

System Hardening Lab Report

Zakiya Moore

April 2025

Table of Contents

1. Introduction
2. Lab Environment
3. Windows 11 System Hardening
 - 3.1 User Account Creation and Management
 - 3.2 Password and Account Lockout Policies
 - 3.3 Services Hardening
 - 3.4 Firewall Configuration and Hardening
 - 3.5 Antivirus and Endpoint Protection
 - 3.6 System Updates
 - 3.7 NTFS Folder Permission Hardening
4. Ubuntu 24.04 System Hardening
 - 4.1 User and Group Management
 - 4.2 SSH and Password Policies
 - 4.3 Firewall (UFW) Configuration
 - 4.4 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, 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)

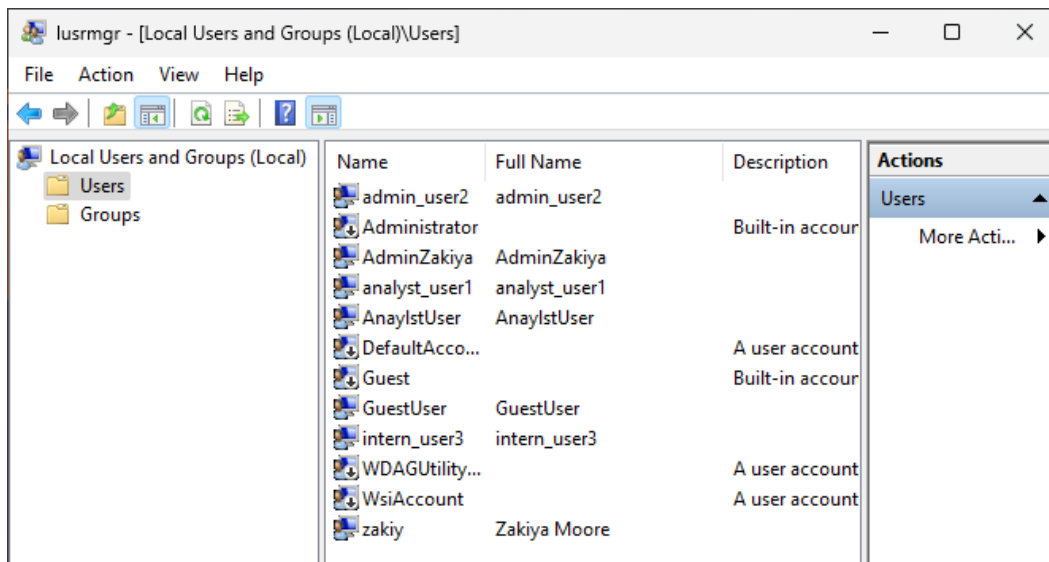


Figure 1: Local users created — AdminZakiya, AnalystUser, GuestUser — in Windows 11 under Local Users and Groups.

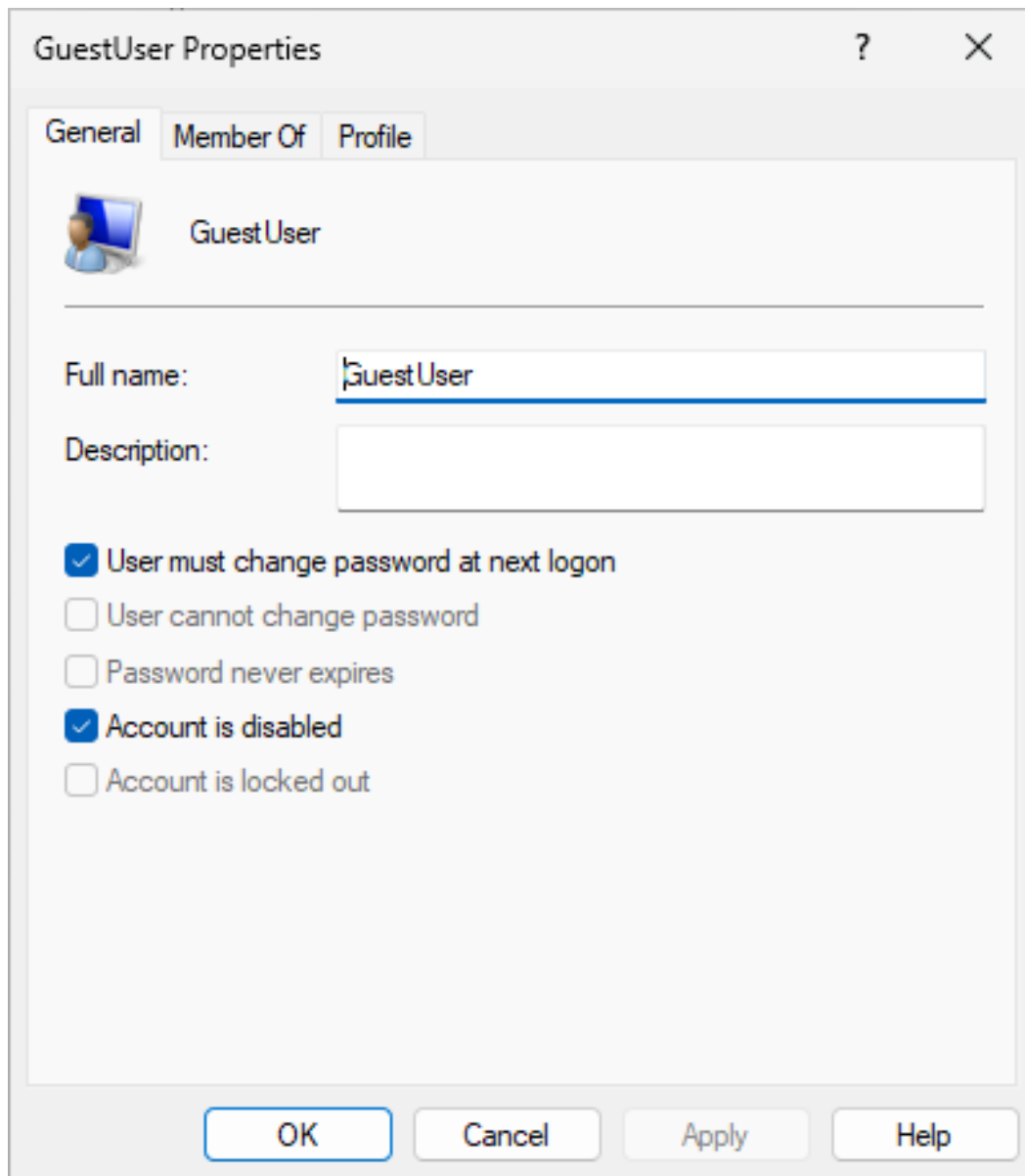


Figure 2: GuestUser account disabled to minimize vulnerabilities.

