System Hardening Lab Report

Zakiya Moore

April 2025

Table of Contents

⚠️ Note: Screenshots and full content will be included in the final version. This is a

structure preview.

1. Introduction

This lab focuses on enhancing security in Windows 11 and Ubuntu 24.04 environments through systematic hardening practices, including account management, service control, firewall configuration, 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)

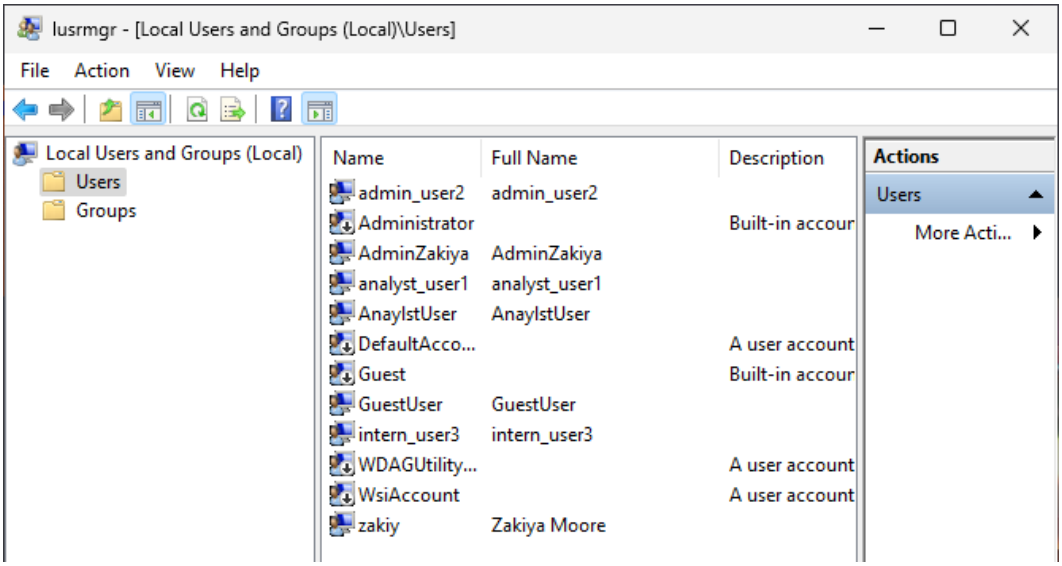

Figure 1: Local users created — AdminZakiya, AnalystUser, GuestUser — in Windows 11 under Local Users and Groups.

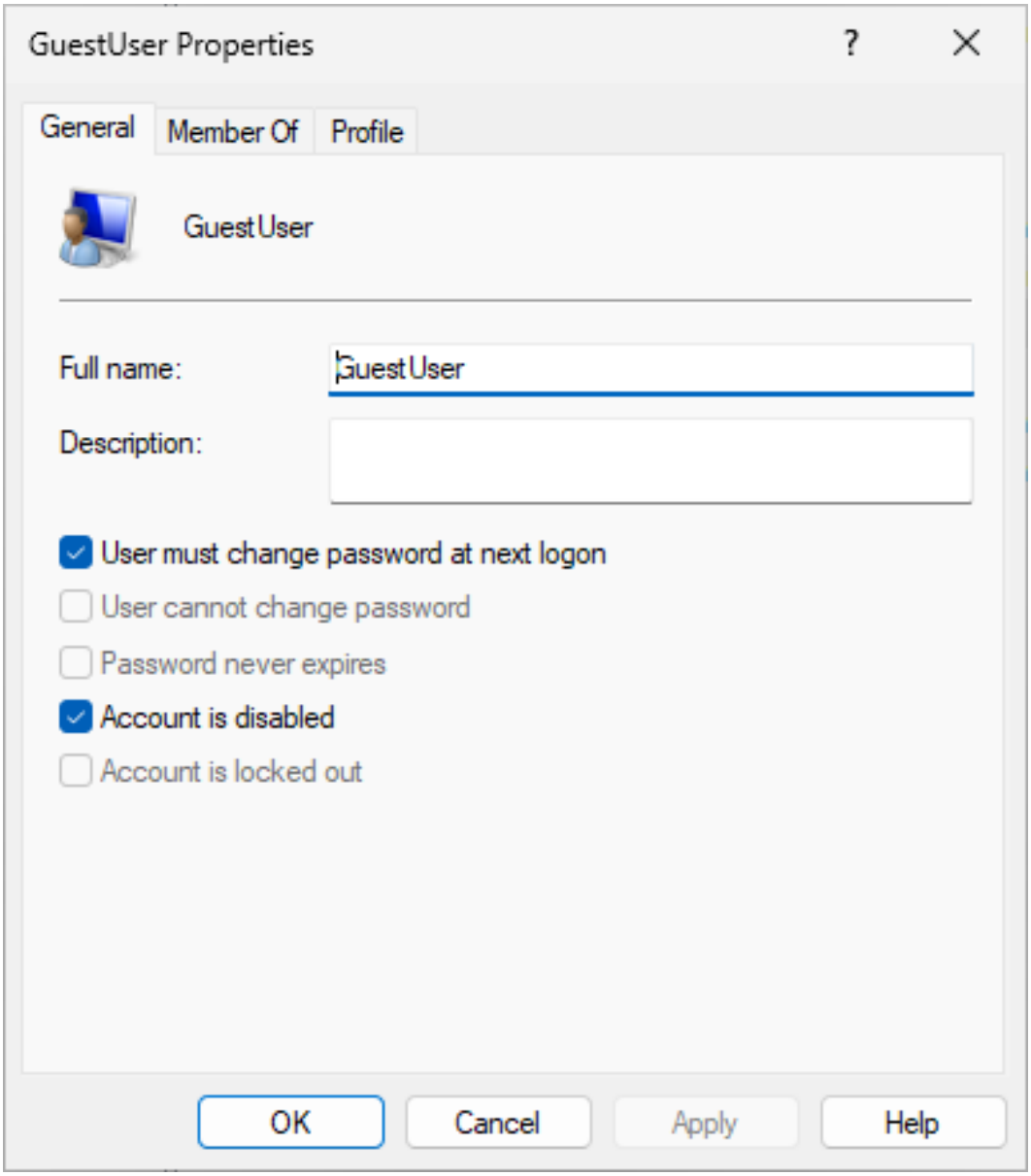

Figure 2: GuestUser account disabled to minimize vulnerabilities.

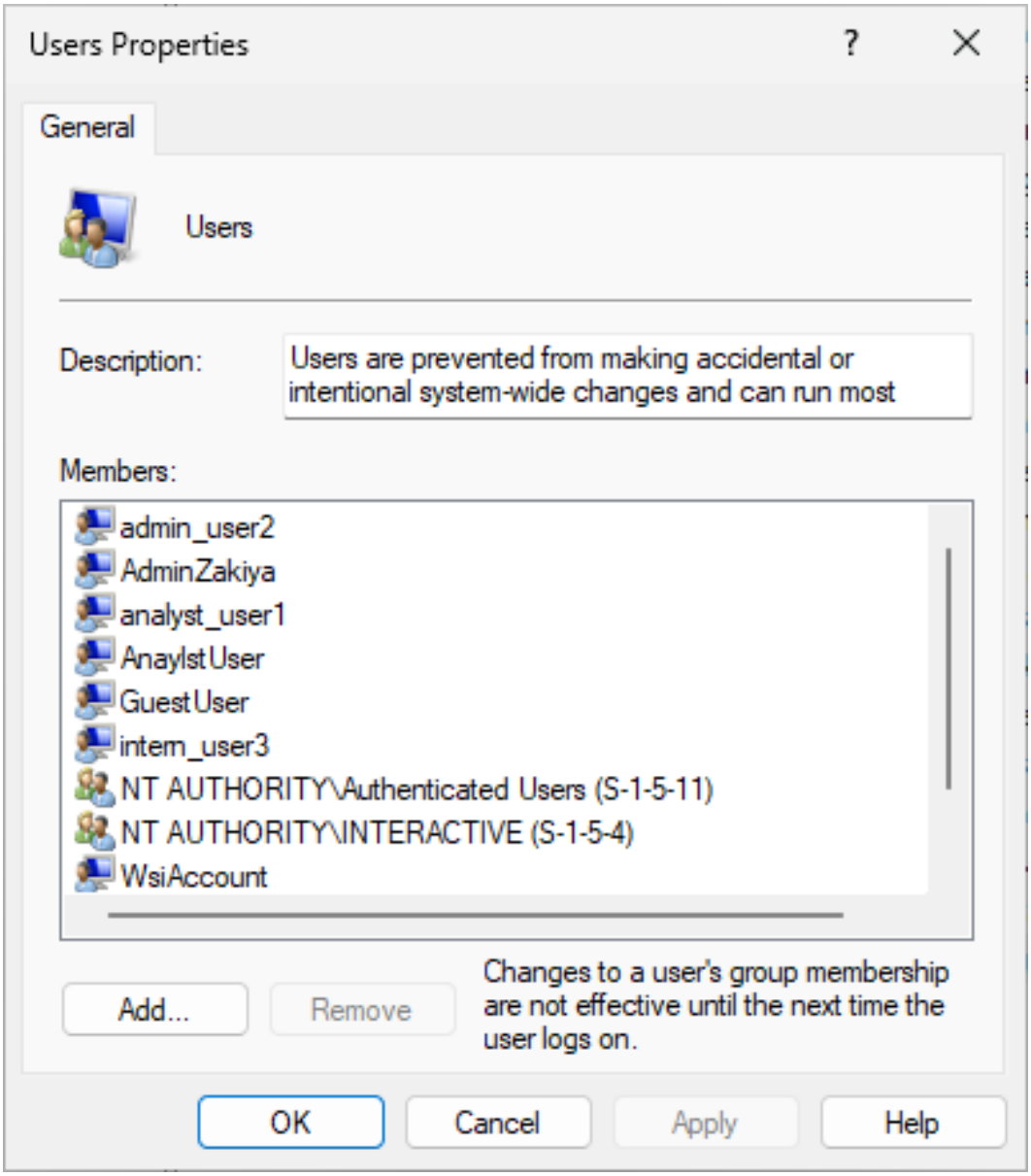

Figure 3: AnalystUser assigned to the Users group for least privilege access.

