Project Team members:

Gamuchirai Muchafa CG/24/0608

Ameera Mwale CG/24/0601

Susanna Idu CG/24/0604

Boluwatife Adetunji CG/24/0602

Pauline Muthoka CG/24/0607

Stella Obatoye CG/24/0609

Literature Review

NIST Special Publication 800-123

NIST's guidelines are foundational in the field, offering a structured approach to hardening

operating systems and ensuring they meet security standards.These measures include configuring the system to reduce unnecessary services, applying security patches regularly, and implementing robust authentication mechanisms. SP 800-53 Rev. 5, Security and Privacy

Controls for Information Systems and Organizations | CSRC

CIS Benchmarks: CIS Benchmarks provide specific configuration settings and best practices that help organizations systematically reduce vulnerabilities. They cover aspects like account and password policies, network configurations, and application settings, offering a comprehensive approach to system hardening.CIS Benchmarks

References

OS Hardening: 15 Best Practices. [Perception Point]. 2023. https://perception-point.io/guides/os-isolation/os-hardening-10-best-practices/

Operating System (OS) Hardening: Pros, Cons, and Importance. [Linford & Company LLP]. 2023. https://linfordco.com/blog/operating-system-hardening/

What is OS Hardening and How Can Developers Implement it. [Spectral]. 2022. https://spectralops.io/blog/os-hardening-for-developers/

Implementation of Operating System Hardening for Enhanced Security

INTRODUCTION

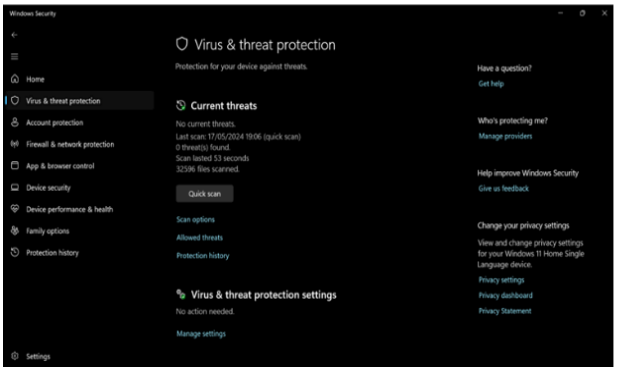
Operating system (OS) hardening is an important practice in cybersecurity that focuses on reducing vulnerabilities and improving system security. This process involves taking various steps to protect the OS from threats like malware, unauthorized access, and exploits.

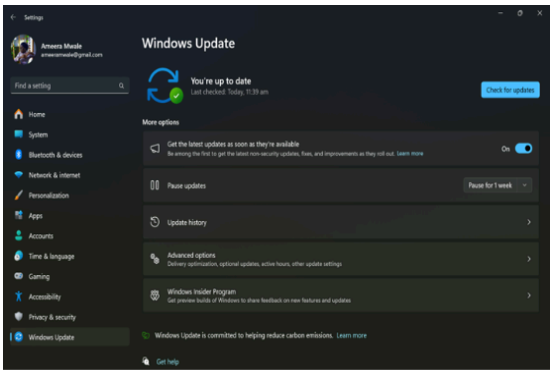
In this report, we will outline the steps taken to harden Windows 11, explaining why each step is important and how it helps improve the system's overall security.

1. Keeping the OS and Software Up to Date

Regular updates ensure that the system is protected against known vulnerabilities and exploits. Security updates often contain security patches that address newly discovered vulnerabilities. Keeping your system updated is essential for maintaining a strong security posture. Here's how to keep your OS and software up to date:

Open Settings, Navigate to Windows Update, Click on Check for updates, and install any available updates.