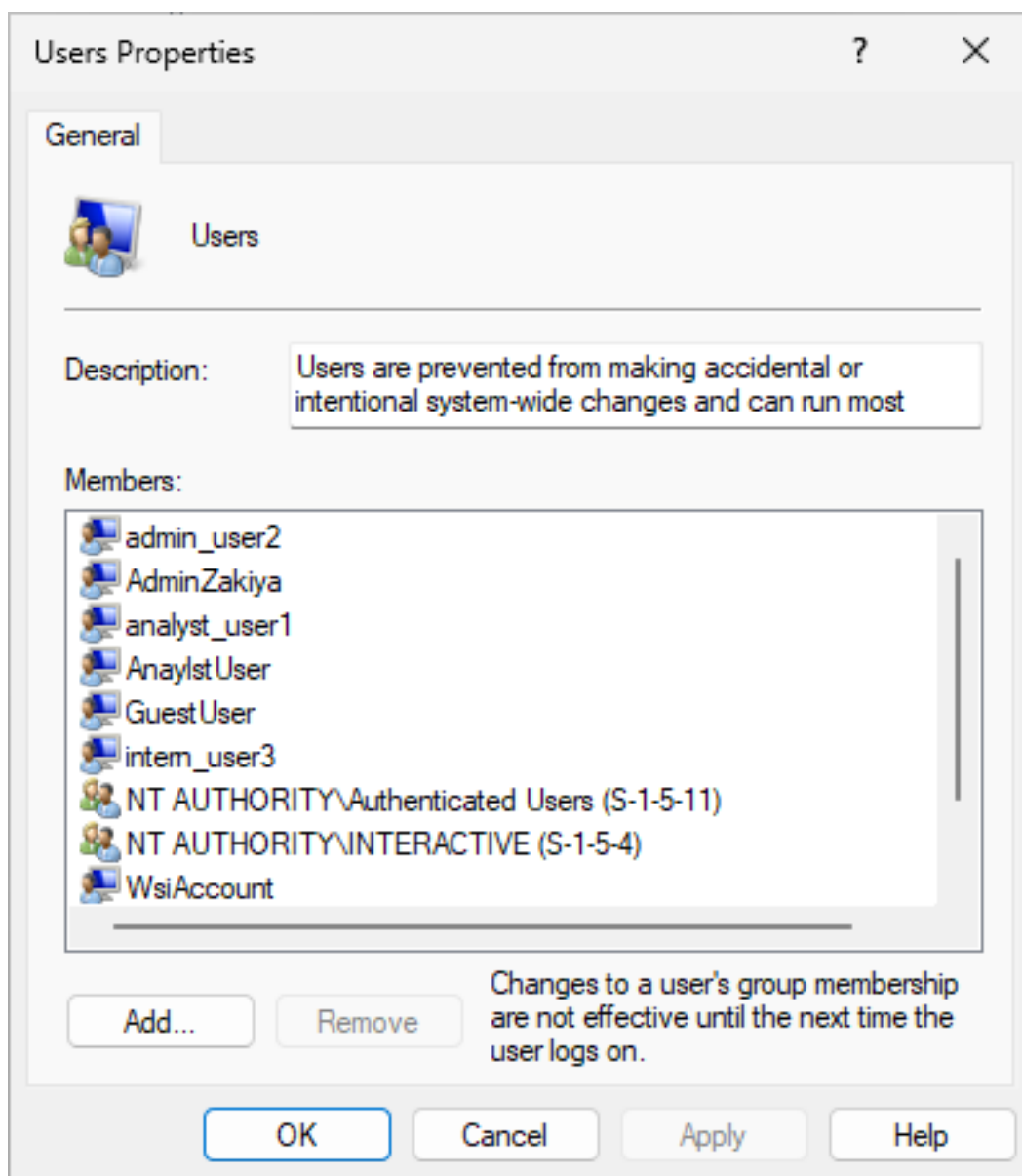


Figure 3: AnalystUser assigned to the Users group for least privilege access.

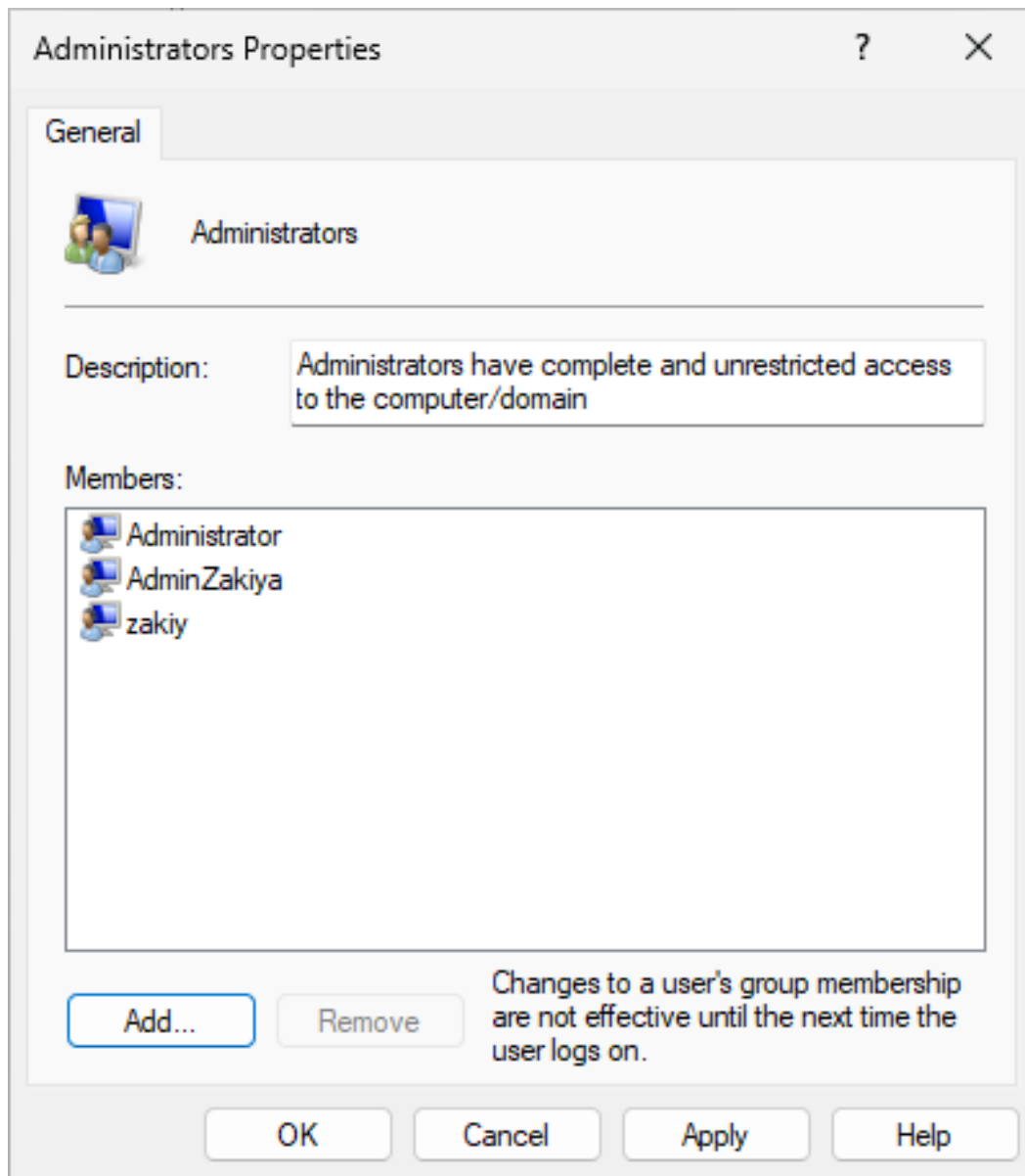


Figure 4: AdminZakiya assigned to the Administrators group with elevated privileges.

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

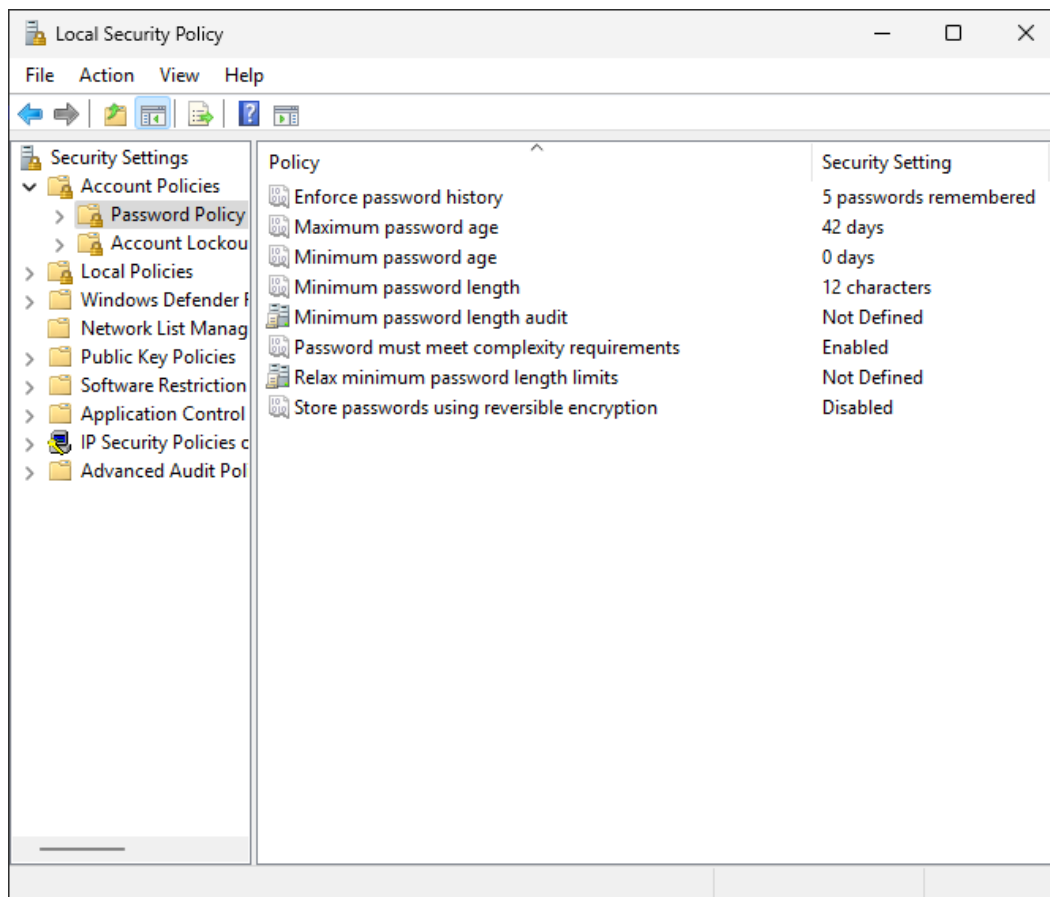


Figure 5: Password policy settings applied using Local Security Policy.