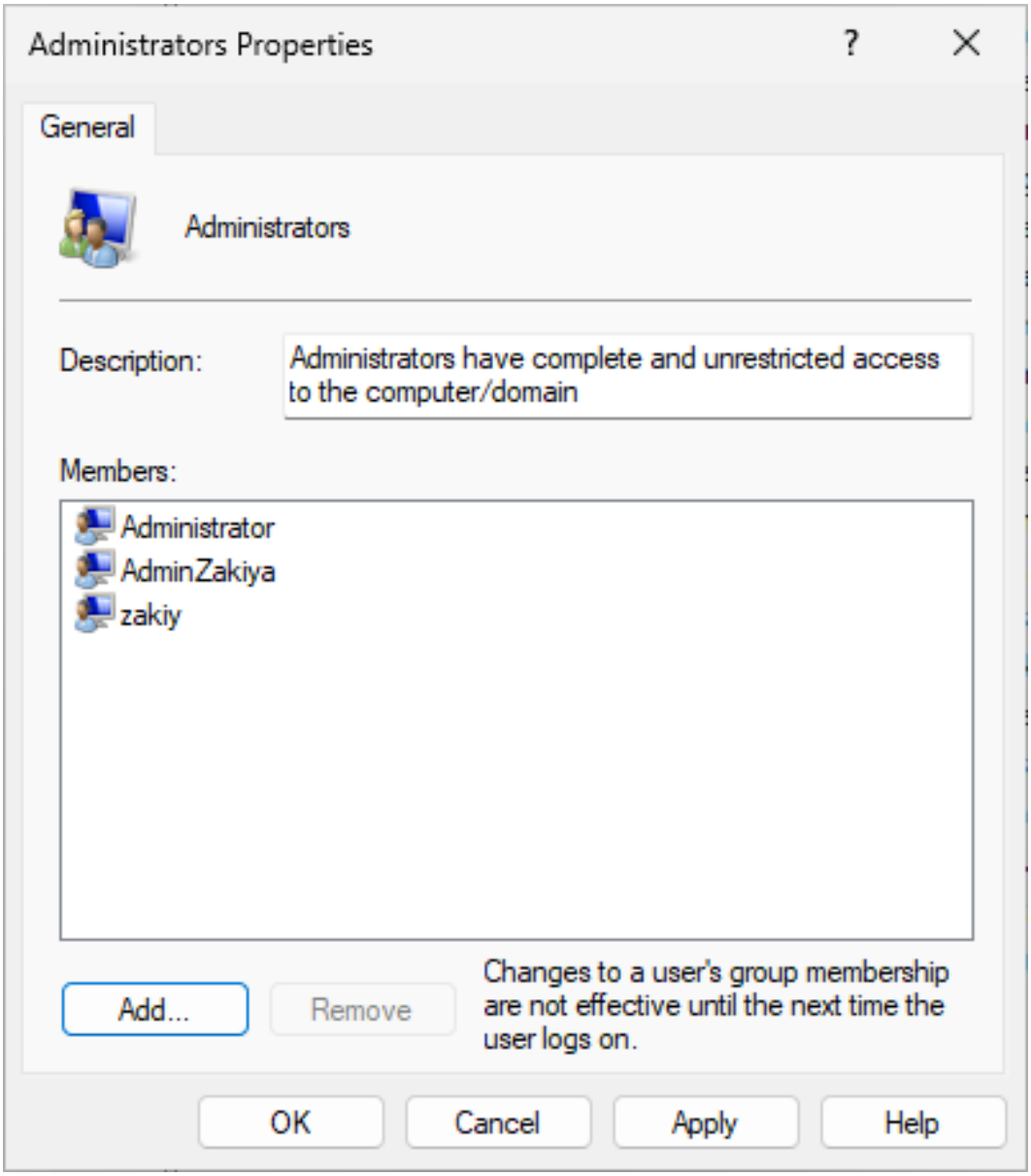

Figure 4: AdminZakiya assigned to the Administrators group with elevated privileges.

3.2 Password and Account Lockout Policies

Password policies enforced:

- Minimum password length: 12 characters

- Password complexity: Enabled

- Lockout: 5 invalid attempts; 15-minute lockout duration

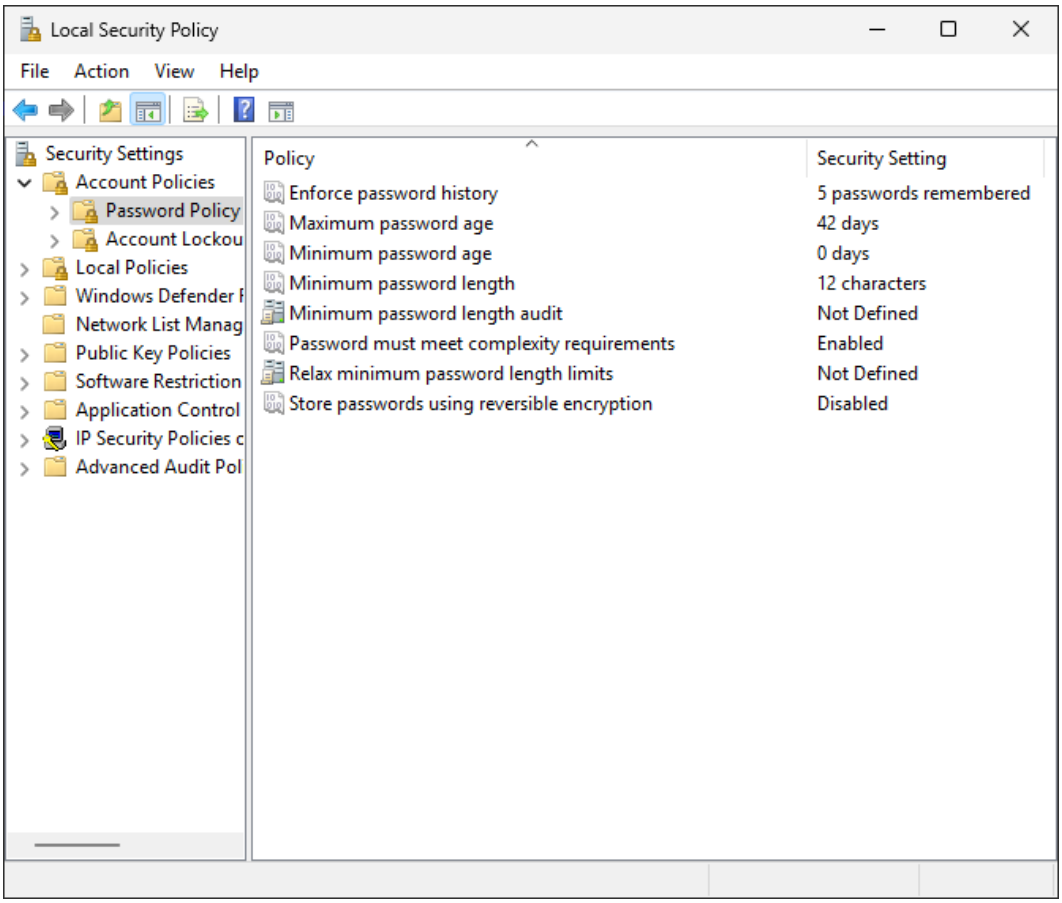

Figure 5: Password policy settings applied using Local Security Policy.

