**System Hardening Lab Report**

**Zakiya Moore**

**April 2025**

**Table of Contents**

1. Introduction
2. Lab Environment
3. Windows 11 System Hardening
   1. User Account Creation and Management
   2. Password and Account Lockout Policies
   3. Services Hardening
   4. Firewall Configuration and Hardening
   5. Antivirus and Endpoint Protection
   6. System Updates
   7. NTFS Folder Permission Hardening
4. Ubuntu 24.04 System Hardening
   1. User and Group Management
   2. SSH and Password Policies
   3. Firewall (UFW) Configuration
   4. System Updates
5. Challenges Encountered
6. Lessons Learned
7. Final Reflection

**1. Introduction**

This lab focuses on enhancing security in Windows 11 and Ubuntu 24.04 environments through systematic hardening practices, including account management, system service control, firewall rules, antivirus settings, and folder permissions.

**2. Lab Environment**

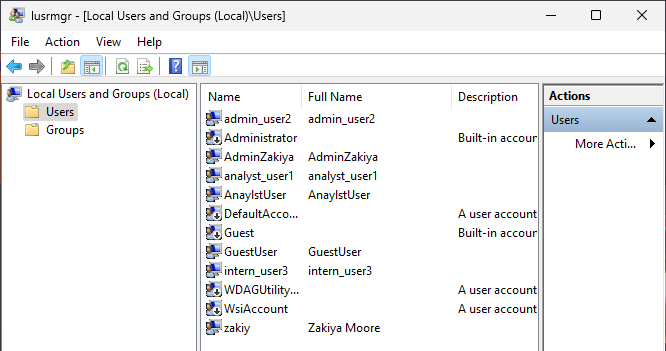
| **Component** | **Description** |
| --- | --- |
| Operating Systems | Windows 11 Pro, Ubuntu 24.04 LTS |
| Tools | secpol.msc, services.msc, eventvwr.msc, ufw, PowerShell, File Explorer |

**3. Windows 11 System Hardening**

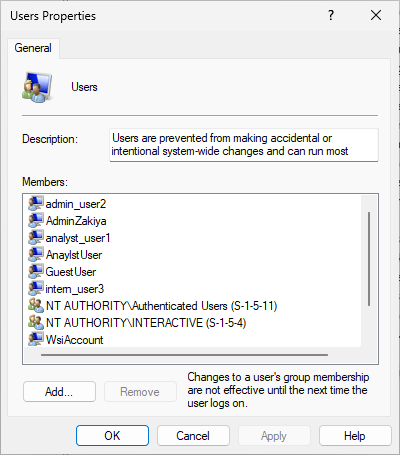
**3.1 User Account Creation and Management**

Three accounts were manually created and assigned to built-in groups:

* **AdminZakiya** (Administrators)
* **AnalystUser** (Users)
* **GuestUser** (Guests; disabled)

**

*Figure 1: Created local user accounts (AdminZakiya, AnalystUser, GuestUser) on Windows 11. Assigned appropriate group memberships to enforce least privilege access and strengthen security controls.*

**

*Figure 2:* Configured security groups on Windows 11 to organize user permissions. Applied group-based access control to simplify account management and improve system security.

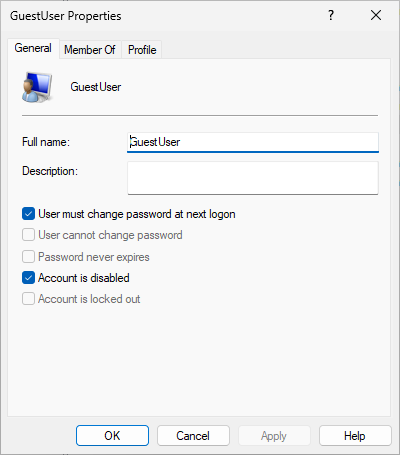
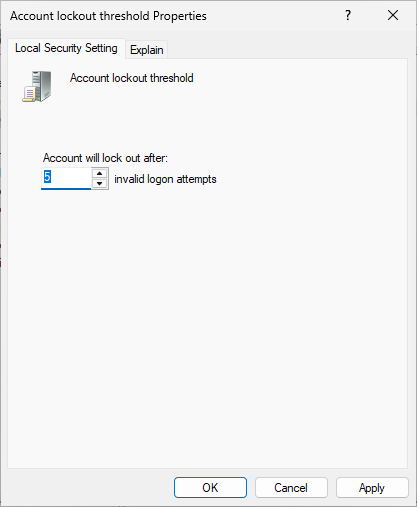
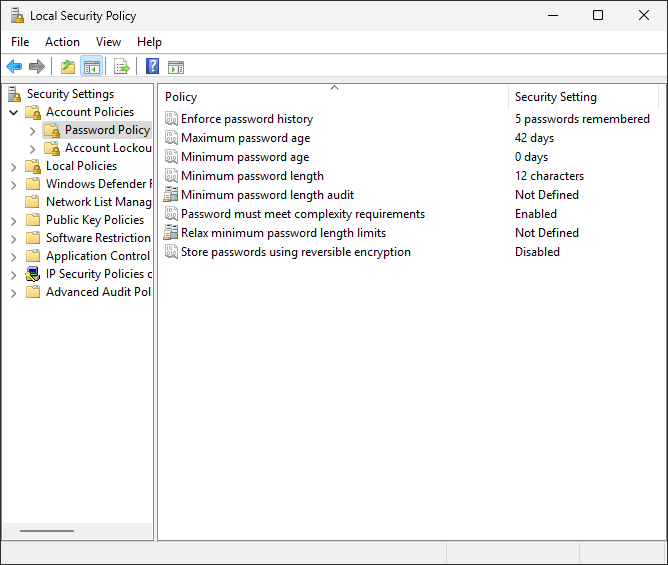