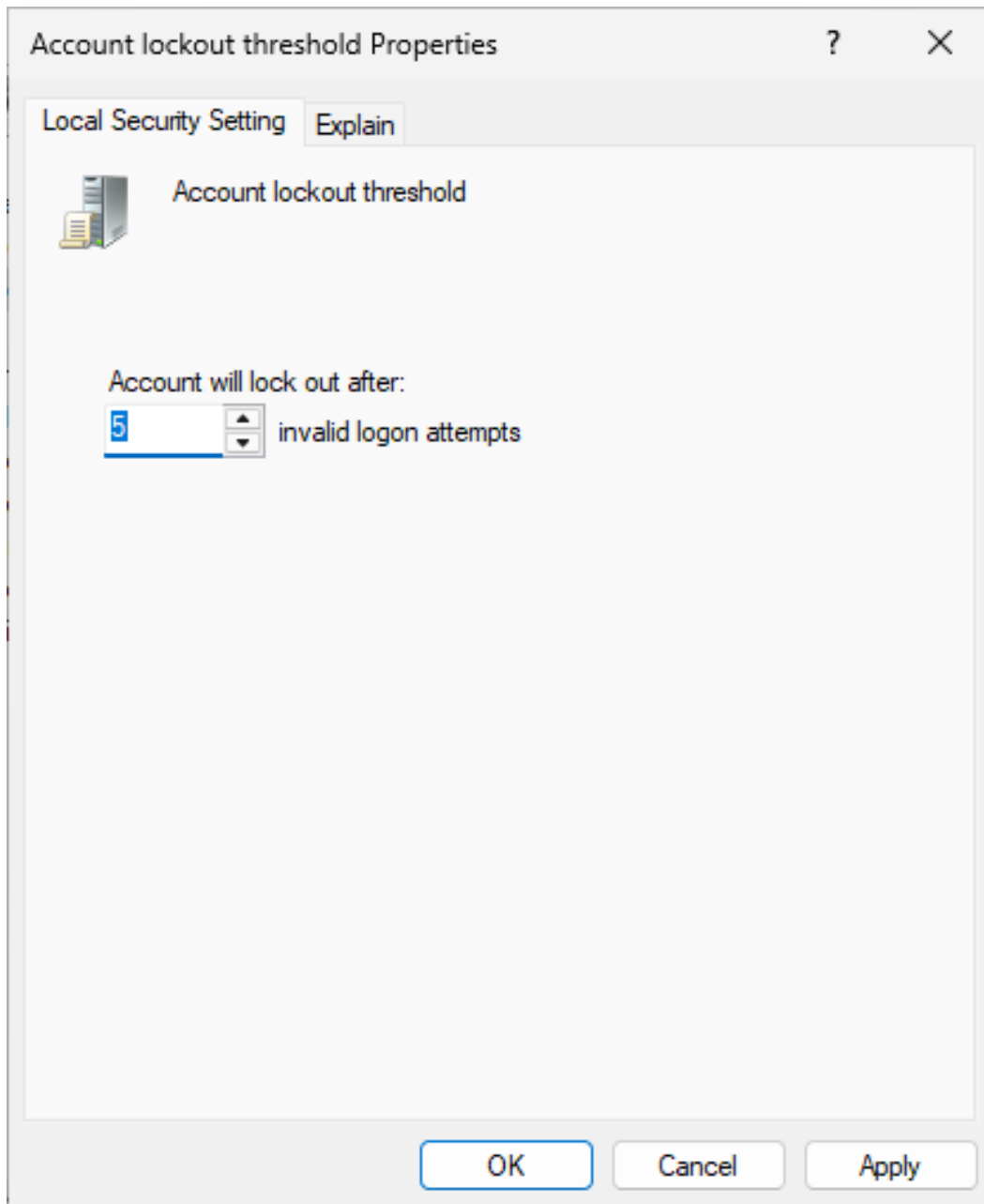


Figure 6: Account lockout threshold set to 5 invalid login attempts.

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.

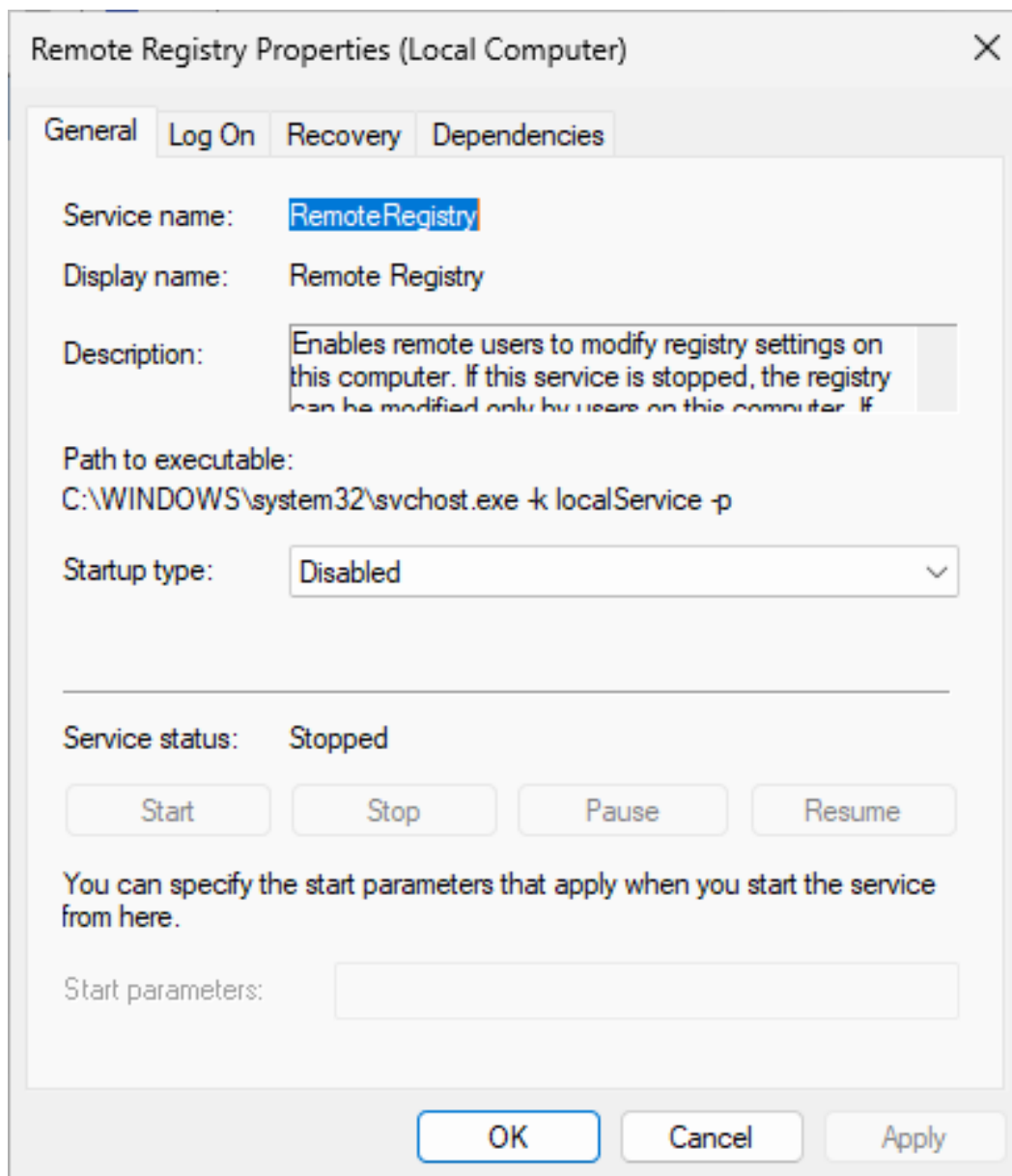


Figure 7: Remote Registry service disabled to prevent remote editing vulnerabilities.