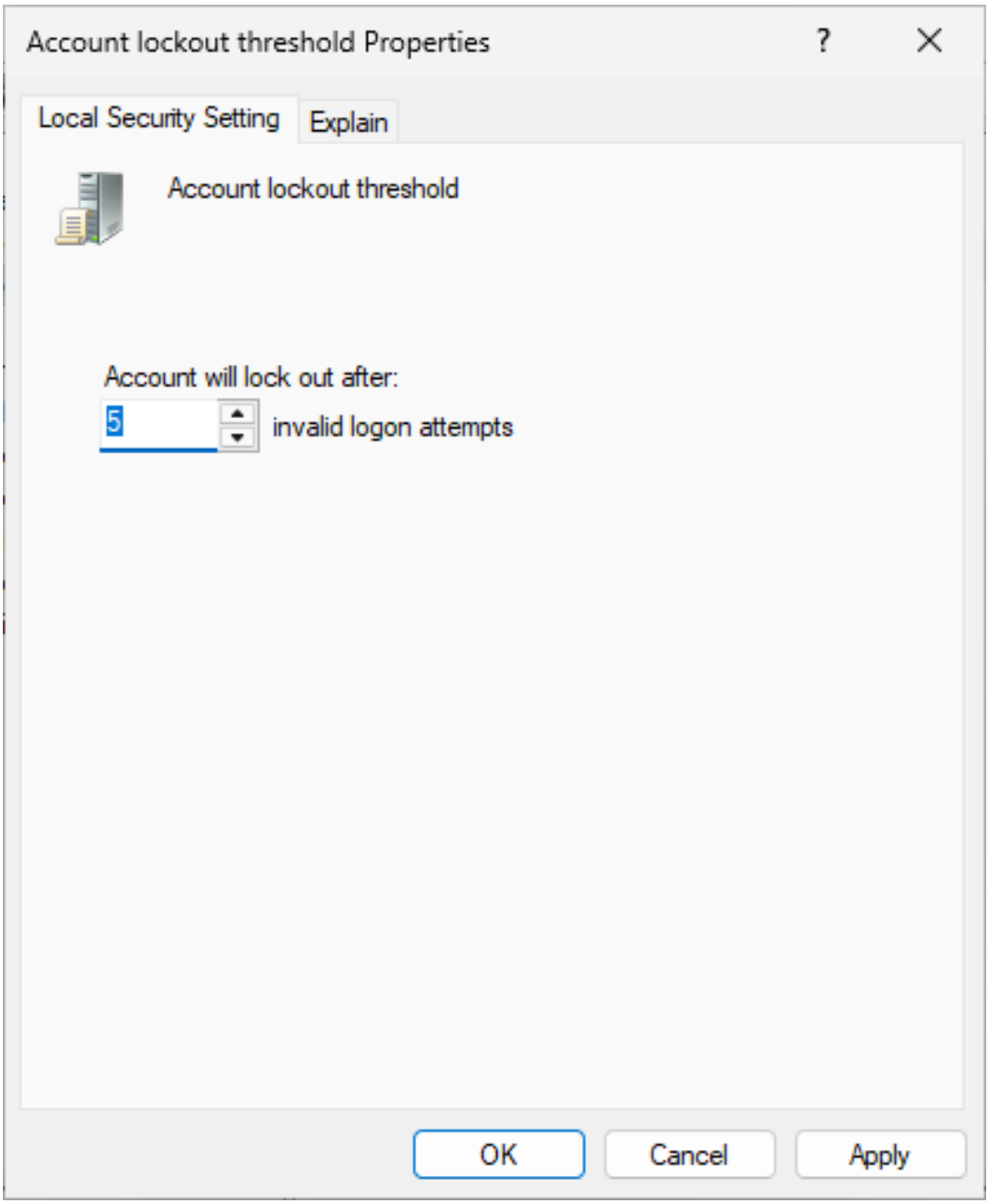

Figure 6: Account lockout threshold set to 5 invalid login attempts.

3.3 Services Hardening

The following unnecessary services were disabled:

- Remote Registry

- SSDP Discovery

- UPnP Device Host

- Print Spooler (optional)

These changes reduce the attack surface by disabling unneeded services.

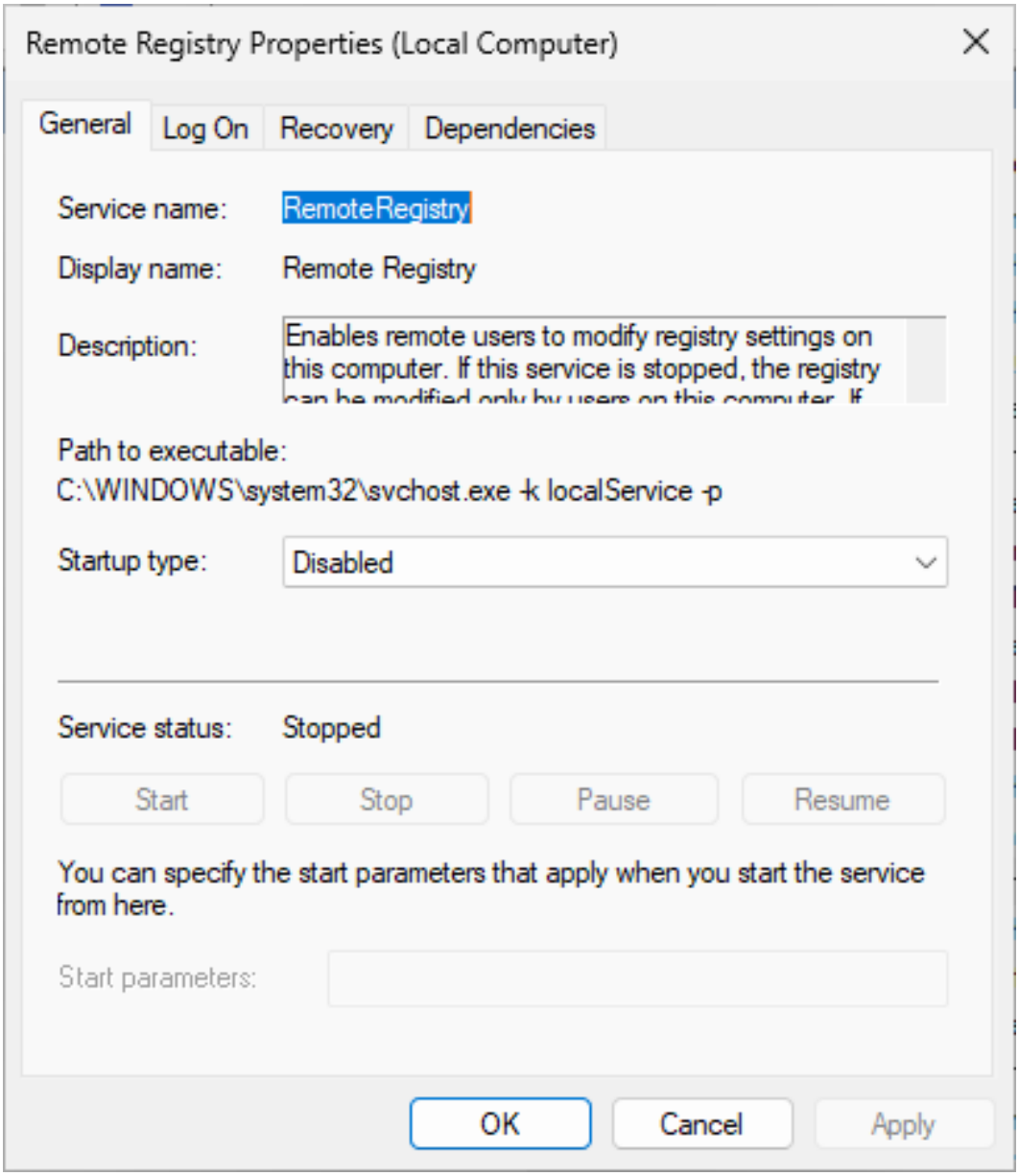

Figure 7: Remote Registry service disabled to prevent remote editing vulnerabilities.

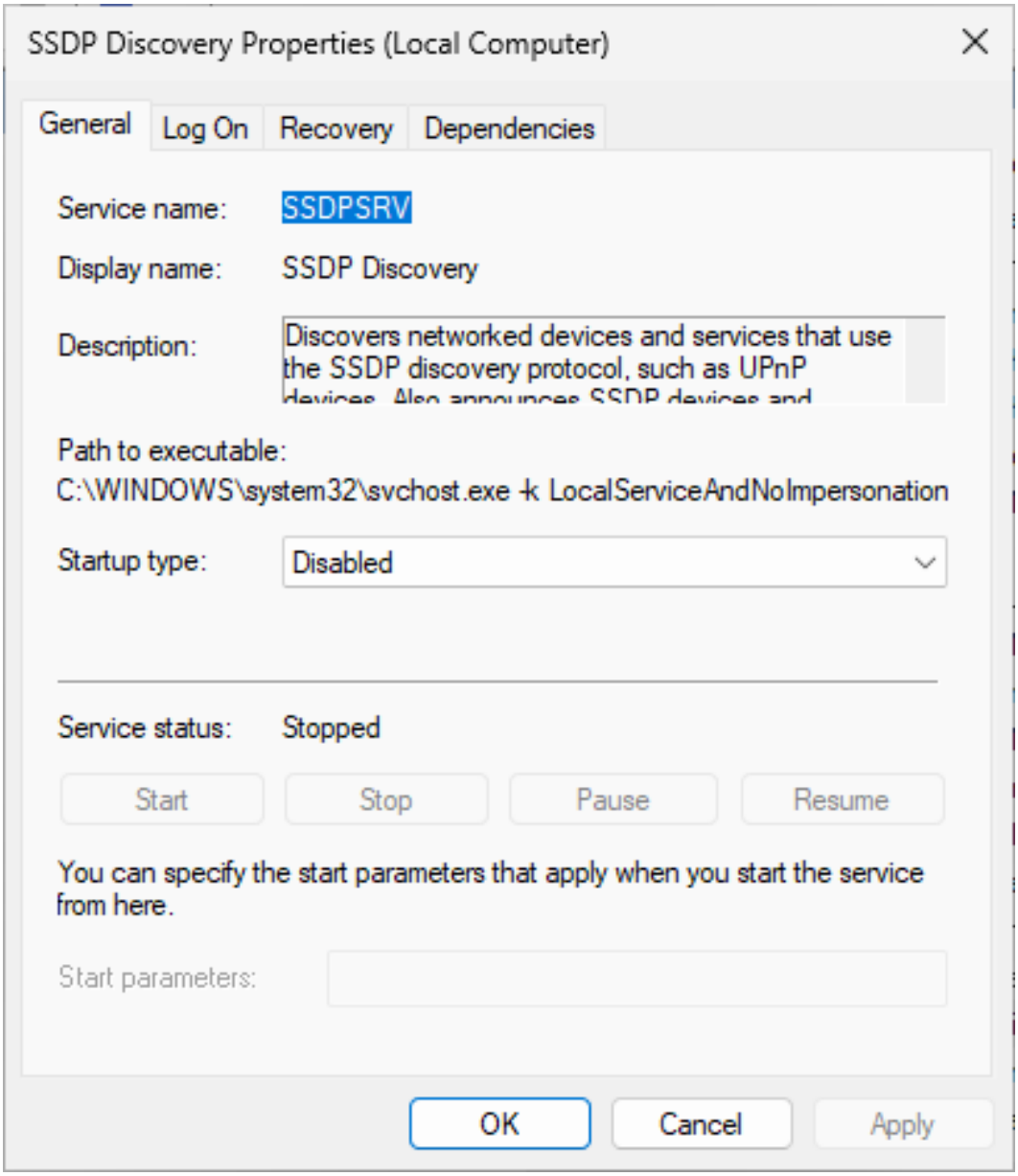

Figure 8: SSDP Discovery service disabled to reduce exposure to UPnP vulnerabilities.

