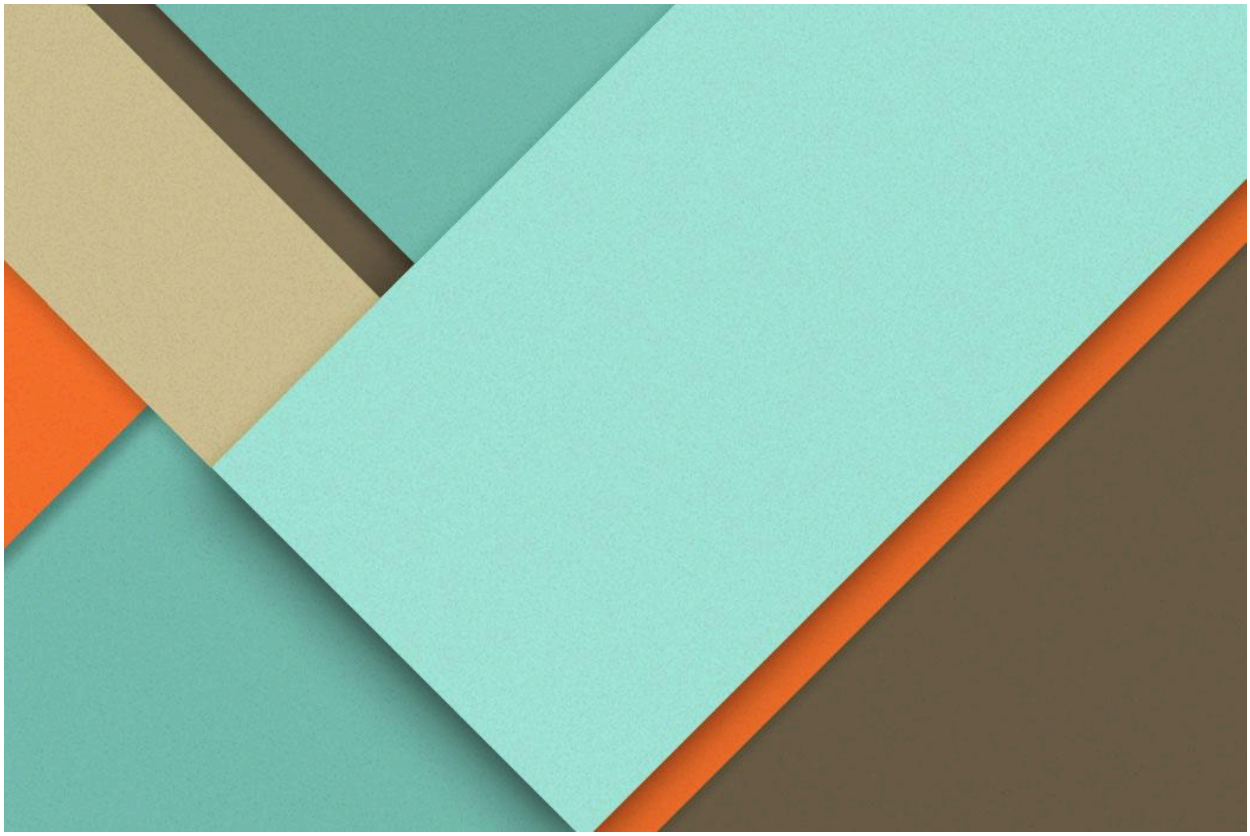


PERSONAL CYBERSECURITY AUDIT & AWARENESS TOOLKIT

29 SEPTEMBER, 2025

➔ PROJECT OVERVIEW

This project involved a comprehensive security audit of my personal system to evaluate its defensive posture and identify potential vulnerabilities. The audit utilized an open-source network discovery and security auditing tool, Nmap. Its full suite of tools was used first to map the network landscape, revealing all active devices on the network, identifying open ports, running services, and the operating system's fingerprint. This was followed by a vulnerability assessment which employed Nmap's scripting engine to pinpoint potential entry points for attackers. The findings from this audit were then used to implement critical security hardening measures on the system. Finally, the process and lessons learned were distilled into a cybersecurity awareness toolkit, designed to educate others on fundamental cyber hygiene practices.

RESOURCES

NMAP	
COMMAND PROMPT	
PORT SCANNER	https://canyouseeme.org/
CANVA	

➔ Scope

This section defines the boundaries of the security assessment, clarifying what was included and what was explicitly excluded.