Figure 3: Disabled the default Guest account on Windows 11 / operating system to reduce unauthorized access risks. This hardening step follows security best practices by limiting anonymous or low-privilege account vulnerabilities.

**3.2 Password and Account Lockout Policies**

Password policies enforced:

* Minimum length: 12 characters
* Complexity: Enabled
* Lockout: 5 invalid attempts; 15-minute duration

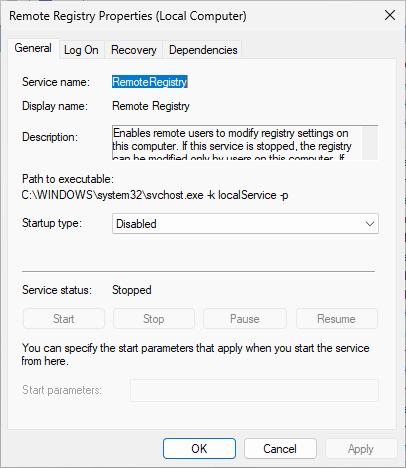
*Figures: 4 and 5:* Demonstrated system hardening steps by configuring password policies on Windows 11. Changes align with CIS Benchmark recommendations to enhance system security and enforce strong authentication practices.

**3.3 Services Hardening**

The following unnecessary services were disabled:

* Remote Registry
* SSDP Discovery
* UPnP Device Host

Telnet was not present by default and required no action.



*Figure 6*

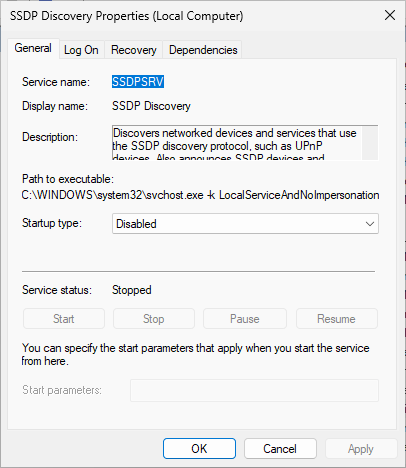
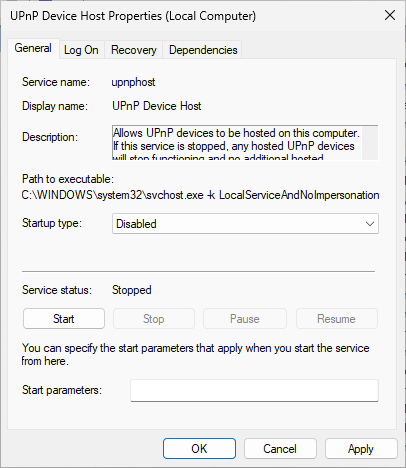


Figure 7



*Figure 8*

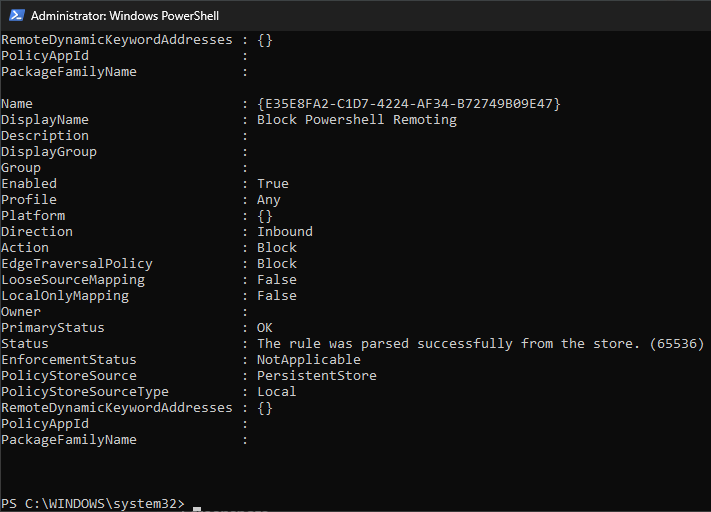
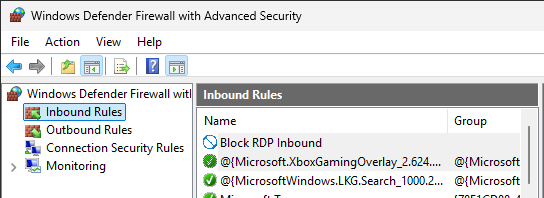
*Figures 6–8: Disabled unnecessary services (Remote Registry, SSDP Discovery, and UPnP Device Host) to reduce system attack surface and harden the Windows 11 environment. Telnet service was not present by default and required no further action. These steps align with CIS Benchmarks and industry, the best practices for minimizing vulnerabilities.*