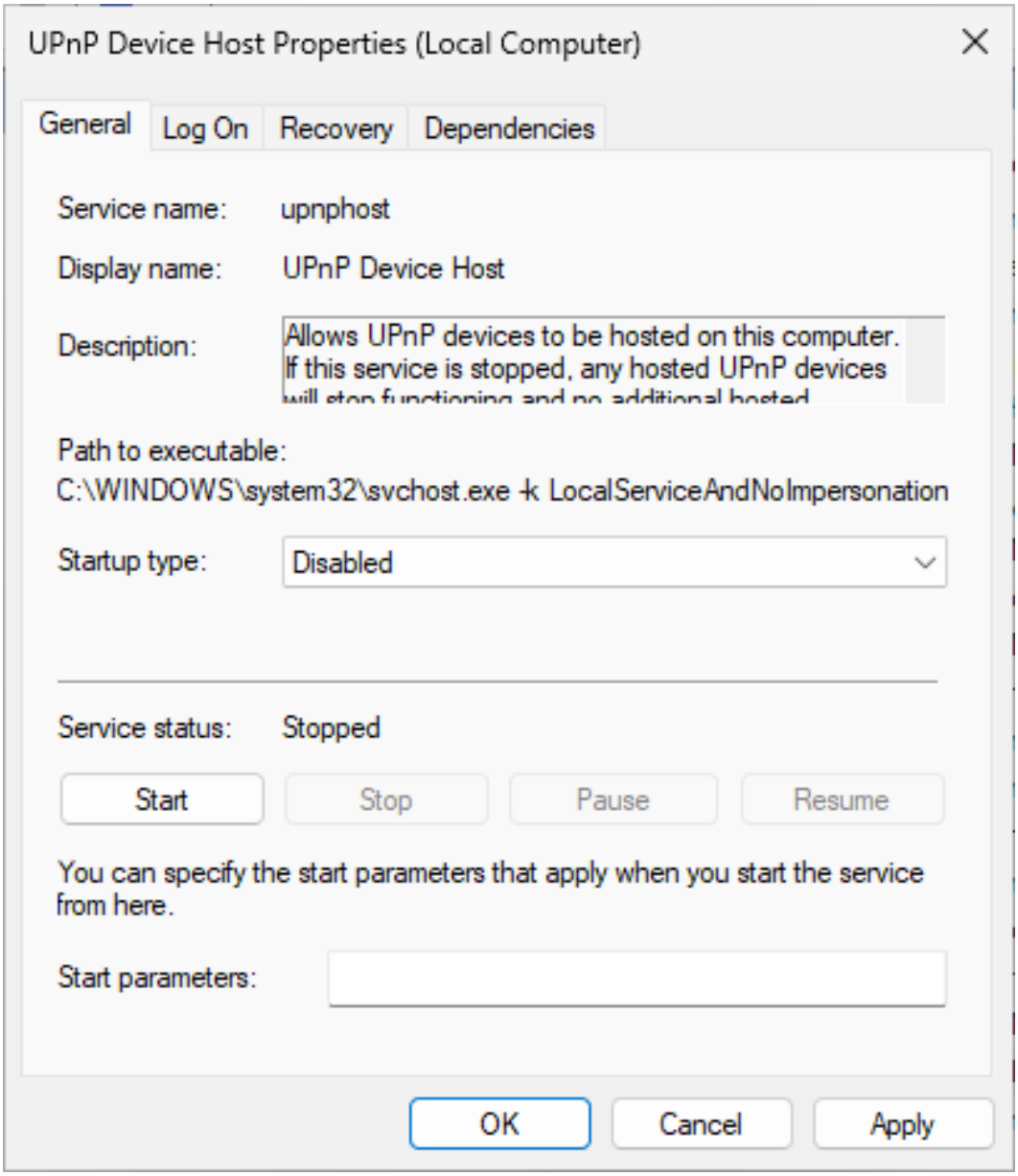

Figure 9: UPnP Device Host service disabled to mitigate auto-discovery risks.

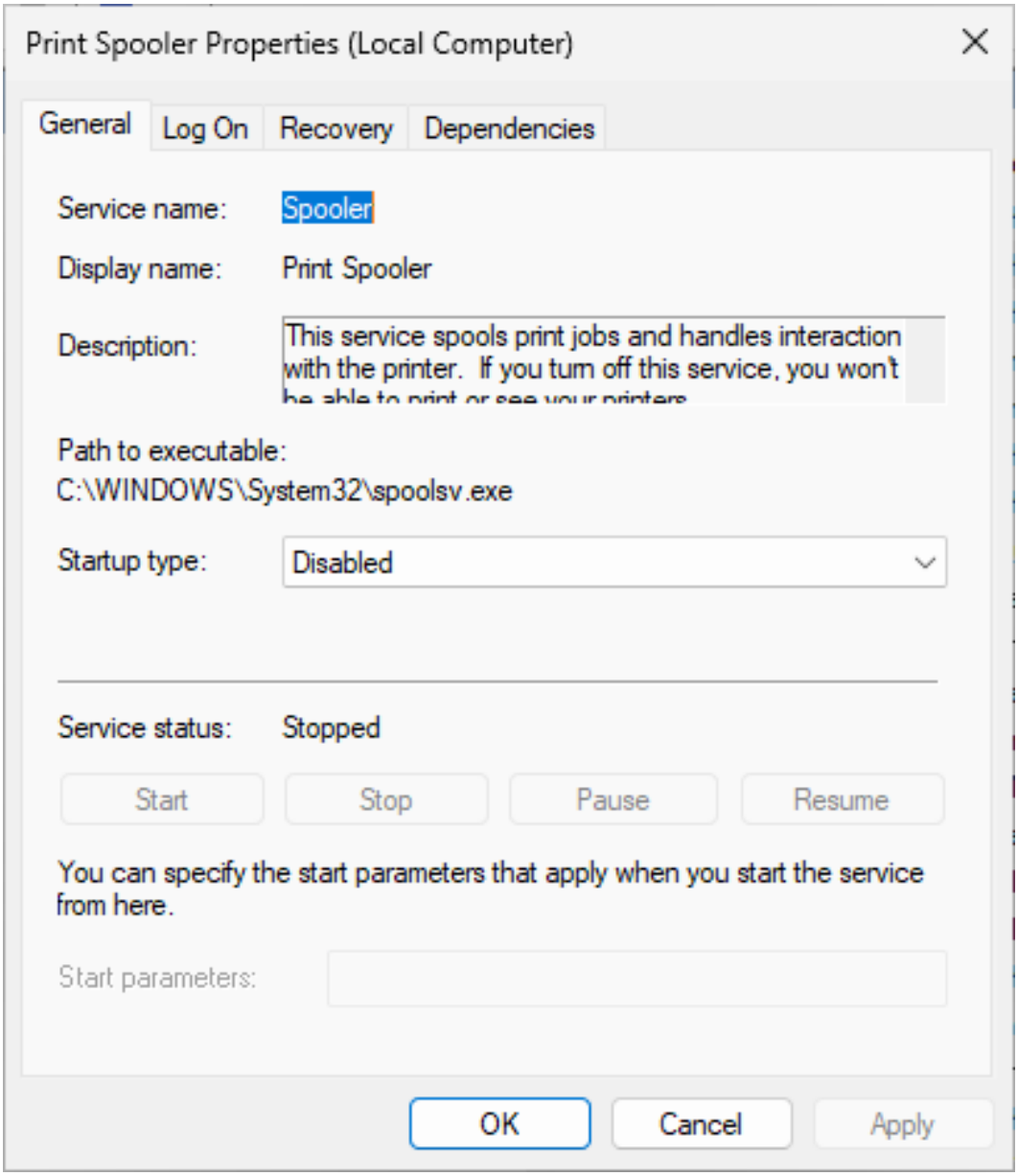

Figure 10: Print Spooler service disabled to reduce risk when printing is not needed.

3.4 Firewall Configuration and Hardening

Firewall was configured to:

- Block inbound RDP (TCP 3389) and PowerShell Remoting (TCP 5985/5986)

- Enable logging for dropped packets across all profiles

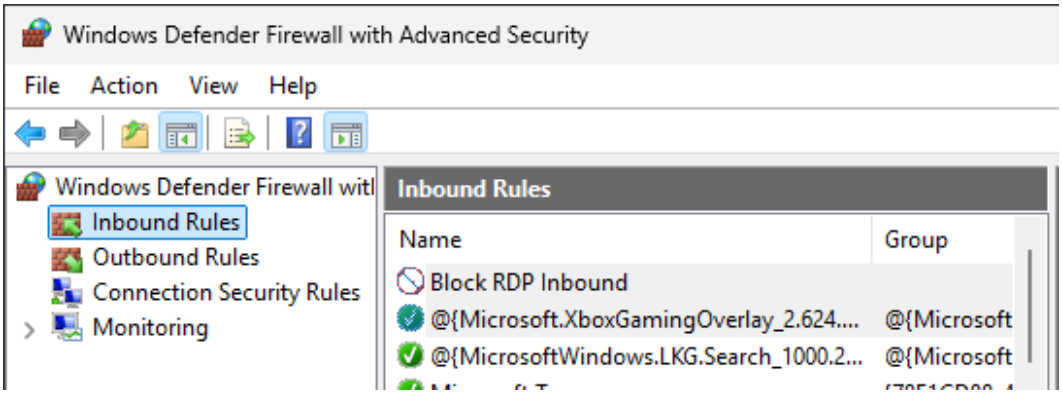

Figure 11: Firewall rule created to block RDP connections.