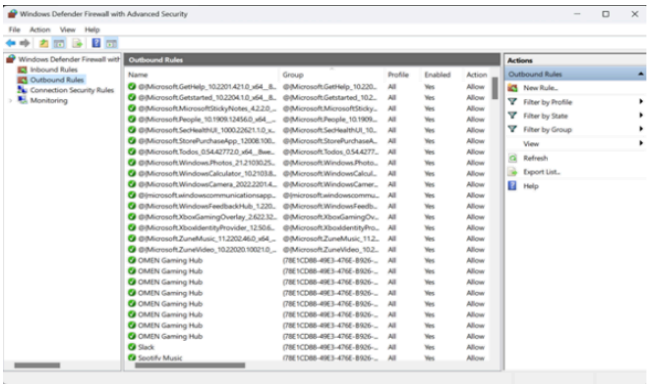


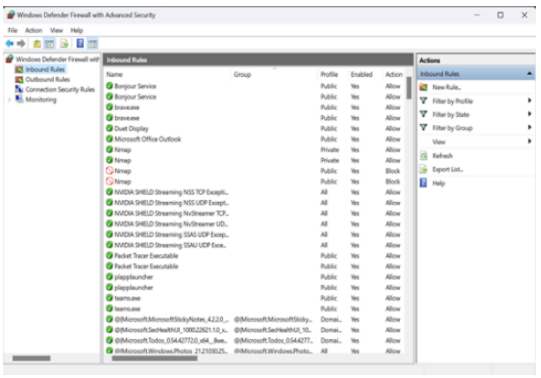


2. Configure Windows Defender

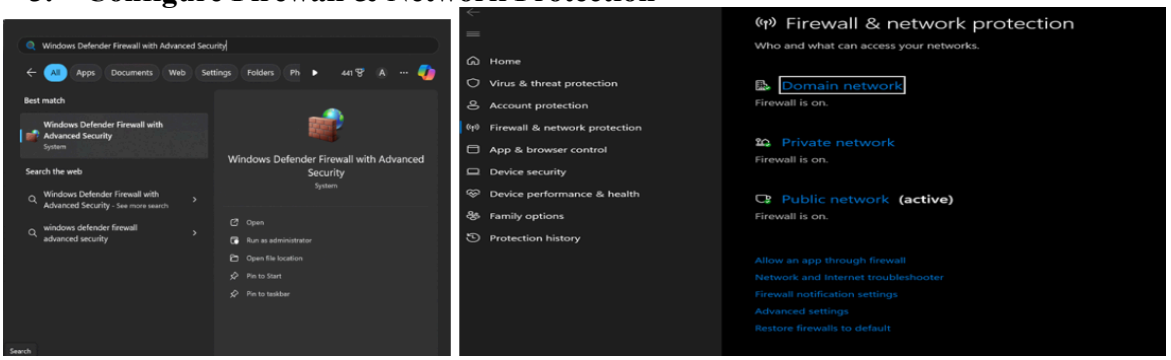
Windows Defender is an integrated antivirus solution that protects the system from various threats including viruses, malware, and spyware. It provides real-time protection and periodic scans to detect and remove malicious software. To configure Windows defender, you can Go to Privacy & Security.> Select Windows Security> Click Virus & Threat

Protection> Ensure Real-Time is ON> Click Quick Scan





3. Configure Firewall & Network Protection



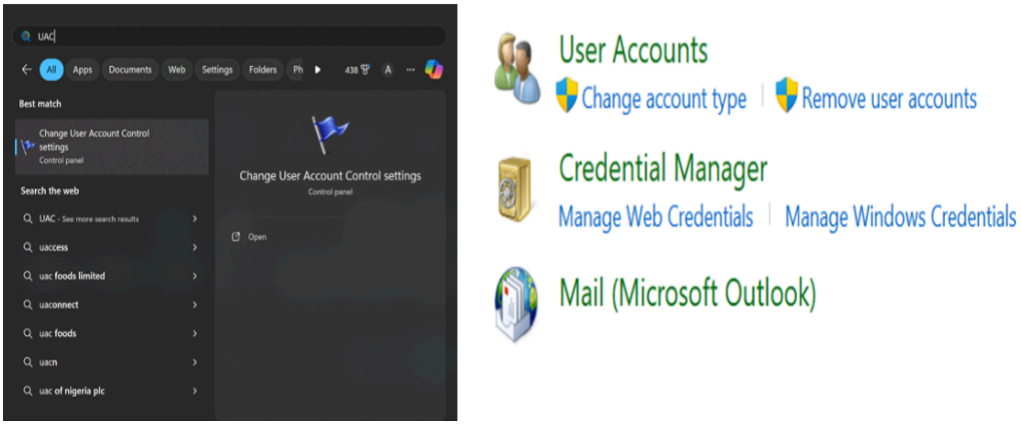
A firewall controls incoming and outgoing network traffic based on predetermined security rules. Properly configuring the firewall helps prevent unauthorized access to the system and blocks malicious traffic.

To activate it, you need to go to Windows Security, Navigate to "Windows Security" in Settings. Select Firewall & Network Protection, then ensure the firewall is turned on and configured correctly.

4. Enable User Account Control (UAC)

UAC prompts for confirmation before making system changes, preventing unauthorized modifications and potential malware execution.

Search for "UAC" in the Windows search bar and open "Change User Account Control settings." Set the slider to the highest level (always notify) for maximum protection. Click “OK” to save the changes. You can also go to Control Panel>User Account> Change Account Type> Set the UAC to second-highest level.

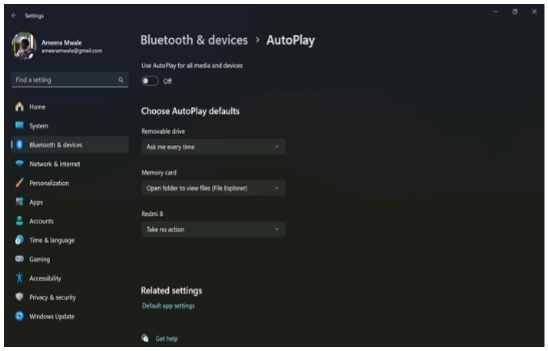


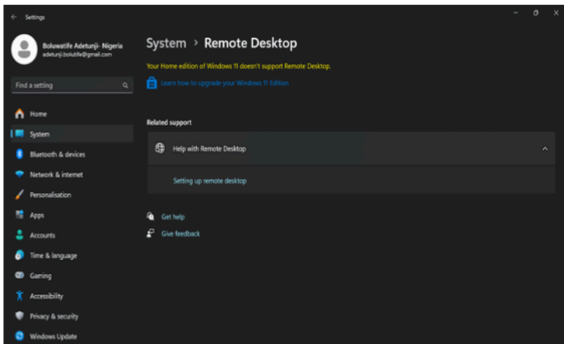
5. Disable Unnecessary Services

Disabling services that are not required reduces the attack surface of the system, as fewer services mean fewer potential entry points for attackers.