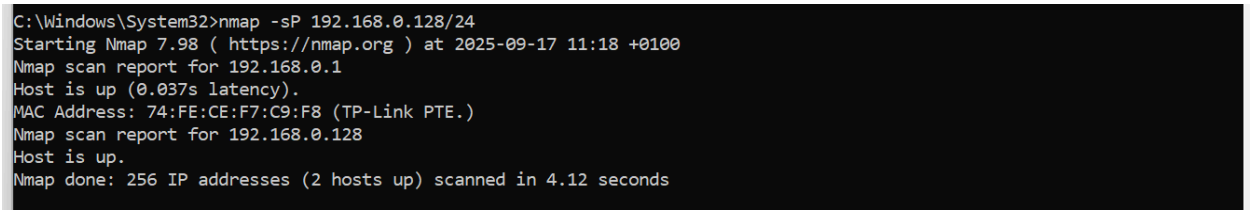
In-Scope	Out-Scope
• The assessment focused exclusively on the localhost (127.0.0.1) and the private network segment 192.168.1.0/24 to which the host belongs. • Actively identifying all live hosts and devices within the defined network range using Nmap's host discovery techniques (-sP)	• The assessment did not involve scanning or testing systems outside the authorized private network. • While services were identified, a detailed, line-by-line audit of application or operating system configuration files was beyond the scope of this initial assessment.

➔ Summary Of Nmap Scan Result

The Nmap scans provided a clear picture of the services running on my system and the ports they were using.

I. Task 1

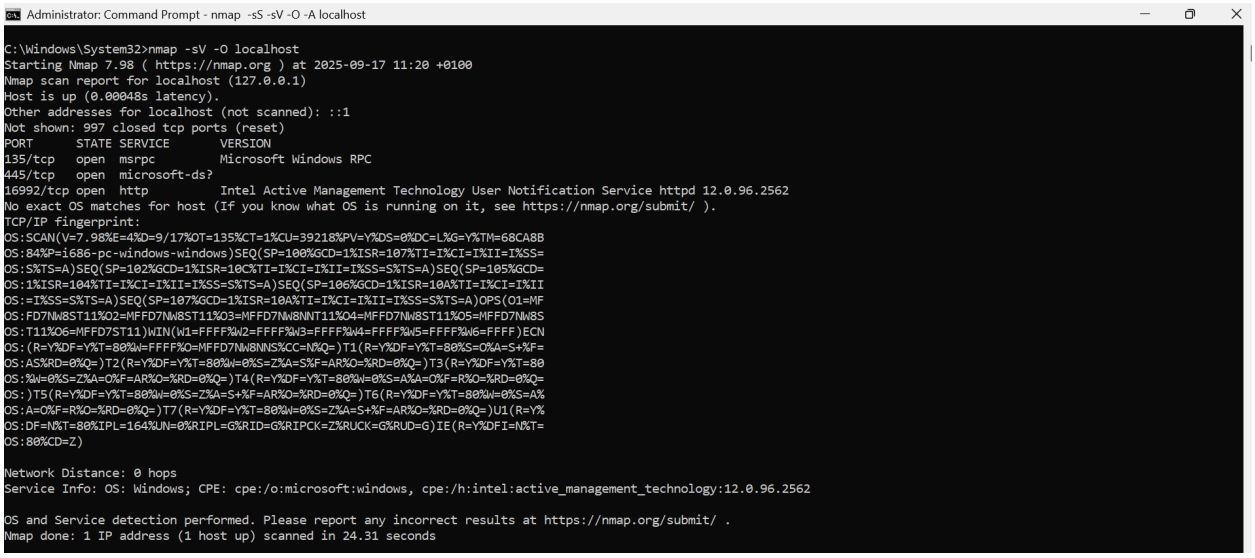
Device Discovery Results (-sP): The nmap -sP 192.168.1.0/24 scan was used for device discovery on my home network. The output listed my router, my computer, and several other devices connected to the network, including my smartphone. This step helped to visualize all connected devices, which is a critical part of a comprehensive security audit.