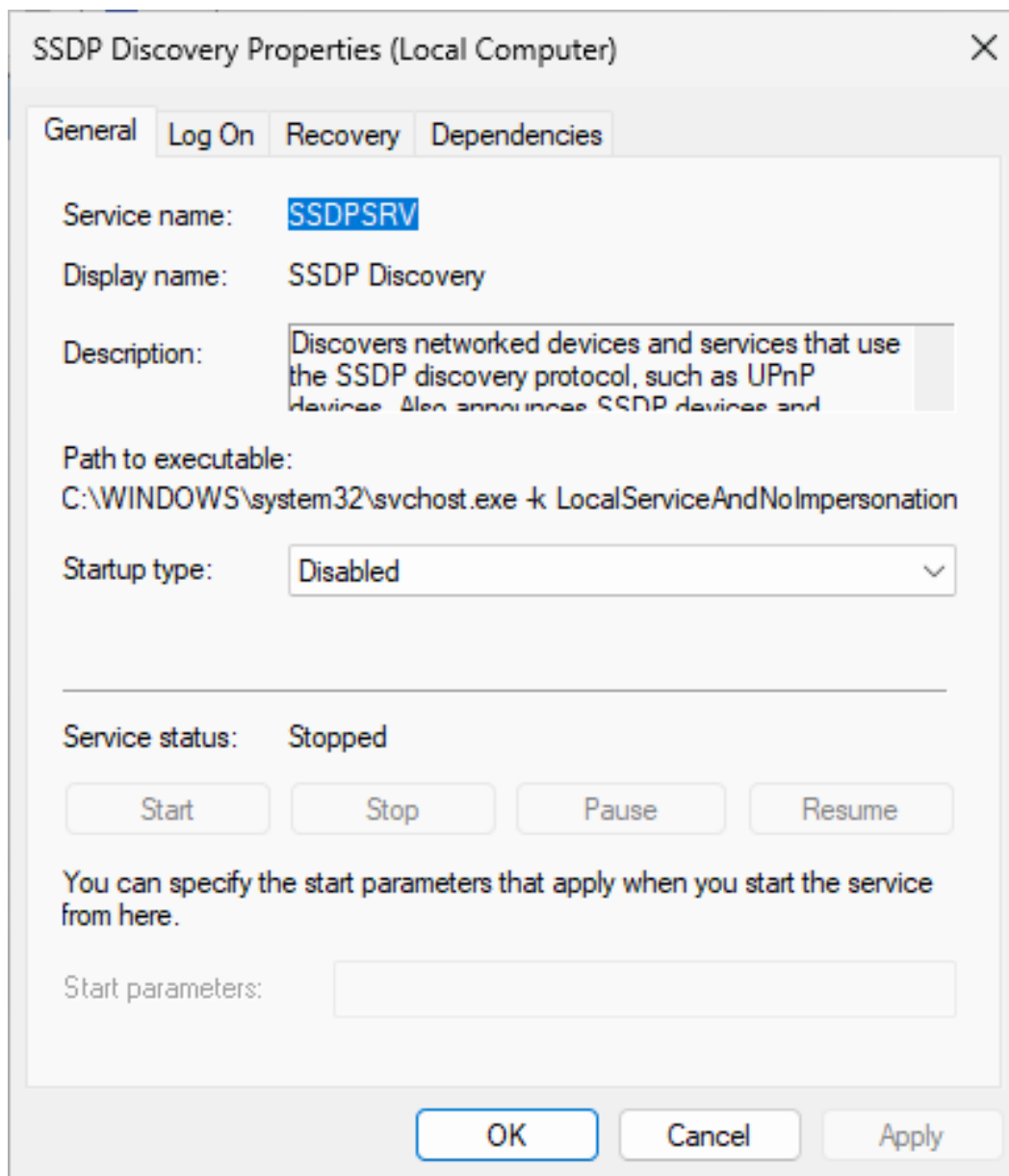


Figure 8: SSDP Discovery service disabled to reduce exposure to UPnP vulnerabilities.

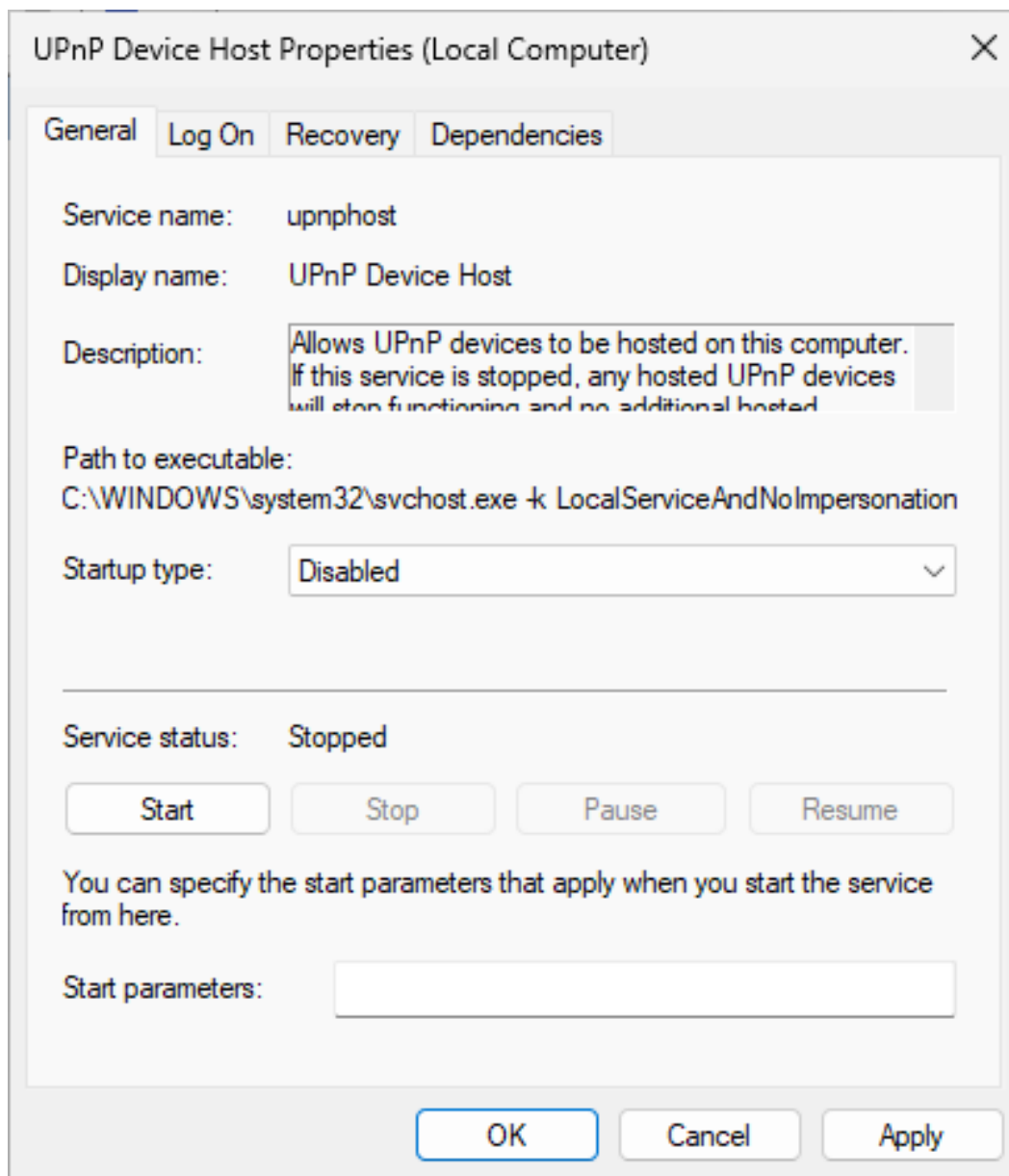


Figure 9: UPnP Device Host service disabled to mitigate auto-discovery risks.

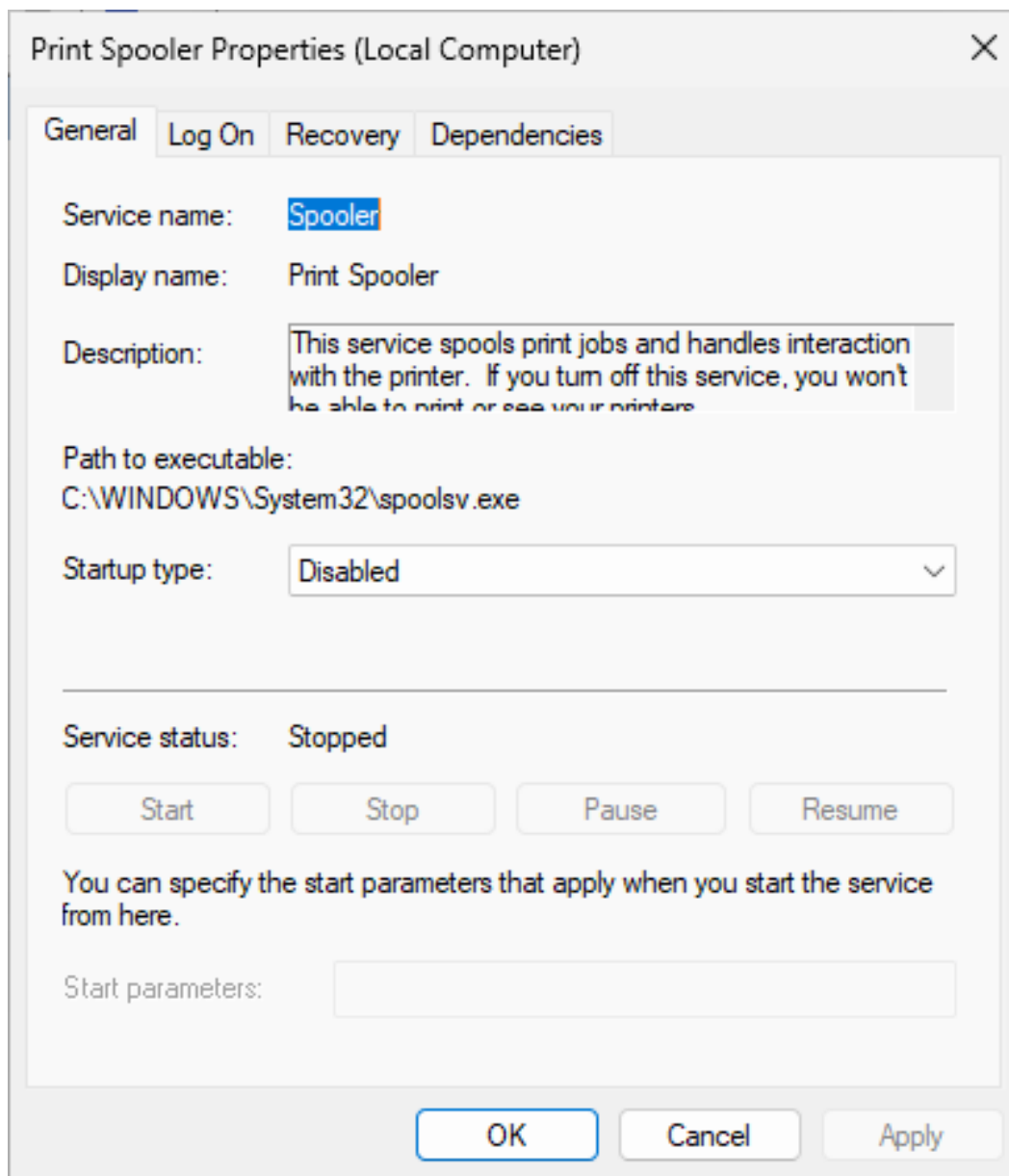


Figure 10: Print Spooler service disabled to reduce risk when printing is not needed.