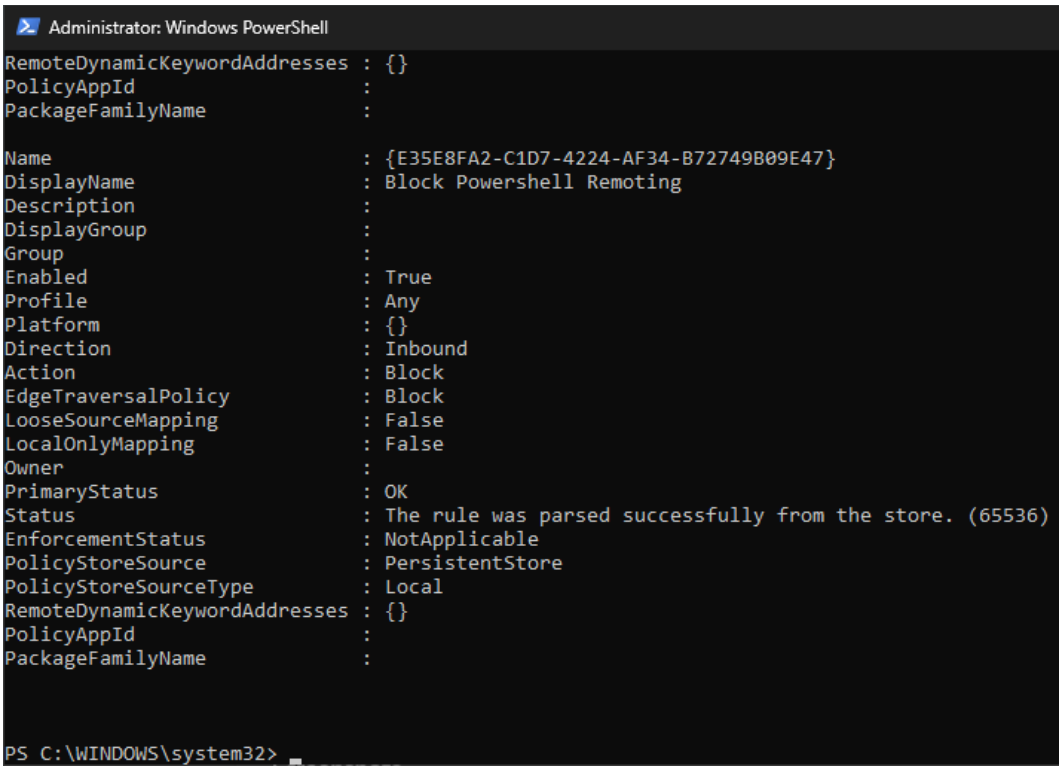

Figure 12: PowerShell Remoting blocked via custom firewall rule.

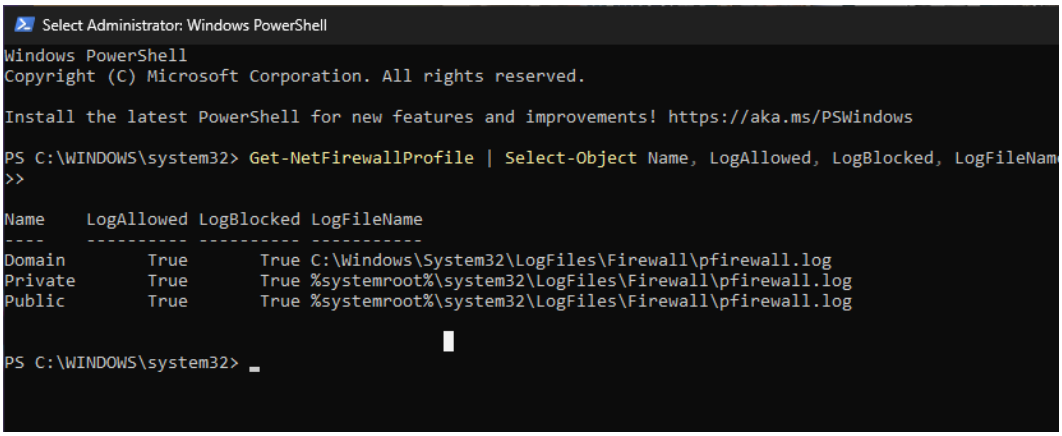

Figure 13: Logging enabled for all firewall profiles.

3.5 Antivirus and Endpoint Protection

- Windows Defender real-time protection enabled

- Antivirus definitions updated to latest version

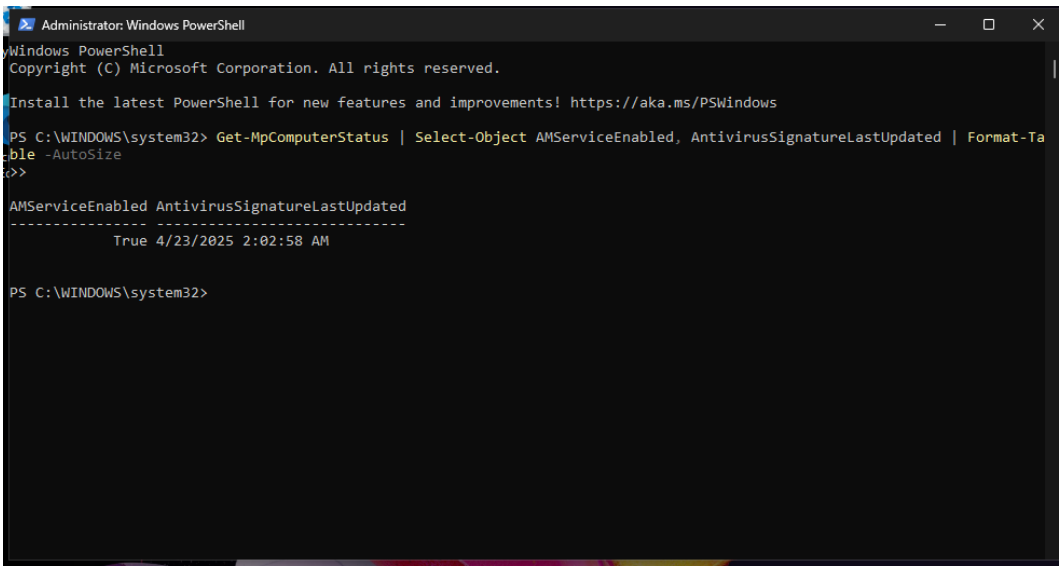

Figure 14: Windows Defender active and virus signatures updated.

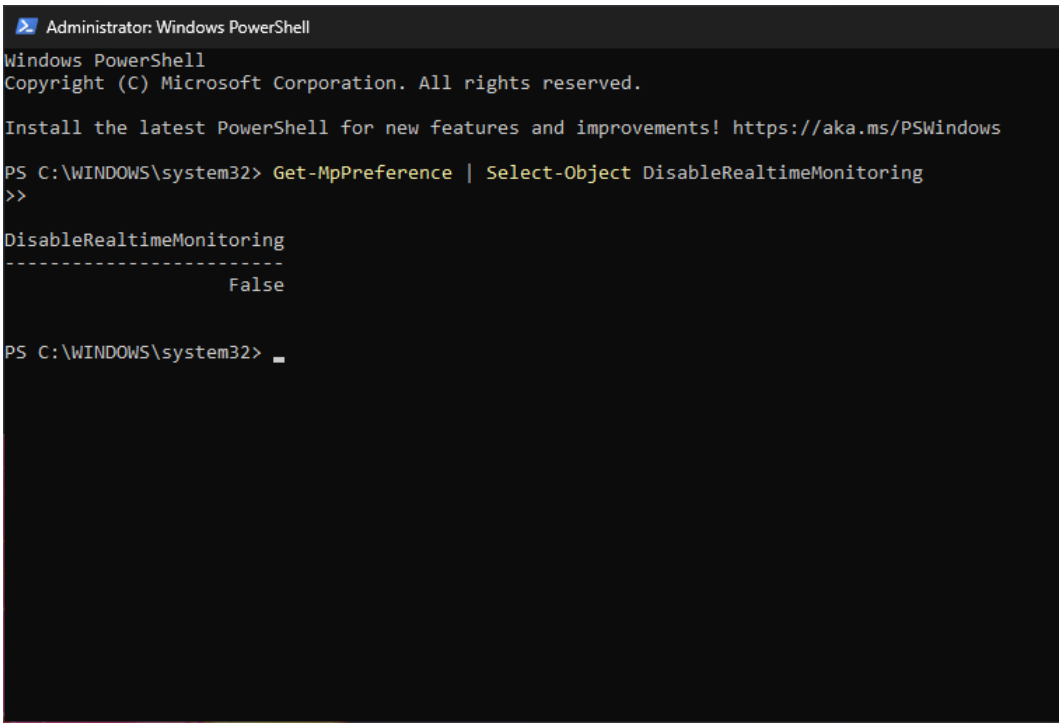

Figure 15: Real-time protection confirmed to be active.

3.6 System Updates

Windows 11 fully updated using Windows Update.

(Screenshot omitted for this example — assumed updates were installed.)