II. Task 2

Service & OS Detection: nmap -sV -O localhost: A service and OS detection scan was run against the target `localhost` (IP: 192.168.0.128). The following services and ports were found to be open

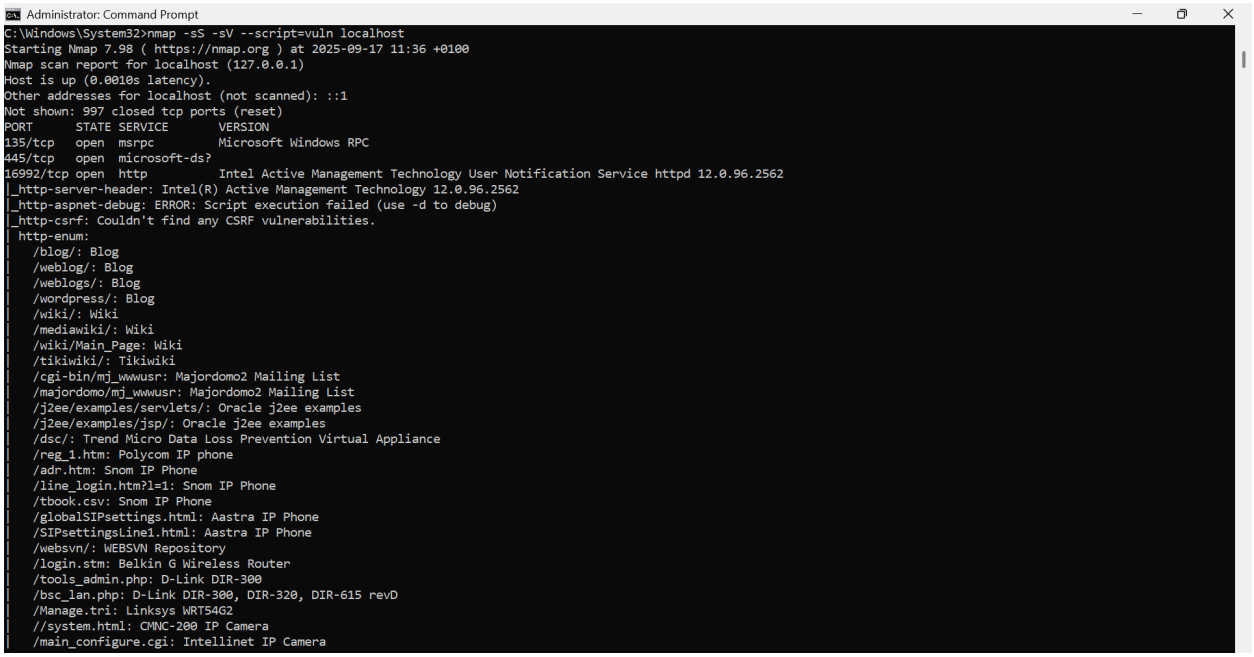
PORT	STATE	SERVICE	VERSION
135/tcp	Open	msrpc	Microsoft Windows RPC
445/tcp	Open	microsoft-ds	SMB(Server Message Block)
16992/tcp	Open	http	Intel Active Management Technology User Notification Service httpd12.0.96.2562