To do that you can Press Win + R, type services.msc, Review the list of services and disable services that are not needed, such as Remote Registry and Bluetooth Support (if not used), such as Remote Registry and Bluetooth Support (if not used).

Remote Desktop allows access to your computer from anywhere. Disabling it ensures that sensitive data remains inaccessible to potential intruders. Disabling remote desktop access reduces the attack surface and improves network performance.

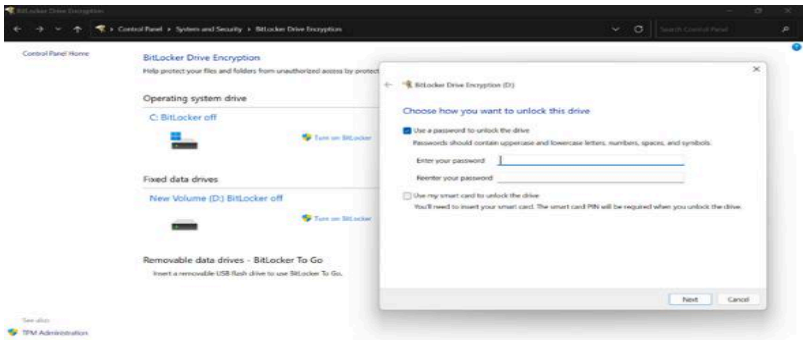




6. Enable BitLocker Encryption

BitLocker encrypts the entire drive, protecting data from unauthorized access in the event of theft or loss. It ensures that data remains confidential and intact.

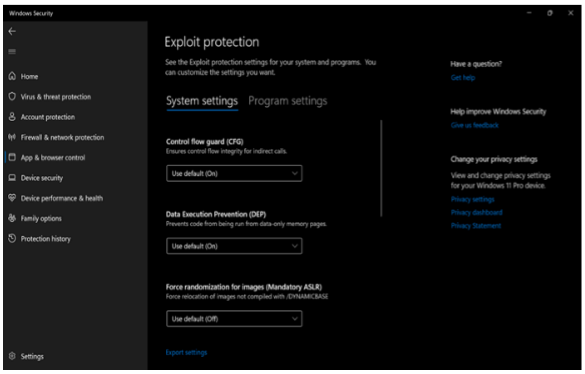
Control Panel> System Security> Select BitLocker Drive Encryption> Turn on BitLocker.

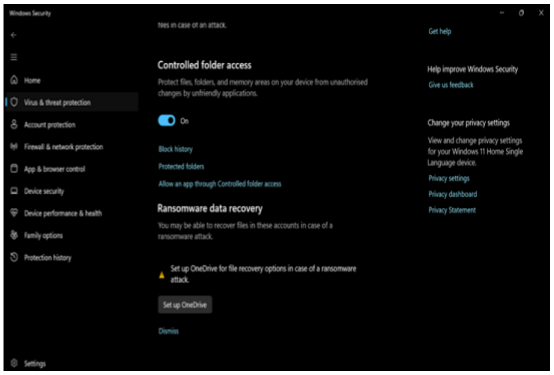


7. Configure Advanced Security Settings

Advanced security settings, such as Exploit Protection, provide additional layers of Defense against sophisticated attacks by mitigating various types of exploits and enhancing overall system resilience.

Go to Settings: Navigate to "Settings." Select Privacy & Security, click on "Windows Security." Click App & Browser Control. Enable Exploit Protection and configure settings for Program Settings and System Settings as required.





8. Use a Robust Security Software

Install a reputable antivirus and anti-malware solution that offers real-time protection, scheduled scans, and additional security features. For example, McAfee, Bitdefender Antivirus Plus, Norton Antivirus Plus, Malwarebytes, and so on. Security software helps detect and prevent malware infections, phishing attempts, and other security threats.

DISADVANTAGES OF OS HARDENING

While OS hardening seeks to reduce a system's attack surface, some of its potential consequences could include lesser convenience of using the operating system, increased configurations, settings, and tools installed monitoring and maintaining time, high cost, and possible systems malfunction after hardening.

Conclusion:

Implementing these hardening measures on Windows 11 significantly enhances the security of the operating system. Each step—updating the OS, configuring Windows Defender, setting up the firewall, adjusting UAC, disabling unnecessary services, enabling BitLocker, configuring advanced security settings, and regular backups—contributes to creating a robust and secure environment. These practices reduce vulnerabilities, protect against various threats, and ensure data integrity and availability. By following these processes, we can effectively harden Windows 11 and provide a secure computing experience.