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

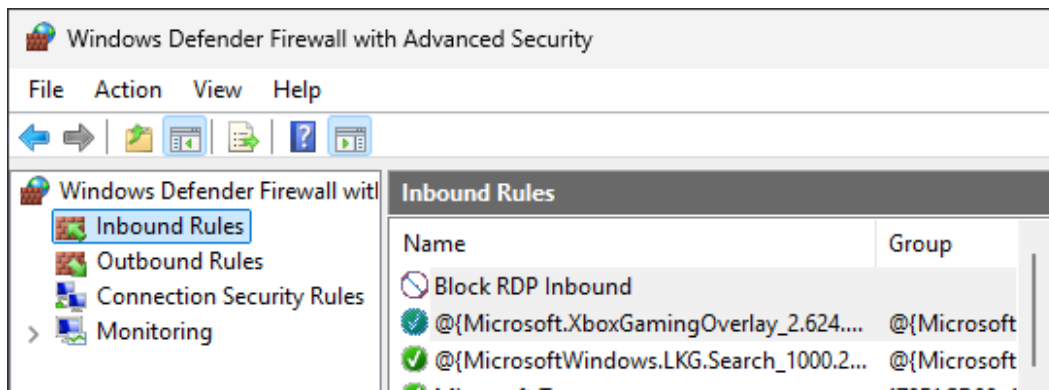


Figure 11: Firewall rule created to block RDP connections.

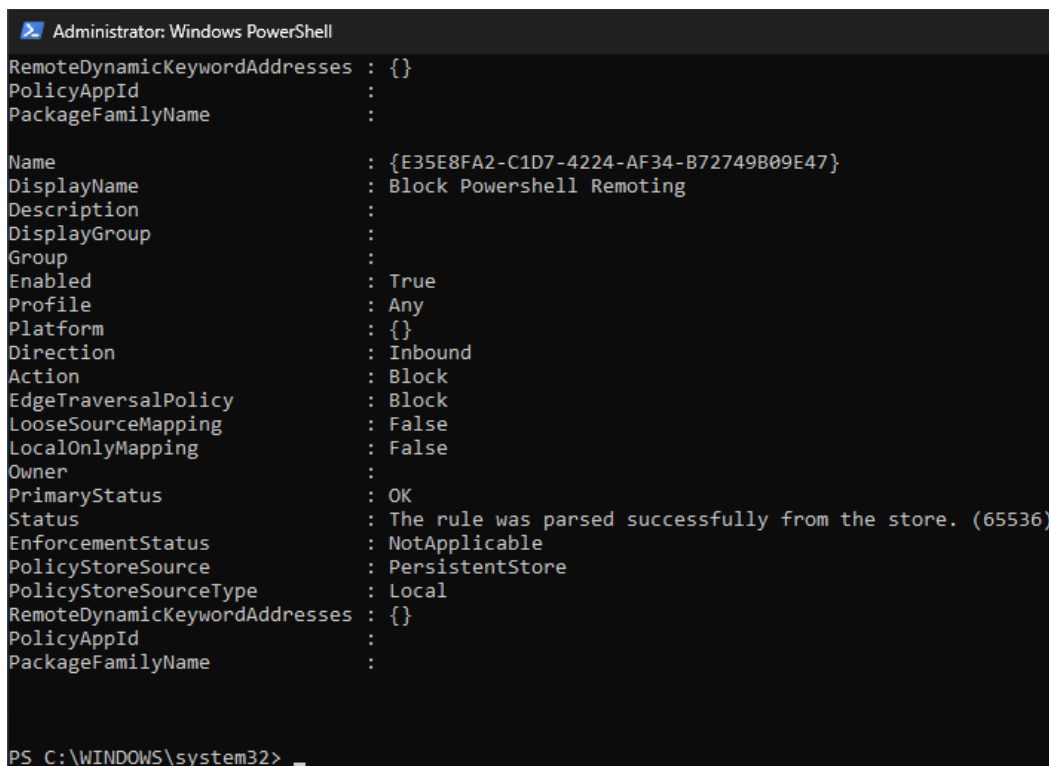


Figure 12: PowerShell Remoting blocked via custom firewall rule.

```
Select Administrator: Windows PowerShell

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\WINDOWS\system32> Get-NetFirewallProfile | Select-Object Name, LogAllowed, LogBlocked, LogFileName
>>

Name      LogAllowed LogBlocked LogFileName
-----
Domain    True       True       C:\Windows\System32\LogFiles\Firewall\pfirewall.log
Private   True       True       %systemroot%\system32\LogFiles\Firewall\pfirewall.log
Public    True       True       %systemroot%\system32\LogFiles\Firewall\pfirewall.log

PS C:\WINDOWS\system32> _
```

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

```
Administrator: Windows PowerShell

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

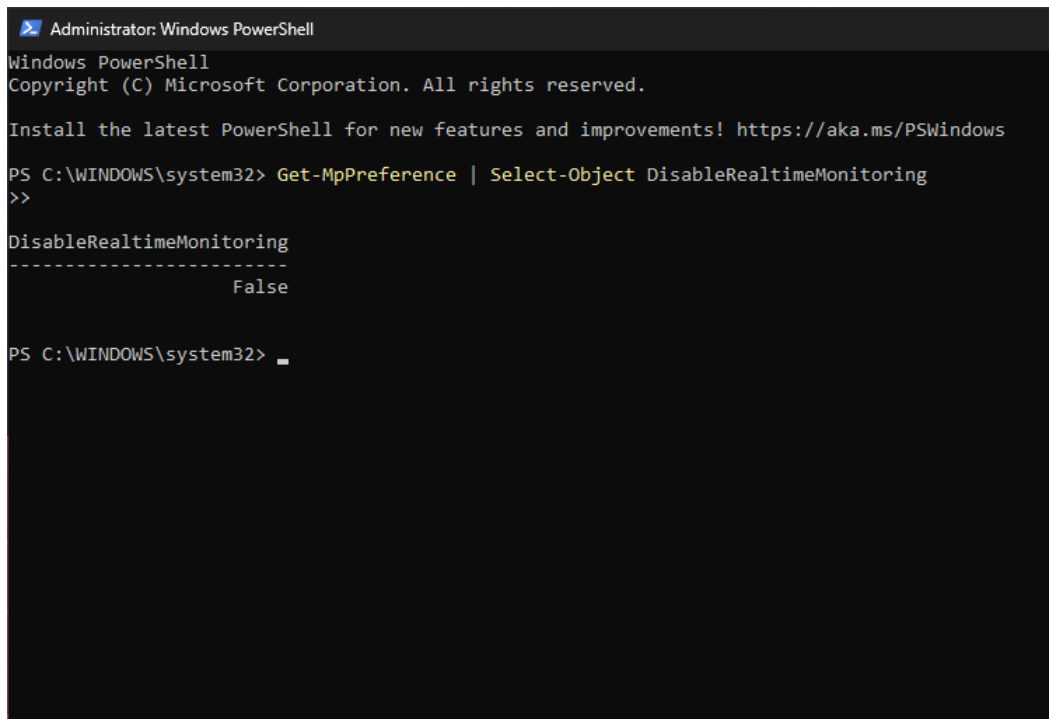
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\WINDOWS\system32> Get-MpComputerStatus | Select-Object AMServiceEnabled, AntivirusSignatureLastUpdated | Format-Table -AutoSize
>>

AMServiceEnabled AntivirusSignatureLastUpdated
-----
True 4/23/2025 2:02:58 AM

PS C:\WINDOWS\system32>
```

Figure 14: Windows Defender active and virus signatures updated.