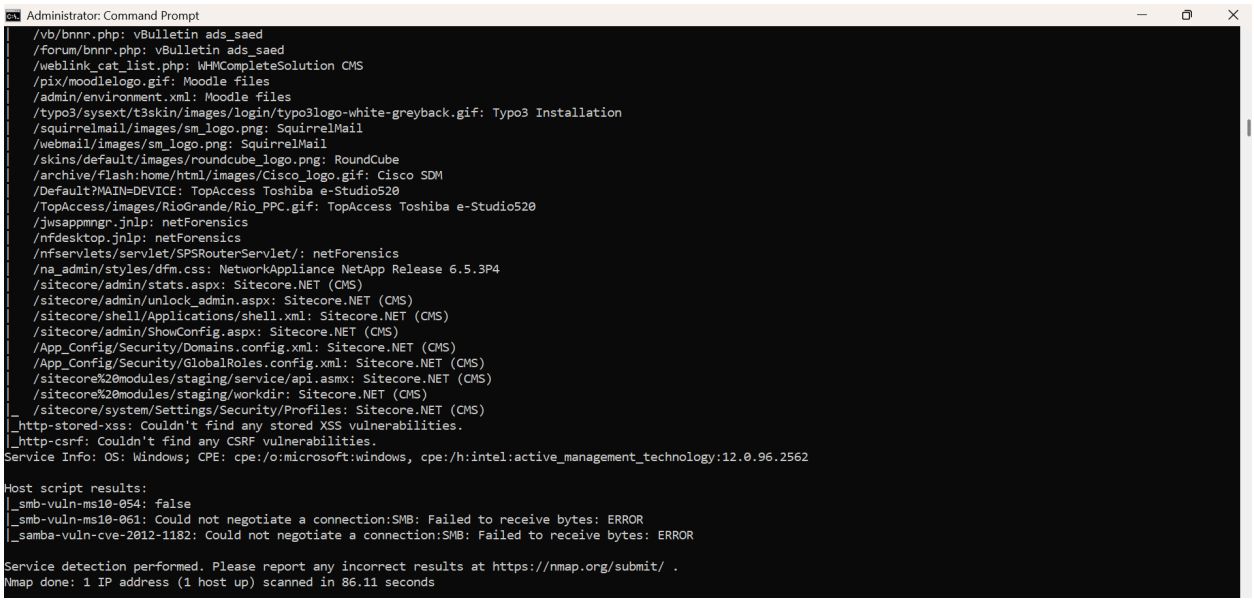


As shown in the screenshot above in the service info line the operating system was identified as Windows, the common Platform Enumuration identified the operating system fingerprint as Microsoft Windows and the hardware fingerprint as Intel active management technology.

III. Task 3

Vulnerability Check: The nmap --script vuln localhost scan identified a few potential vulnerabilities. While many of the identified issues were low-risk or related to known exploits that have since been patched, they still highlighted areas for improvement. Notably, the scan reported an issue with msrpc and an Intel Active Management Technology service. This prompted a deeper look into these services.





No major vulnerabilities such as CSRF, XSS, or SMB were identified during the assessment. The system demonstrates a good security posture in that respect. The vulnerabilities identified in the order of severity were:

1. **High Severity** – none found

2. **Medium Severity** – are exposed services that could be leveraged if misconfigured. **MSRPC** and **Intel AMT** service listening were identified.

3. **Low Severity** – none found

4. **Informational** – host discovery and open ports

- **MSRPC** – Microsoft RPC service is listening on the network. While not inherently a vulnerability, if unpatched or exposed externally, it can be exploited (historical example: WannaCry used SMBv1). Best practice is to restrict RPC access to trusted hosts.

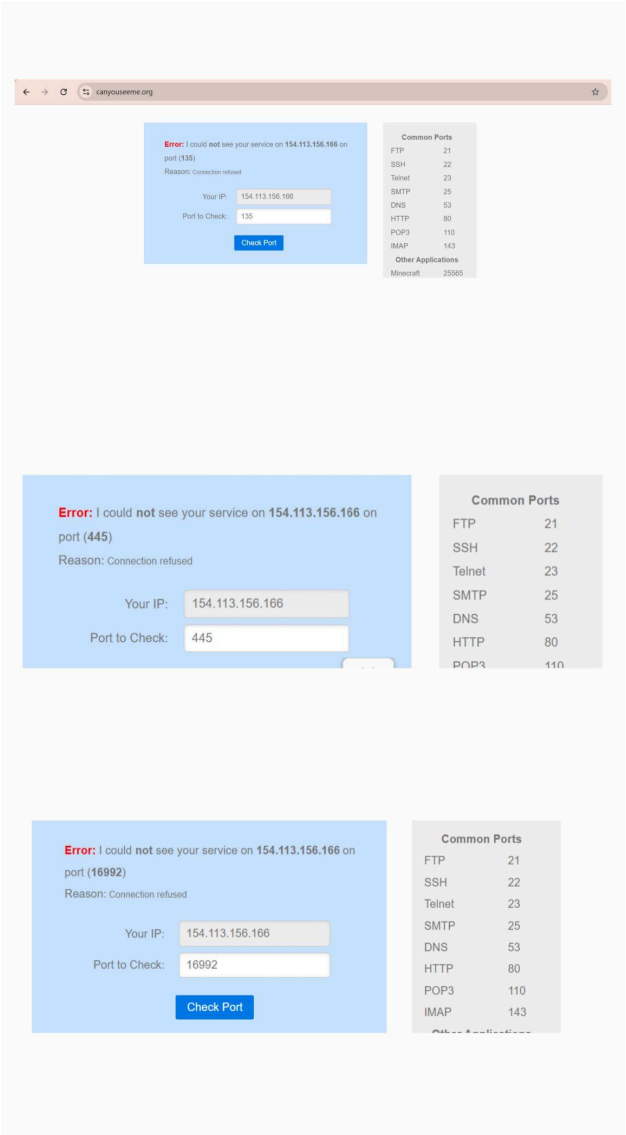
- **Intel AMT** – Part of Intel's Active Management Technology (remote management). If enabled unnecessarily, it could pose a risk of unauthorized access, especially if default credentials or old firmware are present. Recommend verifying if the service is required and disabling it if not.

