on laptops, smartphones, and any other devices in transit.	https://www.cisa.gov/sites/default/files/publications/RisksOfPortableDevices.pdf
RTO Informational	The article highlights the need for businesses to determine their RTO and establish a recovery plan accordingly. The article assisted in my conclusion of a well-planned disaster recovery strategy with a realistic RTO for this network.	https://www.rubrik.com/insights/recovery-time-objective

APPENDIX C: KEY TERMS

The following table provides definitions and explanations for terms and acronyms relevant to the content presented within this document.

Term	Definition
TB	Terabyte
OS	Operating System
VE	Virtual Environment
AV	AntiVirus
MFA	Multi-Factor Authentication
VM	Virtual Machine
DMZ	Demilitarized Zone
IDS	Intrusion Detection System
PED	Portable Electronic Device
RTO	Recovery Time Objective
CVSS	Common Vulnerability Scoring System

APPENDIX D: System Hardware Inventory

Name/ ID	Type	Model/ Version	Physical Location	Equipment Owner (Person or Dept)	Maintenance Contract? Y/N	Maintenance Contact Point	Maintenance Type/ Level of Coverage	Maintenance Period Expiration Date	Required Licenses

Desktop-1	Desktop Computer	N/A	Study Room-1	Ethan Couch	N/A	Ethan Couch	Minimal	N/A (part-by-part warranty)	None
Desktop-2	Desktop Computer	Alienware Aurora r5	Bedroom-2	Addison Couch	Y	Ethan Couch	Minimal	5 years (expired)	None
Desktop-3	Desktop Computer	HP Pavilion	Study Room-2	Wesley Couch	Y	Wesley Couch	Minimal	expired	None
Laptop-1	Laptop	XPS 9510	Study Room-1	Ethan Couch	Y	Ethan Couch	Minimal	1 year	None
Laptop-2	Laptop	HP Spectre	Living Room	Lisa Couch	Y	Ethan Couch	Minimal	1 year	None
Iphone 13-1	IPhone	Iphone 13-Pro-Max	Bedroom-1	Ethan Couch	Y	Ethan Couch	Minimal	1 year	None
Iphone 13-2	IPhone	IPhone 13-Pro-Max	Bedroom-2	Addison Couch	Y	Ethan Couch	Minimal	1 year	None
Iphone-M	IPhone	IPhone 12 Mini	Bedroom-3	Lisa Couch	Y	Ethan Couch	Minimal	1 year	None
Eero Pro Router	Router	Eero Pro 6	Study Room-1	Ethan Couch	Y	Ethan Couch	Medium	1 year	None
Redundant Eero Pro router	Router	Eero Pro 6	Living Room	Ethan Couch	Y	Ethan Couch	Medium	1 year	None
TV-1	TV	Sony Bravia	Living Room	Wesley Couch	Y	Wesley Couch	Minimal	1 year	None
HP6AA744	Printer	HP Envy 7800	Study Room-2	Wesley Couch	Y	Ethan Couch	Minimal	1 year	None
HOMELAB	Server	Dell PowerEdge	Garage	Ethan Couch	Y	Ethan Couch	Medium	2 year	None

APPENDIX E: System Software Inventory

Name/ ID	Type	Model/ Version	Physical Location	Equipment Owner (Person or Dept)	Maintenance Contract? Y/N	Maintenance Contact Point	Maintenance Type/ Level of Coverage	Maintenance Period Expiration Date	Required Licenses
MalwareBytes	AV	4.5.14	All devices	N/A	N	Ethan Couch	High	None	Malwarebytes Subscription (PC & IOS)
Windows 10	OS	22h2	Desktops (All)	N/A	N	Ethan Couch	Moderate	N/A	Windows Home License + Windows Enterprise License
Windows 11	OS	22h2	Laptop-1	Ethan Couch	N	Ethan Couch	Moderate	N/A	Windows 11 Home
iOS	OS	16.4	iPhones (All versions)	N/A	N	Ethan Couch	High	N/A	N/A
Windows Defender	AV	Windows 10 & 11	Desktops + Laptops	N/A	N	Ethan Couch	High	N/A	None (Free with Windows 10/11)
Remote Desktop	OS	Windows 10 & 11	Desktops + Laptops	N/A	N	Ethan Couch	Moderate	N/A	Windows 10/11 License
Proxmox VE	OS	7.2-1	Home Server	Ethan Couch	N	Ethan Couch	High	N/A	N/A

Teamviewer	Remote Administration	15	Desktops + Laptops	N/A	N	Ethan Couch	N/A	N/A	N/A
Yubico Authenticator	Authentication	3.0	XPS 9510	Ethan Couch	N	Ethan Couch	Moderate	N/A	Yubikey Compatible Security Key
Nessus Vulnerability Scanner	Virus Detection	10.2.3	HOMELAB (Dell Server)	Ethan Couch	N	Ethan Couch	High	N/A	Free License
VMware Workstation Pro	OS	17	XPS 9510, Laptop-1, Desktop-1	Ethan Couch	N	Ethan Couch	High	N/A	VMware license key

APPENDIX F: Milestone-1 Check-List

Checklist

Check **Yes** or **No**. If No, provide (or provide reference to) an **Explanation**. If explanation is acceptable from a risk management standpoint, check **Accepts Risk**.

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 Mondays 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: 2/26/23

APPENDIX G: Milestone-2 Check-List

Checklist

Check **Yes** or **No**. If No, provide (or provide reference to) an **Explanation**. If explanation is acceptable from a risk management standpoint, check **Accepts Risk**.