**Lessons Learned:** Service hardening significantly reduces potential attack vectors by disabling unused or risky services. Confirming the system configuration is crucial for accurate hardening.

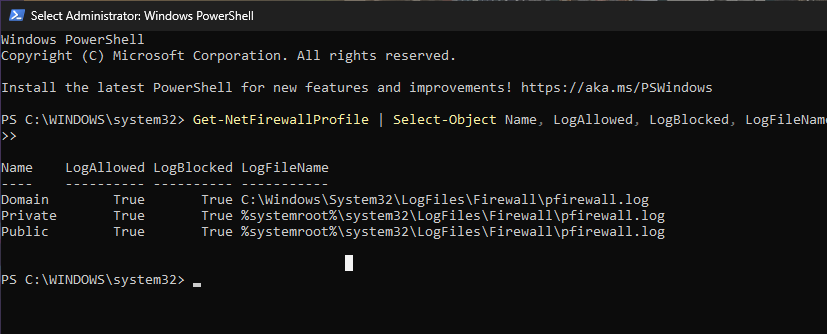
**3.4 Firewall Configuration and Hardening**

Windows Firewall configured to:

* Block RDP (TCP 3389) and PowerShell Remoting (TCP 5985/5986)
* Enable logging for dropped packets

*Figure 9 Figure 10*



*Figure 11*

***Figures 9–11:*** *Configured Windows Firewall to block inbound RDP (TCP 3389) and PowerShell Remoting (TCP 5985/5986) traffic. Enabled firewall logging for dropped packets across all profiles to support auditing and intrusion detection. These changes align with CIS Benchmark recommendations for host-based network defense.***3.5 Antivirus and Endpoint Protection**

* Enabled Windows Defender real-time protection
* Updated virus definitions

A screenshot of a computer

AI-generated content may be incorrect.

Figure 12–13: PowerShell output confirming Windows Defender real-time protection is active and virus definitions are current, in alignment with CIS Benchmark security best practices.

**3.6 System Updates**

* Fully updated Windows 11 through Windows Update

*(Figure 14: System fully updated)*

**3.7 NTFS Folder Permission Hardening**

Secured folders created with appropriate NTFS permissions:

* **C:\Security\_Logs:** AdminZakiya only
* **C:\Admin\_Tools:** AdminZakiya only
* **C:\Shared\_Documents:** AdminZakiya and AnalystUser (Modify)

*(Figures 15–17: Folder permission configurations)*

**Lessons Learned:** Proper NTFS permissions significantly reduce unauthorized data access and exposure risks, highlighting the importance of strict access control.

**4. Ubuntu 24.04 System Hardening**

**4.1 User and Group Management**

Users created and assigned:

* **adminzakiya** (sudo, admin)
* **analystuser** (secops)
* **guestuser** (guests)

*(Figures 18–20: Ubuntu user and group creation)*

**4.2 SSH and Password Policies**

* Disabled SSH root login in /etc/ssh/sshd\_config
* Password complexity enforced via pam\_pwquality

*(Figures 21–22: SSH and password policies)*

**4.3 Firewall (UFW) Configuration**

* Enabled UFW firewall
* Blocked unnecessary ports

*(Figures 23–24: UFW firewall configurations)*

**4.4 System Updates**

* System packages fully updated via terminal commands

*(Figure 25: Ubuntu system updated)*

**5. Challenges Encountered**

Identifying specific system services to disable required careful research to avoid disabling essential system functionality. Understanding default security configurations, such as the absence of Telnet, was also crucial.

**6. Lessons Learned**

This lab provided hands-on experience in essential system hardening practices, emphasizing identity and access management, strong policy enforcement, service and firewall configurations, and cross-platform hardening strategies.

**7. Final Reflection**

Completing the System Hardening Lab has significantly deepened my understanding of the practical application of security principles. I recognize how essential proactive system configuration and documentation are to maintaining secure and resilient environments. This experience will greatly inform my future cybersecurity practices.