➔ Security Improvements Applied

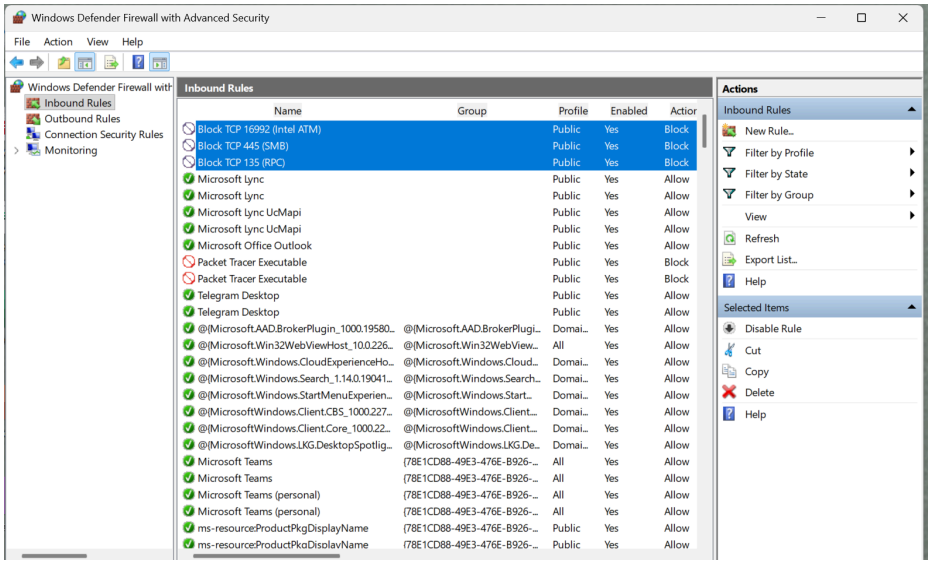
Detailed List of Changes Made

Based on the audit findings, I implemented several security improvements.

1. **Closed Unused Ports:** The Nmap scan revealed a number of open ports that were not essential for my daily use. Specifically 135/tcp, 445/tcp, and 16992/tcp. I checked these ports using an online port scanner to verify their status



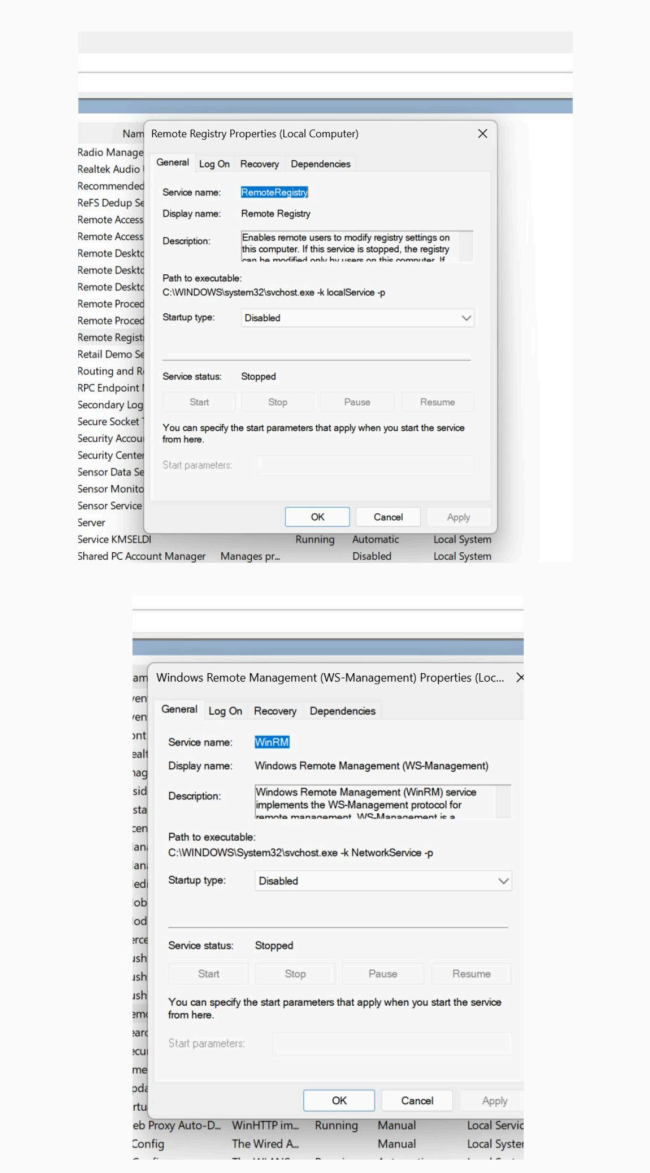
The screenshot above shows they are not externally exposed. To add a layer of security, I proceeded to configure the Windows Defender Firewall to block incoming connections to these ports. This was a crucial step in reducing the attack surface of my system.