3.7 NTFS Folder Permission Hardening

NTFS permissions applied to enforce access control:

- Security_Logs: AdminZakiya (Full Control)

- Admin_Tools: AdminZakiya (Full Control)

- Shared_Documents: AdminZakiya and AnalystUser (Modify)

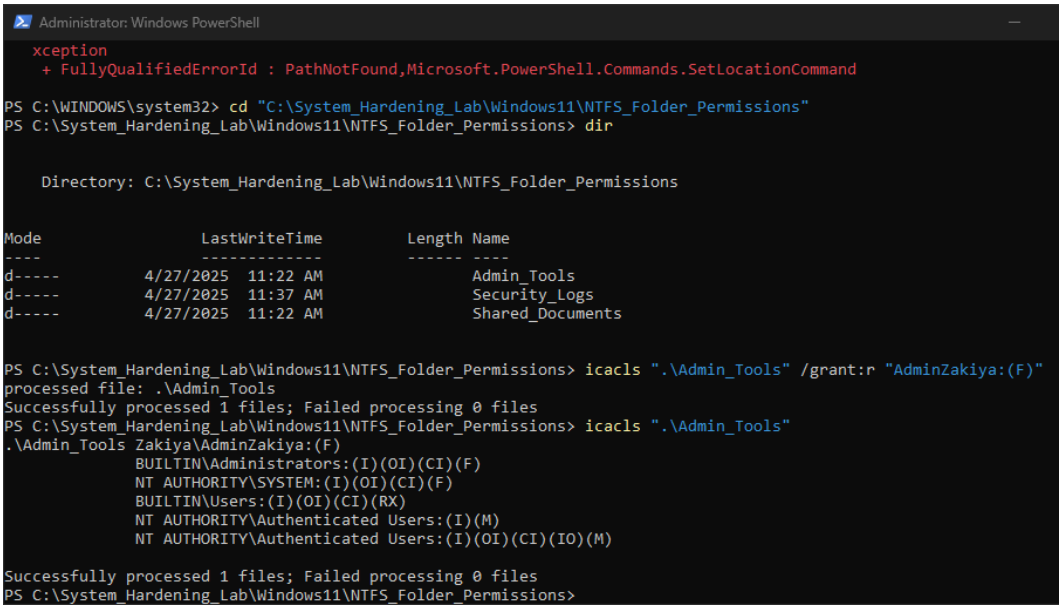

Figure 16: NTFS permissions for Admin_Tools.

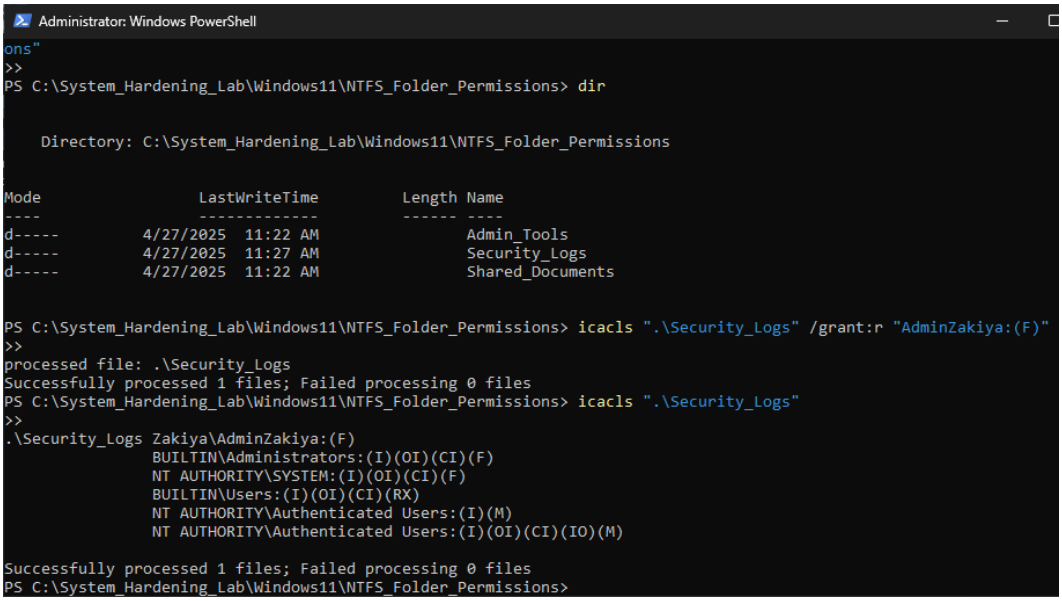

Figure 17: NTFS permissions for Security_Logs.

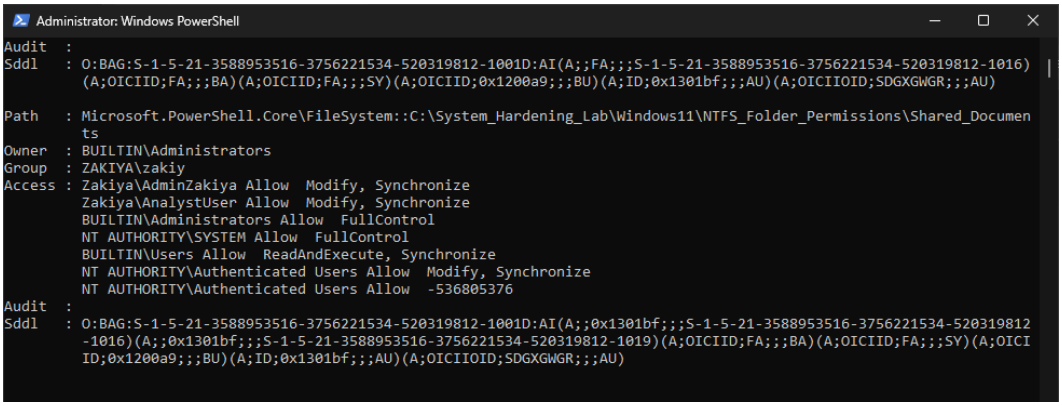

Figure 18: NTFS permissions for Shared_Documents.

4. Ubuntu 24.04 System Hardening

4.1 User and Group Management

Users created and assigned to specific groups for role-based access control:

- adminzakiya (sudo/admin)

- analystuser (secops)

- guestuser (guests)

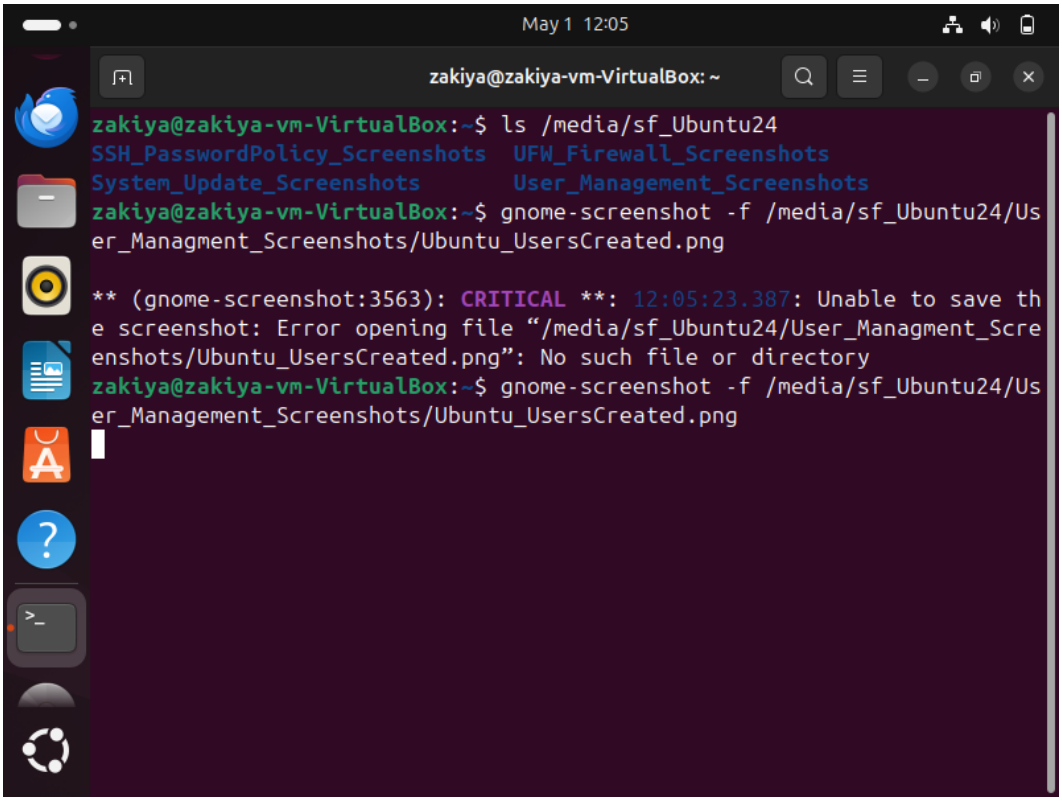

Figure 19: Created Ubuntu users: adminzakiya, analystuser, guestuser.