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\WINDOWS\system32> Get-MpPreference | Select-Object DisableRealtimeMonitoring
>>

DisableRealtimeMonitoring
-----
False

PS C:\WINDOWS\system32> _
```

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)

```

Administrator: Windows PowerShell

Exception
+ FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.SetLocationCommand

PS C:\WINDOWS\system32> cd "C:\System_Hardening_Lab\Windows11\NTFS_Folder_Permissions"
PS C:\System_Hardening_Lab\Windows11\NTFS_Folder_Permissions> dir

Directory: C:\System_Hardening_Lab\Windows11\NTFS_Folder_Permissions

Mode                LastWriteTime         Length Name
----                -
d-----          4/27/2025  11:22 AM             Admin_Tools
d-----          4/27/2025  11:37 AM             Security_Logs
d-----          4/27/2025  11:22 AM             Shared_Documents

PS C:\System_Hardening_Lab\Windows11\NTFS_Folder_Permissions> icacls ".\Admin_Tools" /grant:r "AdminZakiya:(F)"
processed file: .\Admin_Tools
Successfully processed 1 files; Failed processing 0 files
PS C:\System_Hardening_Lab\Windows11\NTFS_Folder_Permissions> icacls ".\Admin_Tools"
.\Admin_Tools Zakiya\AdminZakiya:(F)
BUILTIN\Administrators:(I)(OI)(CI)(F)
NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
BUILTIN\Users:(I)(OI)(CI)(RX)
NT AUTHORITY\Authenticated Users:(I)(M)
NT AUTHORITY\Authenticated Users:(I)(OI)(CI)(IO)(M)

Successfully processed 1 files; Failed processing 0 files
PS C:\System_Hardening_Lab\Windows11\NTFS_Folder_Permissions>

```

Figure 16: NTFS permissions for Admin_Tools.

```

Administrator: Windows PowerShell

ons"
>>
PS C:\System_Hardening_Lab\Windows11\NTFS_Folder_Permissions> dir

Directory: C:\System_Hardening_Lab\Windows11\NTFS_Folder_Permissions

Mode                LastWriteTime         Length Name
----                -
d-----          4/27/2025  11:22 AM             Admin_Tools
d-----          4/27/2025  11:27 AM             Security_Logs
d-----          4/27/2025  11:22 AM             Shared_Documents

PS C:\System_Hardening_Lab\Windows11\NTFS_Folder_Permissions> icacls ".\Security_Logs" /grant:r "AdminZakiya:(F)"
>>
processed file: .\Security_Logs
Successfully processed 1 files; Failed processing 0 files
PS C:\System_Hardening_Lab\Windows11\NTFS_Folder_Permissions> icacls ".\Security_Logs"
>>
.\Security_Logs Zakiya\AdminZakiya:(F)
BUILTIN\Administrators:(I)(OI)(CI)(F)
NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
BUILTIN\Users:(I)(OI)(CI)(RX)
NT AUTHORITY\Authenticated Users:(I)(M)
NT AUTHORITY\Authenticated Users:(I)(OI)(CI)(IO)(M)

Successfully processed 1 files; Failed processing 0 files
PS C:\System_Hardening_Lab\Windows11\NTFS_Folder_Permissions>

```

Figure 17: NTFS permissions for Security_Logs.


```
Administrator: Windows PowerShell
Audit :
Sddl : O:BAG:S-1-5-21-3588953516-3756221534-520319812-1001D:AI(A;;FA;;;S-1-5-21-3588953516-3756221534-520319812-1016)
(A;OICIID;FA;;;BA)(A;OICIID;FA;;;SY)(A;OICIID;0x1200a9;;;BU)(A;ID;0x1301bf;;;AU)(A;OICIIOID;SDGXGWR;;;AU)

Path : Microsoft.PowerShell.Core\FileSystem::C:\System_Hardening_Lab\Windows11\NTFS_Folder_Permissions\Shared_Documen
ts
Owner : BUILTIN\Administrators
Group : ZAKIYA\zakiy
Access : Zakiya\AdminZakiya Allow Modify, Synchronize
Zakiya\AnalystUser Allow Modify, Synchronize
BUILTIN\Administrators Allow FullControl
NT AUTHORITY\SYSTEM Allow FullControl
BUILTIN\Users Allow ReadAndExecute, Synchronize
NT AUTHORITY\Authenticated Users Allow Modify, Synchronize
NT AUTHORITY\Authenticated Users Allow -536805376