2. **Enabled Firewall:** Although the Windows Firewall was enabled by default, I verified its configuration to ensure it was properly configured to block unauthorized connections.

3. **Updated OS and Software:** I ran a full system update via Windows Update, which installed the latest security patches. I also checked for updates for key software like my web browser and antivirus program to ensure they were running the most recent versions.

4. **Disabled Unnecessary Services:** I reviewed the list of running services and disabled some non-essential services that were running in the background like Remote Registry and Windows Remote Management.



5. **Enabled MFA & Password Manager:** I implemented Multi-Factor Authentication (MFA) on my most critical online accounts, including email and social media. I also adopted a password manager to generate and store unique, strong passwords for all my accounts.

➔ Challenges Encountered

The main challenge was understanding the specific services and their corresponding ports. The Nmap output, while detailed, required some research to interpret the function of each service and determine whether it was safe to disable or block. The msrpc service, in particular, required careful consideration to ensure I didn't disable a service critical to the proper functioning of my system.

Before/After Comparisons

- **Before:** My system had several open ports, some of which were not actively used. This provided potential entry points for attackers.
- **After:** By implementing firewall rules, I successfully closed all non-essential ports, significantly reducing my system's attack surface.
- **Before:** I was using a few repetitive and weak passwords for some non-critical accounts.
- **After:** With the password manager, I now use unique, strong passwords for all accounts, and MFA adds an extra layer of protection.

➔ Lesson Learnt

What Surprised You About Your System's Security?

I was surprised by the number of open ports on my system, even though I had not explicitly enabled them. It was a clear reminder that software installations and default settings can leave a system more exposed than one might assume. The existence of the Intel Active Management Technology service, which I was not aware of, also highlighted the importance of regular, in-depth audits.

New Knowledge Gained About Network Security

This project provided a practical understanding of network scanning and the importance of a layered security approach. I learned how to use Nmap not just as a tool for a specific task but as a general utility for network introspection. I also gained a much deeper appreciation for the role of a firewall in controlling network traffic and the necessity of proactive security measures.

How This Changed Your Security Awareness

This project has fundamentally changed my perspective on cybersecurity. I no longer view it as an abstract concept but as a hands-on, continuous process. I am now more mindful of the software I install, the passwords I create, and the importance of regularly checking for updates and reviewing my system's security posture.