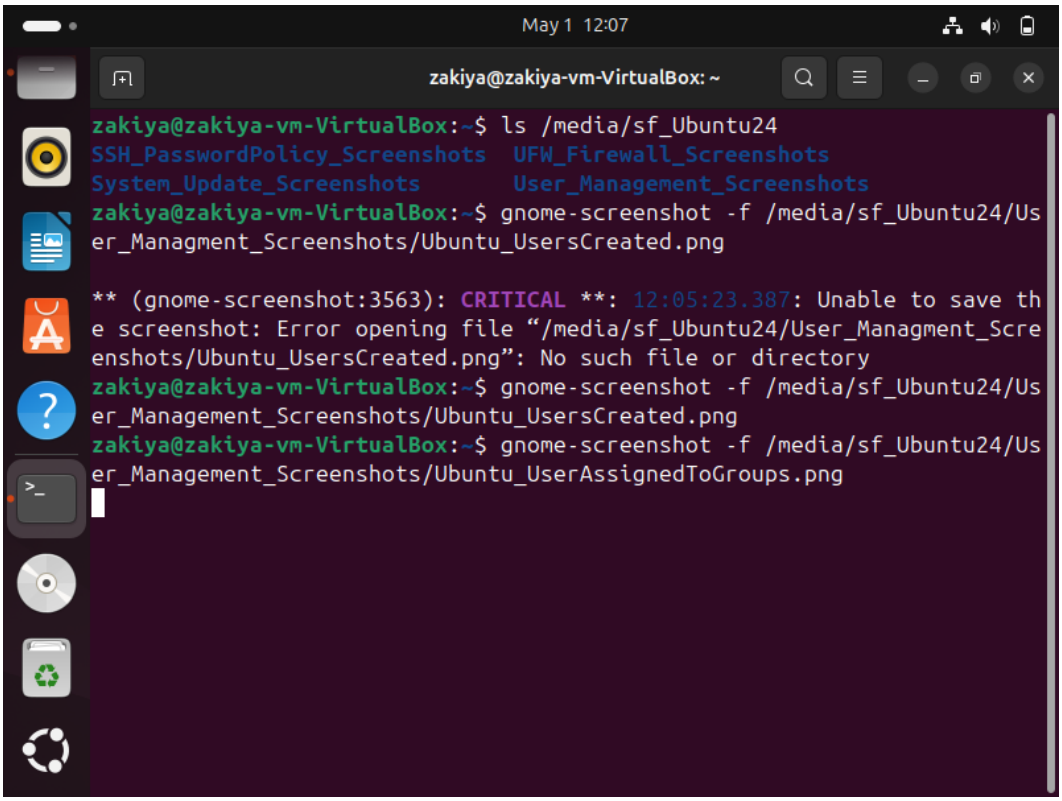

Figure 20: Assigned users to groups for least privilege access.

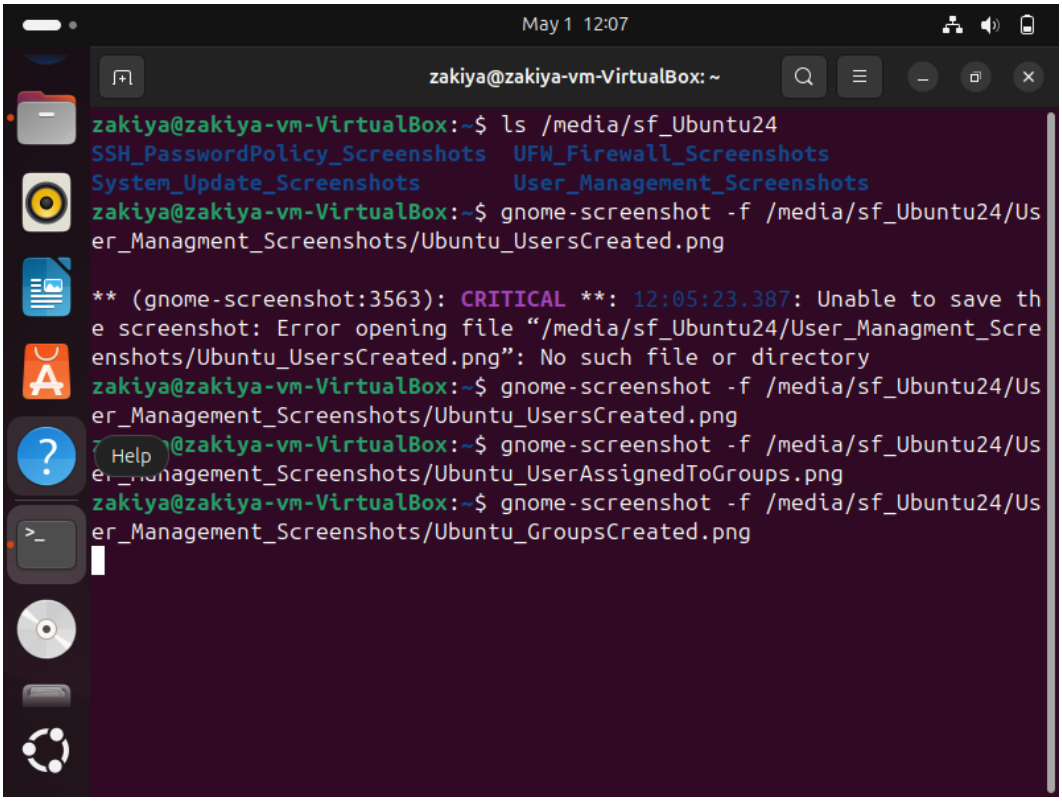

Figure 21: Custom groups created and verified.

4.2 SSH and Password Policies

- Disabled SSH root login in /etc/ssh/sshd_config

- Enforced password complexity using pam_pwquality

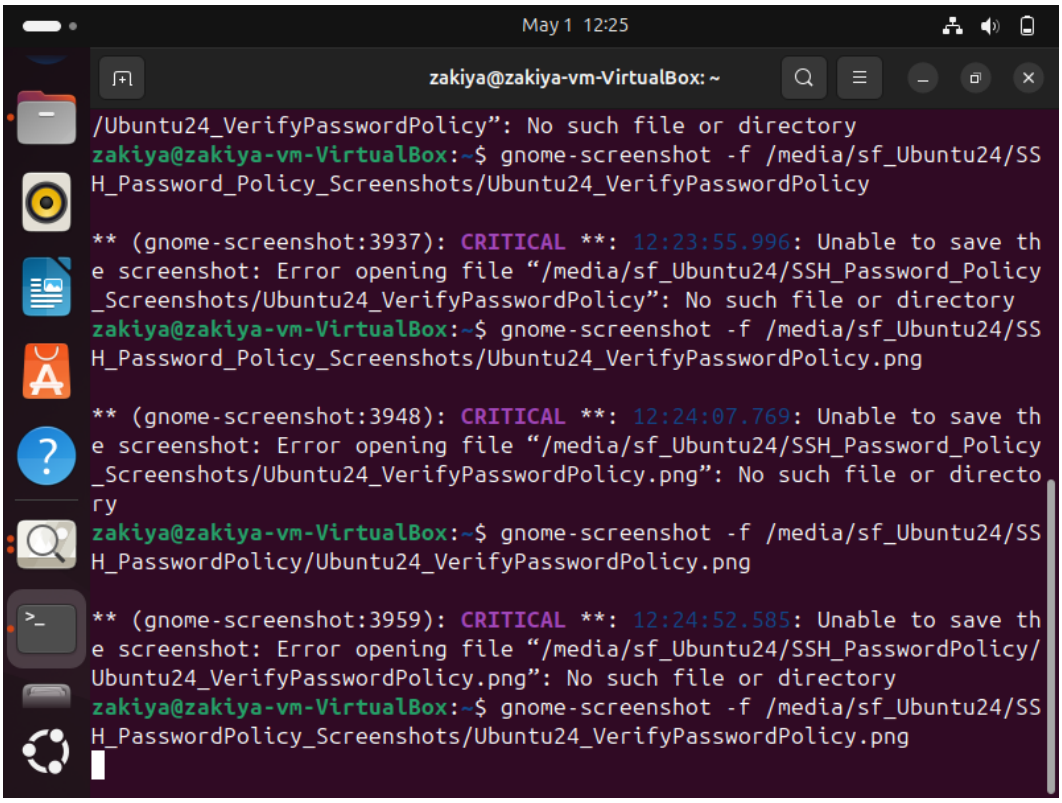

Figure 22: Password complexity enforced via pam_pwquality.

4.3 Firewall (UFW) Configuration

- UFW enabled and configured

- SSH allowed explicitly, all other connections denied by default

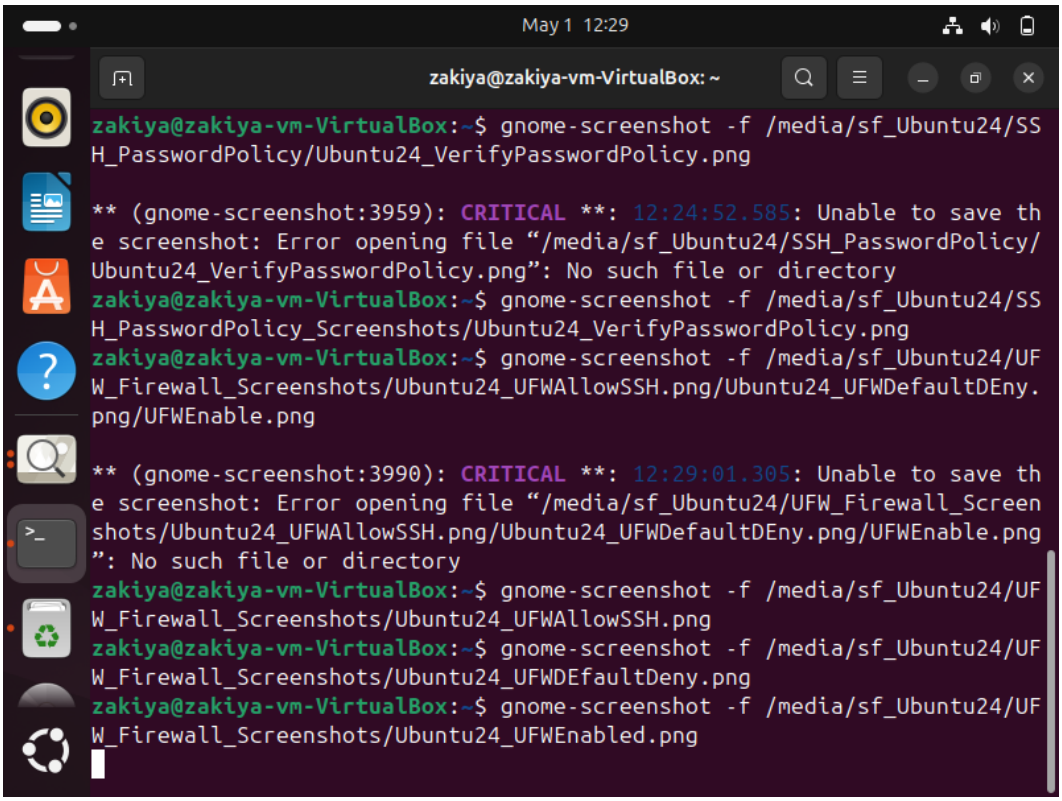

Figure 23: Confirmed UFW is active and enabled.