Audit :
Sddl : O:BAG:S-1-5-21-3588953516-3756221534-520319812-1001D:AI(A;;0x1301bf;;;S-1-5-21-3588953516-3756221534-520319812
-1016)(A;;0x1301bf;;;S-1-5-21-3588953516-3756221534-520319812-1019)(A;OICIID;FA;;;BA)(A;OICIID;FA;;;SY)(A;OICI
ID;0x1200a9;;;BU)(A;ID;0x1301bf;;;AU)(A;OICIIOID;SDGXGWR;;;AU)
```

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)

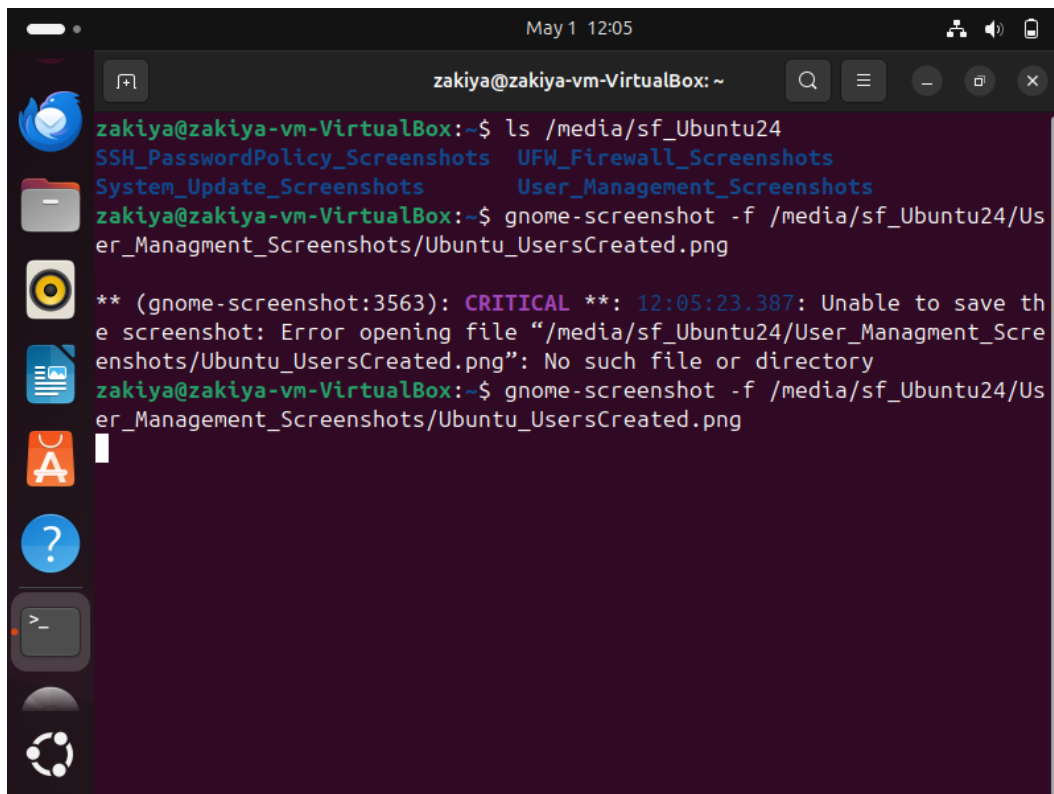


Figure 19: Created Ubuntu users: adminzakiya, analystuser, guestuser.

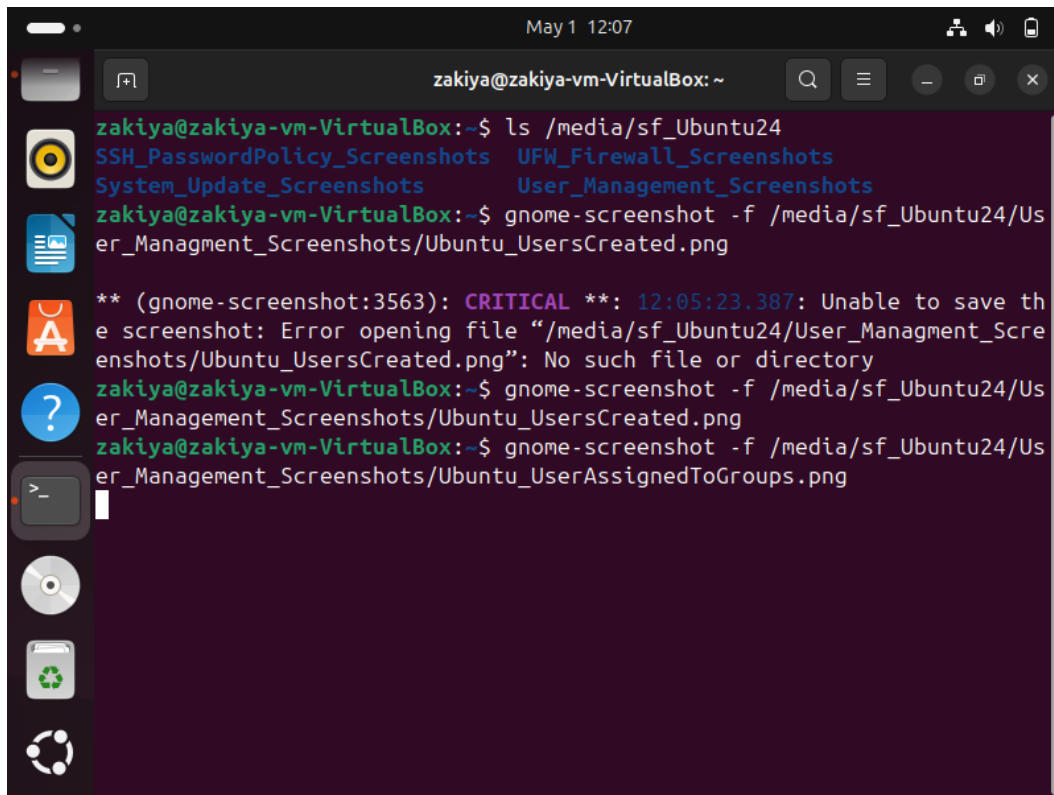


Figure 20: Assigned users to groups for least privilege access.

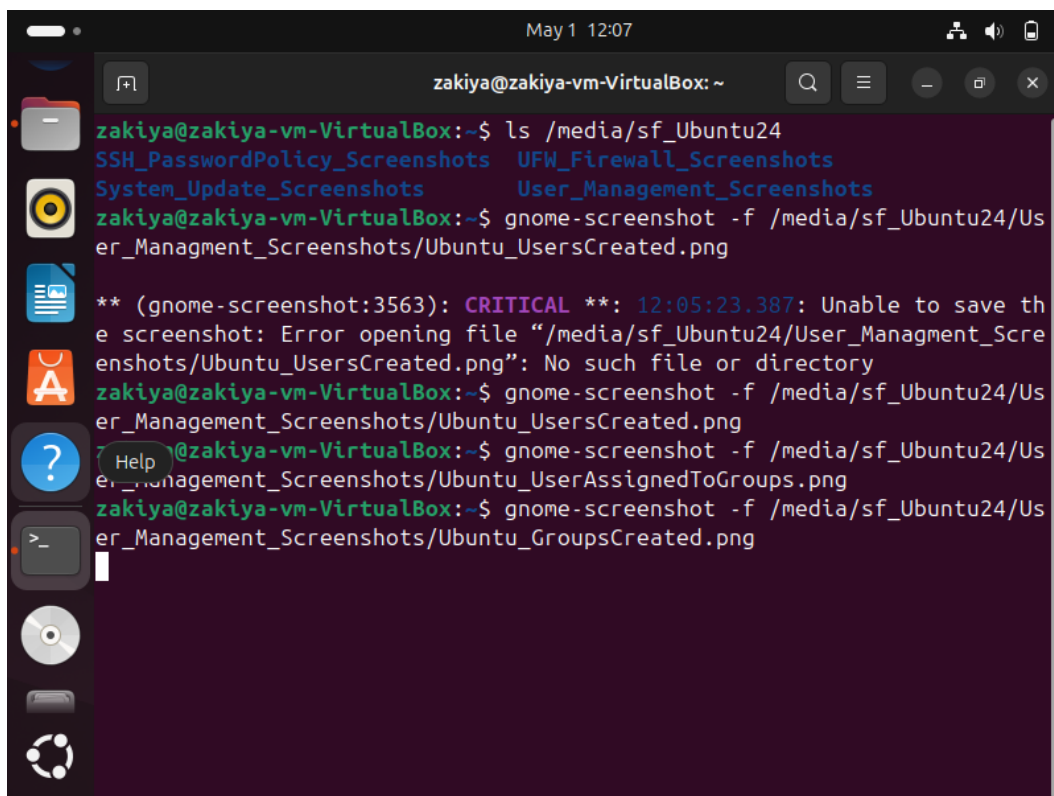


Figure 21: Custom groups created and verified.

4.2 SSH and Password Policies

- Disabled SSH root login in `/etc/ssh/sshd_config`
- Enforced password complexity using `pam_pwquality`

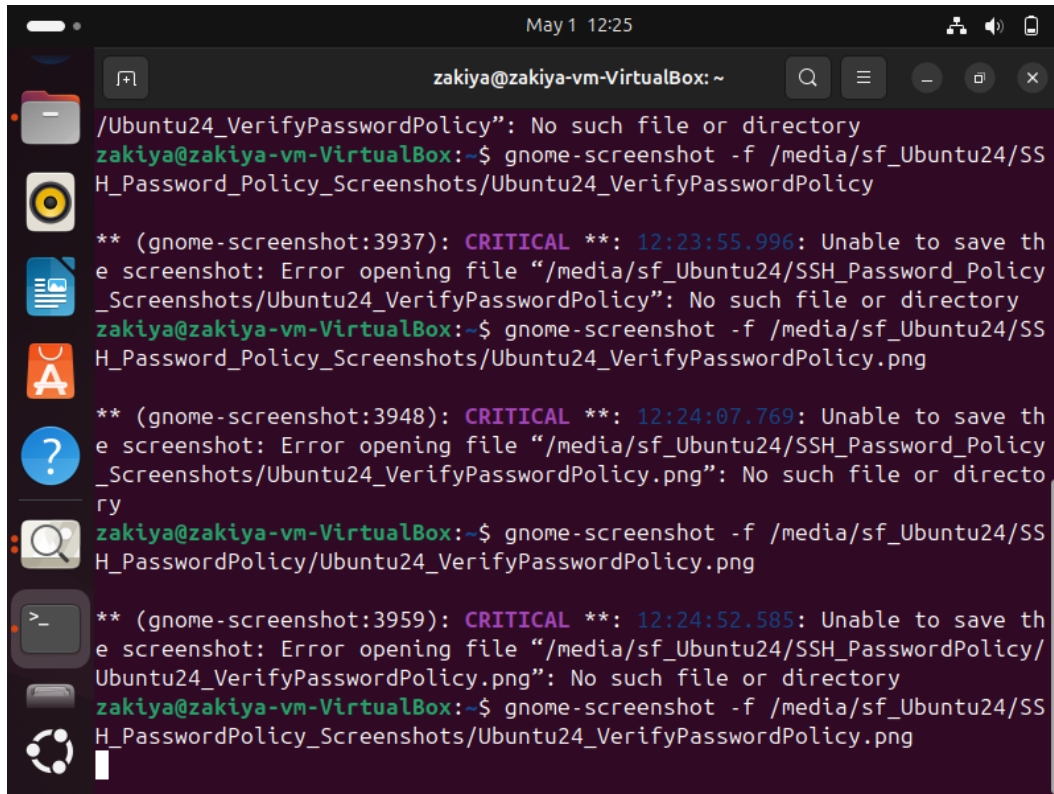


Figure 22: Password complexity enforced via `pam_pwquality`.

4.3 Firewall (UFW) Configuration

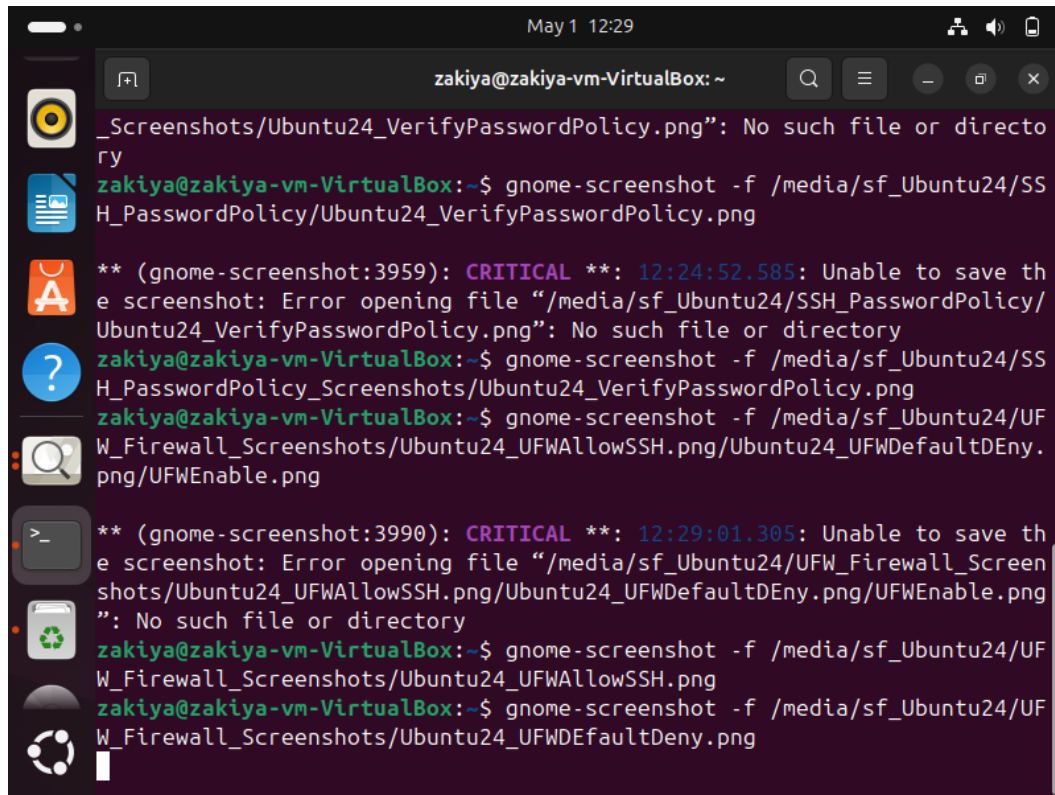
- UFW enabled and configured
- SSH allowed explicitly, all other connections denied by default