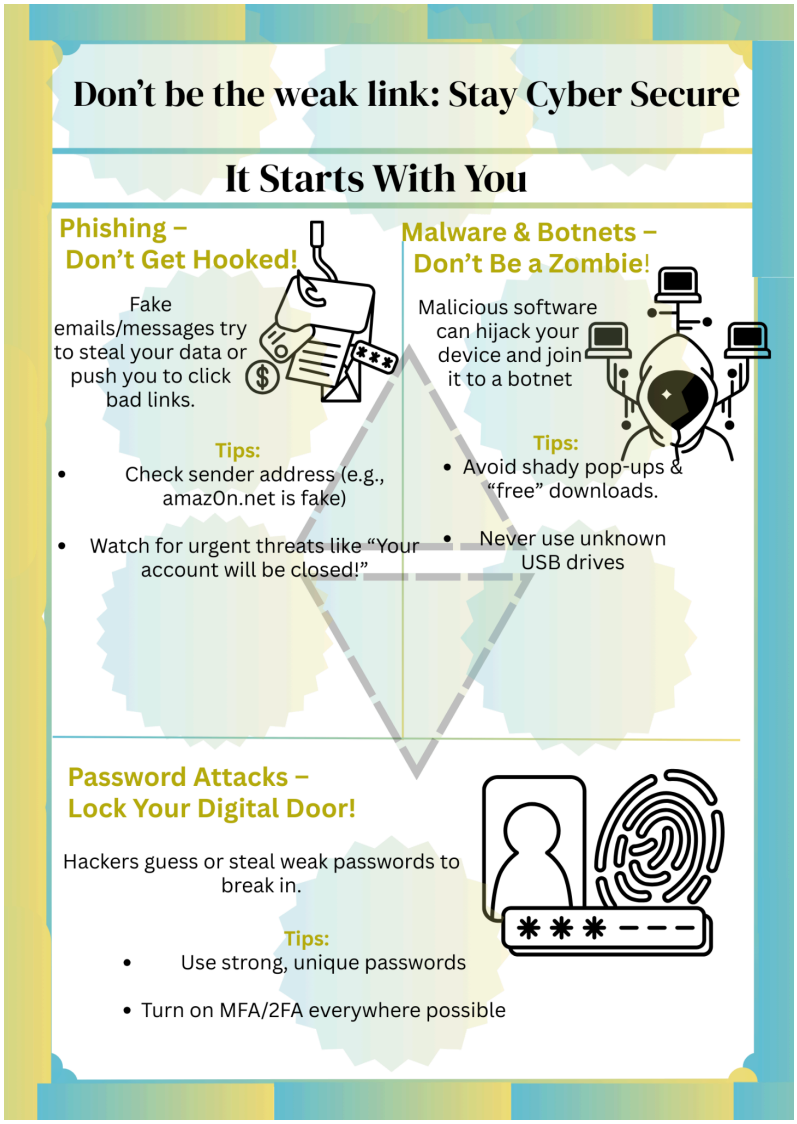
Future Security Practices You'll Implement

Moving forward, I plan to:

1. **Schedule Regular Scans:** I will run Nmap scans on a monthly basis to check for any new open ports or vulnerabilities that may have been introduced by new software.
2. **Continue Using a Password Manager:** I will continue to use a password manager to maintain strong and unique passwords for all my accounts.
3. **Stay Informed:** I will make an effort to stay informed about the latest cybersecurity threats and best practices.

➔ Awareness Poster

This cybersecurity awareness poster is aimed at the general public, providing simple and accessible information about three common online threats: phishing, malware and botnets, and password attacks. The poster explains each threat in clear, concise terms and offers practical safety tips, such as verifying sender addresses, avoiding suspicious downloads, and using strong passwords with multi-factor authentication. The intention is to promote safer online practices, increase awareness of cyber risks, and empower individuals to better protect their personal data and digital devices.



➔ Conclusion & Recommendation

Overall Assessment of Your System's Security

My system's security has significantly improved as a result of this project. It has moved from a state of passive reliance on default settings to one of active and informed security management. The audit identified and addressed key weaknesses, and the improvements have created a more robust defense against common cyber threats.

Recommendations for Others

Based on my experience, I would highly recommend the following to others:

- **Conduct a Self-Audit:** Use a tool like Nmap to get a clear picture of your system's security posture. It's an eye-opening experience.
- **Don't Rely on Defaults:** Never assume that your system is secure out of the box. Proactively configure your firewall and other security settings.
- **Use MFA:** Enable Multi-Factor Authentication on every account that supports it. It is one of the easiest and most effective ways to prevent unauthorized access.
- **Use a Password Manager:** Stop reusing passwords. A password manager makes it easy to use unique and strong passwords for everything.

Importance of Regular Security Audits

This project has reinforced the importance of regular security audits. The digital landscape is constantly changing, with new threats and vulnerabilities emerging every day. A one-time audit is not enough. Continuous monitoring and a proactive approach are essential to maintaining strong personal cybersecurity.