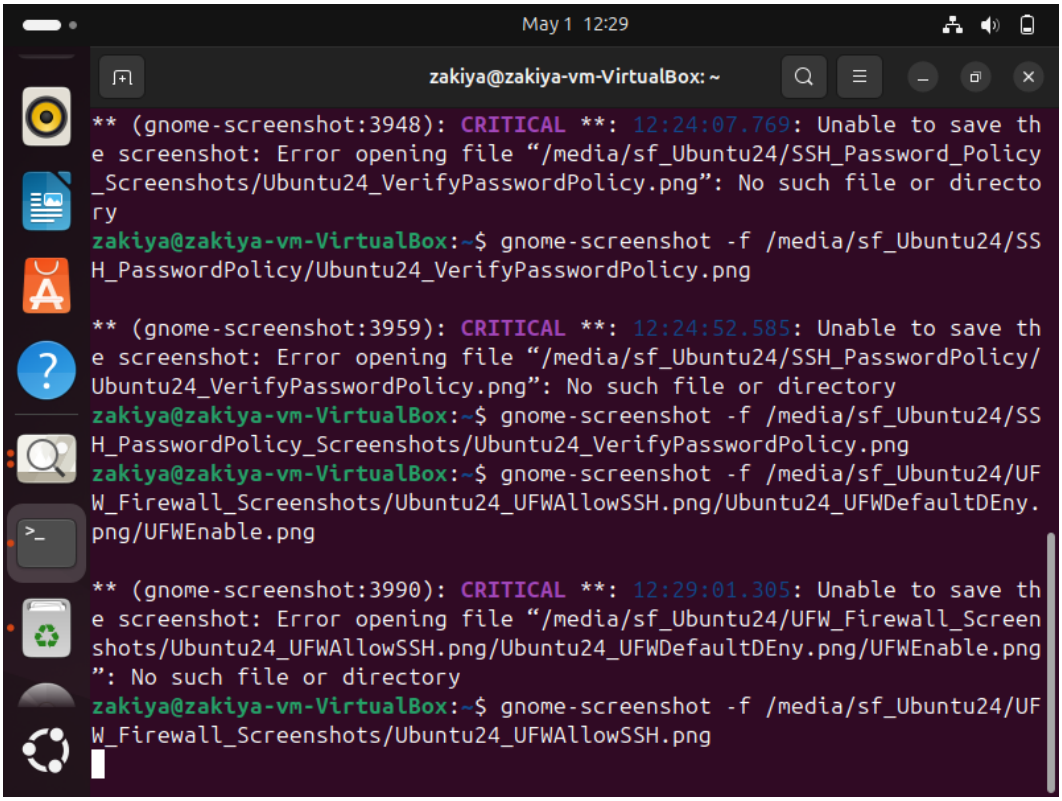

Figure 24: UFW rule to allow SSH configured.

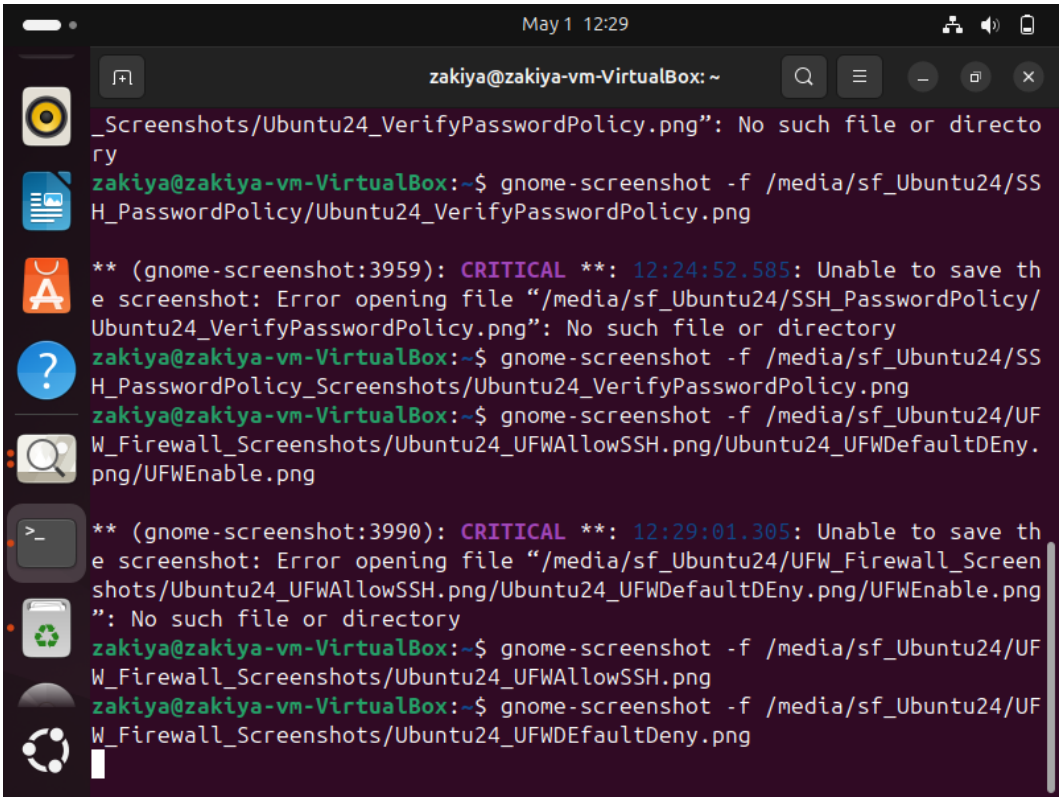

Figure 25: Default UFW policy set to deny incoming connections.

4.4 System Updates

System packages were updated using the apt package manager.

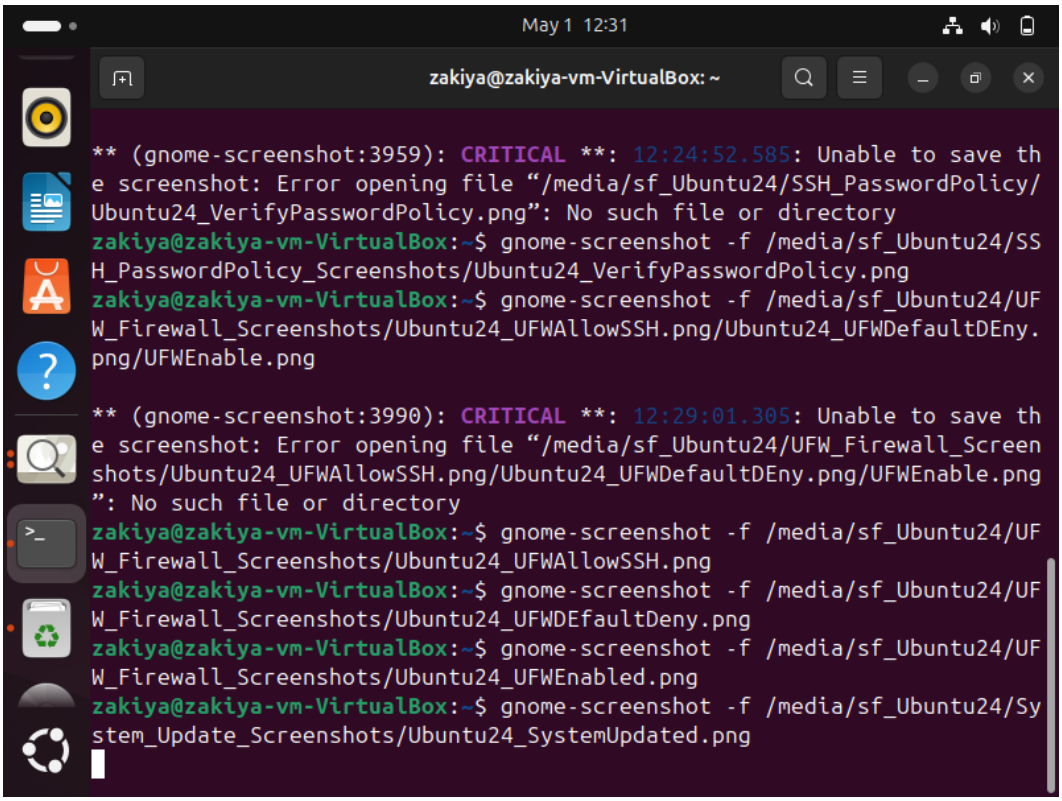

Figure 26: Screenshot showing Ubuntu system updates applied.