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 Monday		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 Monday 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: 2/26/23

APPENDIX H: Milestone-3 Check-List

Checklist

Check **Yes** or **No**. If No, provide (or provide reference to) an **Explanation**. If explanation is acceptable from a risk management standpoint, check **Accepts Risk**.

Yes	No	Explanation	Accepts Risk	Milestone 3: Protect Your Network (Network Architecture)
X		Not applicable, enclaves are recent within the network.	X	Have you identified and documented your current network enclaves?
X		Yes, high-value assets and choke points are elaborated upon.	X	Have you identified and documented the current high-value assets and choke points on your network?
X		The documentation will be updated on a weekly schedule.	X	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		Yes, re-evaluations will be conducted every month to ensure that the network most effectively protects high-value assets and contains damages. Trust relationships are reviewed every month to determine elimination of redundant accounts.	X	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		Yes	X	Have you gone over the points to consider for this Milestone?

Checklist date: 04/02/2023

APPENDIX I: Milestone-4 Check-List

Checklist

Check **Yes** or **No**. If No, provide (or provide reference to) an **Explanation**. If explanation is acceptable from a risk management standpoint, check **Accepts Risk**.

Yes	No	Explanation	Accepts Risk	Milestone 4: Reach Your Network (Device Accessibility)
	X	Documentation has been composed for secure access and administration of devices, yet not all documented procedures have been enacted.	X	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		Updates to access and administration will be provided to Milestone 4 as necessary.	X	Are you updating your device access/administration process and documentation as necessary?
X		Yes	X	Have you gone over the points to consider for this Milestone?

Checklist date: 04/03/2023

APPENDIX J: Milestone-5 Check-List

Checklist

Check **Yes** or **No**. If No, provide (or provide reference to) an **Explanation**. If explanation is acceptable from a risk management standpoint, check **Accepts Risk**.

Yes	No	Explanation	Accepts Risk	Milestone 5: Control Your Network (User Access)
X		About 90% of the accounts on the network are for non-privileged users. The remaining percentage are those with administrative privileges.	X	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* nonprivileged accounts? (Higher % is more secure)
X		Reviews of permissions and privileges will be conducted every month in addition to trust relationships. If deemed invalid, permissions will be removed as soon as possible from respective accounts. Approximately 50% of the elevated privileged accounts will be restricted to the performance of local configuration actions.	X	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		User permissions and accounts will be verified every month. If an unverifiable account arises, the account will be deleted/disabled within 3 days of discovery. Terminated users will have their accounts revoked as soon as possible.	X	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		All points have been considered for Milestone 5.	X	Have you gone over the points to consider for this Milestone?

Checklist date: 04/03/2023

APPENDIX K: Milestone-6 Check-List

Checklist

Check **Yes** or **No**. If No, provide (or provide reference to) an **Explanation**. If explanation is acceptable from a risk management standpoint, check **Accepts Risk**.

Yes	No	Explanation	Accepts Risk	Milestone 6: Manage Your Network, Part I (Patch Management)
x		See Patch Management sections (Milestone 6). Patch management strategies are outlined via attributes such as the type of device, and the priority of the device in the operation of the network.	x	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		It is accepted as the ongoing job of the administrator to continuously monitor the network and update endpoint and policy statuses as necessary.	x	Are you updating your patch management process and documentation as necessary?
x		Rubric and security considerations have been properly examined.	x	Have you gone over the points to consider for this Milestone?

Checklist date: 4/24/2023

APPENDIX L: Milestone-7 Check-List

Checklist

Check **Yes** or **No**. If No, provide (or provide reference to) an **Explanation**. If explanation is acceptable from a risk management standpoint, check **Accepts Risk**.

Yes	No	Explanation	Accepts Risk	Milestone 7: Manage Your Network, Part II (Baseline Management)
x		Approved applications have been documented, restrictions on execution of media have been recognized to be 70% within the network (administrator approval required for the majority of devices).	x	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, politicy outlines for adding an application to the approved list have been recognized to be within the discretion of the administrator.	x	Have you established and documented the criteria and process for getting an application on the approved list?
x		Baselines have been attributed to each network device to account for a healthy suite of software that distributes automated notifications concerning necessary updates.	x	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		Administrator regularly reviews compliance policies.	x	Are you updating your device baselines on a regular basis?

x		Yes, see second checklist entry.	x	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		All points have been exhaustively evaluated.	x	Have you gone over the points to consider for this Milestone?

Checklist date: 4/24/2023

APPENDIX M: Milestone-8 Check-List

Checklist

Check **Yes** or **No**. If No, provide (or provide reference to) an **Explanation**. If explanation is acceptable from a risk management standpoint, check **Accepts Risk**.

Yes	No	Explanation	Accepts Risk	Milestone 8: Document Your Network
x		The expected response in the event of a disaster is clearly indicated.	x	Are the procedures to rebuild servers and other important devices on your network fully documented and kept up to date?
x		Comprehensively covered in Milestone 5 and section 8.3.1.	x	Are the procedures for adding and removing users and systems from your network fully documented and kept up to date?
x		As mentioned before, the administrator will keep all administrative processes and network expansion initiatives within documentation.	x	As time permits, are you documenting all other administrative processes and procedures, and keeping them up to date?
x		All points have been considered.	x	Have you gone over the points to consider for this Milestone?

Checklist date: 4/24/2023