```
May 1 12:29
zakiya@zakiya-vm-VirtualBox: ~
zakiya@zakiya-vm-VirtualBox:~$ gnome-screenshot -f /media/sf_Ubuntu24/SSH_PasswordPolicy/Ubuntu24_VerifyPasswordPolicy.png
** (gnome-screenshot:3959): CRITICAL **: 12:24:52.585: Unable to save the screenshot: Error opening file "/media/sf_Ubuntu24/SSH_PasswordPolicy/Ubuntu24_VerifyPasswordPolicy.png": No such file or directory
zakiya@zakiya-vm-VirtualBox:~$ gnome-screenshot -f /media/sf_Ubuntu24/SSH_PasswordPolicy_Screenshots/Ubuntu24_VerifyPasswordPolicy.png
zakiya@zakiya-vm-VirtualBox:~$ gnome-screenshot -f /media/sf_Ubuntu24/UFW_Firewall_Screenshots/Ubuntu24_UFWAllowSSH.png/Ubuntu24_UFWDefaultDeny.png/UFWEnable.png
** (gnome-screenshot:3990): CRITICAL **: 12:29:01.305: Unable to save the screenshot: Error opening file "/media/sf_Ubuntu24/UFW_Firewall_Screenshots/Ubuntu24_UFWAllowSSH.png/Ubuntu24_UFWDefaultDeny.png/UFWEnable.png": No such file or directory
zakiya@zakiya-vm-VirtualBox:~$ gnome-screenshot -f /media/sf_Ubuntu24/UFW_Firewall_Screenshots/Ubuntu24_UFWAllowSSH.png
zakiya@zakiya-vm-VirtualBox:~$ gnome-screenshot -f /media/sf_Ubuntu24/UFW_Firewall_Screenshots/Ubuntu24_UFWDefaultDeny.png
zakiya@zakiya-vm-VirtualBox:~$ gnome-screenshot -f /media/sf_Ubuntu24/UFW_Firewall_Screenshots/Ubuntu24_UFWEnabled.png
```

Figure 23: Confirmed UFW is active and enabled.

```
May 1 12:29
zakiya@zakiya-vm-VirtualBox: ~
** (gnome-screenshot:3948): CRITICAL **: 12:24:07.769: Unable to save the screenshot: Error opening file "/media/sf_Ubuntu24/SSH_PasswordPolicy_Screenshots/Ubuntu24_VerifyPasswordPolicy.png": No such file or directory
zakiya@zakiya-vm-VirtualBox:~$ gnome-screenshot -f /media/sf_Ubuntu24/SSH_PasswordPolicy/Ubuntu24_VerifyPasswordPolicy.png
** (gnome-screenshot:3959): CRITICAL **: 12:24:52.585: Unable to save the screenshot: Error opening file "/media/sf_Ubuntu24/SSH_PasswordPolicy/Ubuntu24_VerifyPasswordPolicy.png": No such file or directory
zakiya@zakiya-vm-VirtualBox:~$ gnome-screenshot -f /media/sf_Ubuntu24/SSH_PasswordPolicy_Screenshots/Ubuntu24_VerifyPasswordPolicy.png
zakiya@zakiya-vm-VirtualBox:~$ gnome-screenshot -f /media/sf_Ubuntu24/UFW_Firewall_Screenshots/Ubuntu24_UFWAllowSSH.png/Ubuntu24_UFWDefaultDeny.png/UFWEnable.png
** (gnome-screenshot:3990): CRITICAL **: 12:29:01.305: Unable to save the screenshot: Error opening file "/media/sf_Ubuntu24/UFW_Firewall_Screenshots/Ubuntu24_UFWAllowSSH.png/Ubuntu24_UFWDefaultDeny.png/UFWEnable.png": No such file or directory
zakiya@zakiya-vm-VirtualBox:~$ gnome-screenshot -f /media/sf_Ubuntu24/UFW_Firewall_Screenshots/Ubuntu24_UFWAllowSSH.png
```

Figure 24: UFW rule to allow SSH configured.



The image shows a terminal window titled 'zakiya@zakiya-vm-VirtualBox: ~' with a timestamp of 'May 1 12:29'. The terminal displays the following commands and outputs:

```
_Screenshots/Ubuntu24_VerifyPasswordPolicy.png": No such file or directory
zakiya@zakiya-vm-VirtualBox:~$ gnome-screenshot -f /media/sf_Ubuntu24/SSH_PasswordPolicy/Ubuntu24_VerifyPasswordPolicy.png
** (gnome-screenshot:3959): CRITICAL **: 12:24:52.585: Unable to save the screenshot: Error opening file "/media/sf_Ubuntu24/SSH_PasswordPolicy/Ubuntu24_VerifyPasswordPolicy.png": No such file or directory
zakiya@zakiya-vm-VirtualBox:~$ gnome-screenshot -f /media/sf_Ubuntu24/SSH_PasswordPolicy_Screenshots/Ubuntu24_VerifyPasswordPolicy.png
zakiya@zakiya-vm-VirtualBox:~$ gnome-screenshot -f /media/sf_Ubuntu24/UFW_Firewall_Screenshots/Ubuntu24_UFWAllowSSH.png/Ubuntu24_UFWDefaultDeny.png/UFWEnable.png
** (gnome-screenshot:3990): CRITICAL **: 12:29:01.305: Unable to save the screenshot: Error opening file "/media/sf_Ubuntu24/UFW_Firewall_Screenshots/Ubuntu24_UFWAllowSSH.png/Ubuntu24_UFWDefaultDeny.png/UFWEnable.png": No such file or directory
zakiya@zakiya-vm-VirtualBox:~$ gnome-screenshot -f /media/sf_Ubuntu24/UFW_Firewall_Screenshots/Ubuntu24_UFWAllowSSH.png
zakiya@zakiya-vm-VirtualBox:~$ gnome-screenshot -f /media/sf_Ubuntu24/UFW_Firewall_Screenshots/Ubuntu24_UFWDefaultDeny.png
```

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

4.4 System Updates

System packages were updated using the apt package manager.

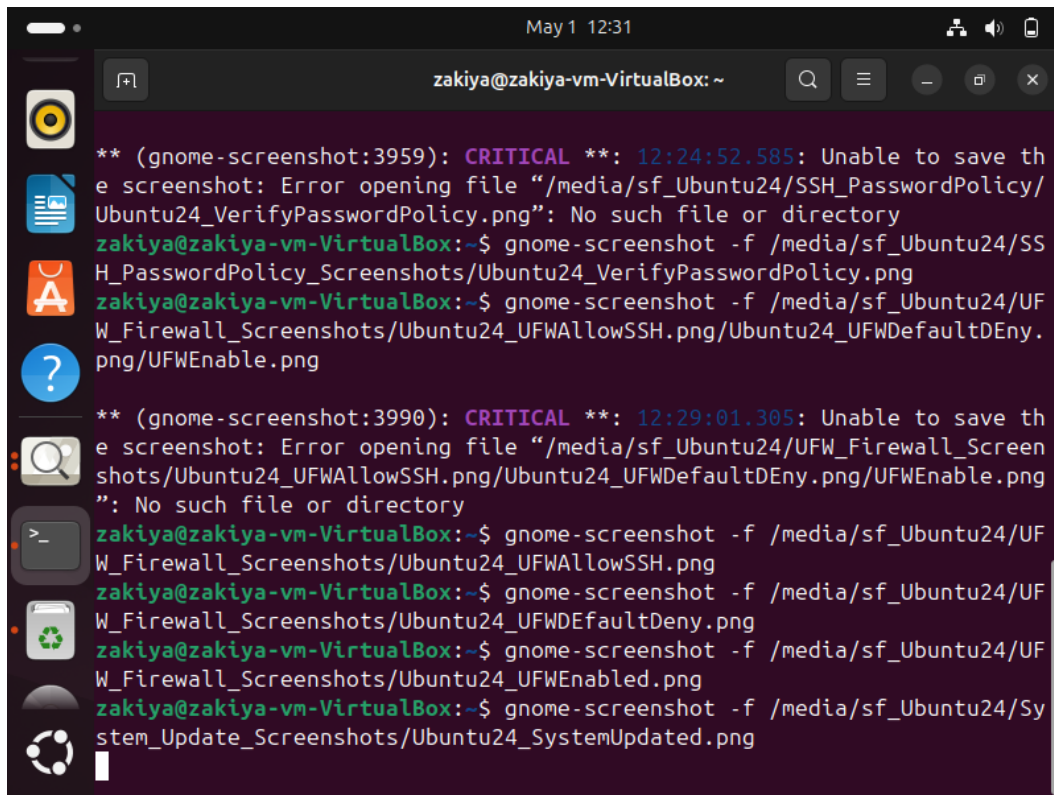


Figure 26: Screenshot showing Ubuntu system updates applied.