

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

⚠ 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)

Name	Full Name	Description	Actions
admin_user2	admin_user2	Built-in account	Users
Administrator			
AdminZakiya	AdminZakiya		
analyst_user1	analyst_user1		
AnaylstUser	AnaylstUser		
DefaultAcco...		A user account	
Guest		Built-in account	
GuestUser	GuestUser		
intern_user3	intern_user3		
WDAGUtility...		A user account	
WsiAccount		A user account	
zakiy	Zakiya Moore		

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

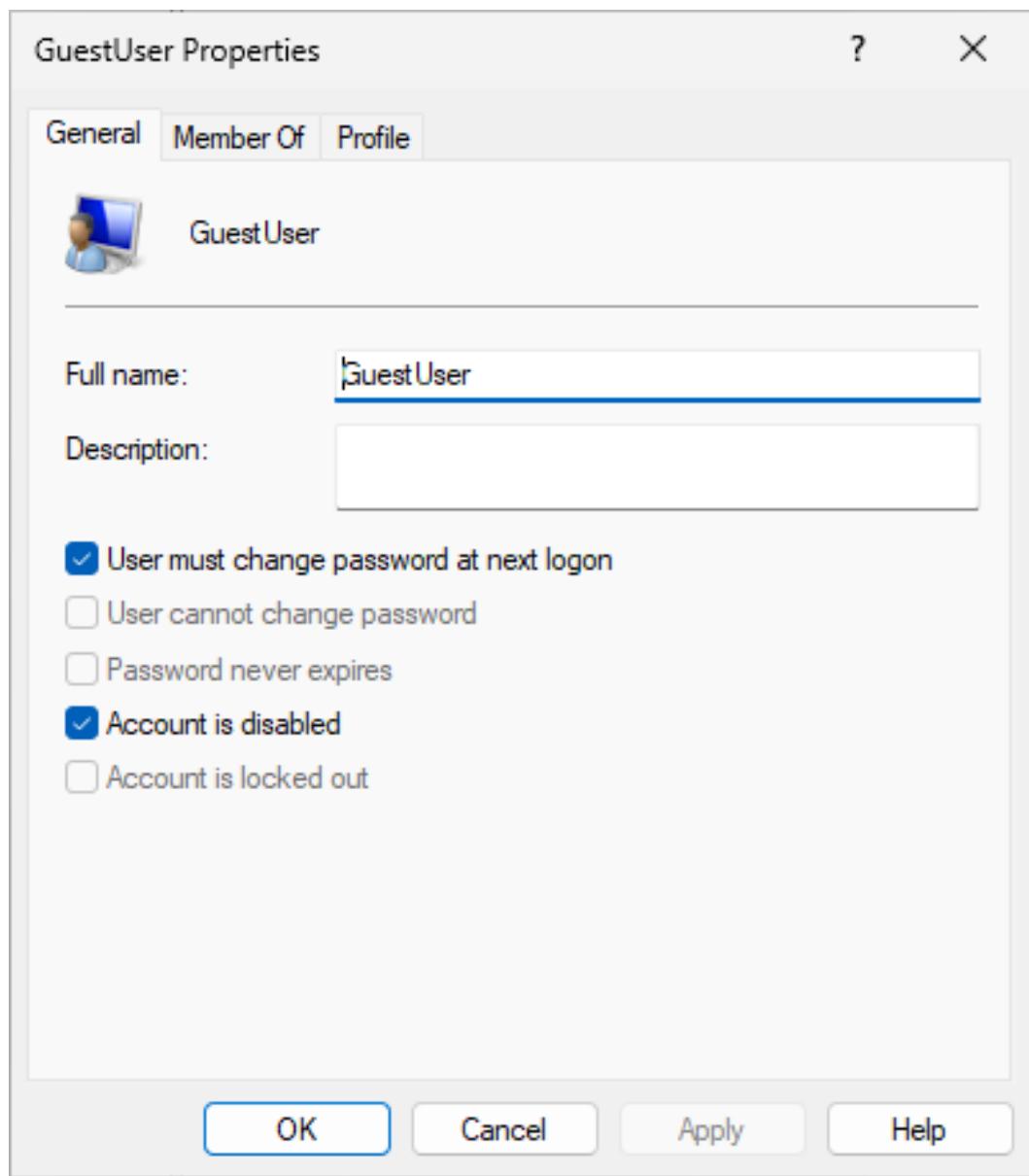


Figure 2: GuestUser account disabled to minimize vulnerabilities.

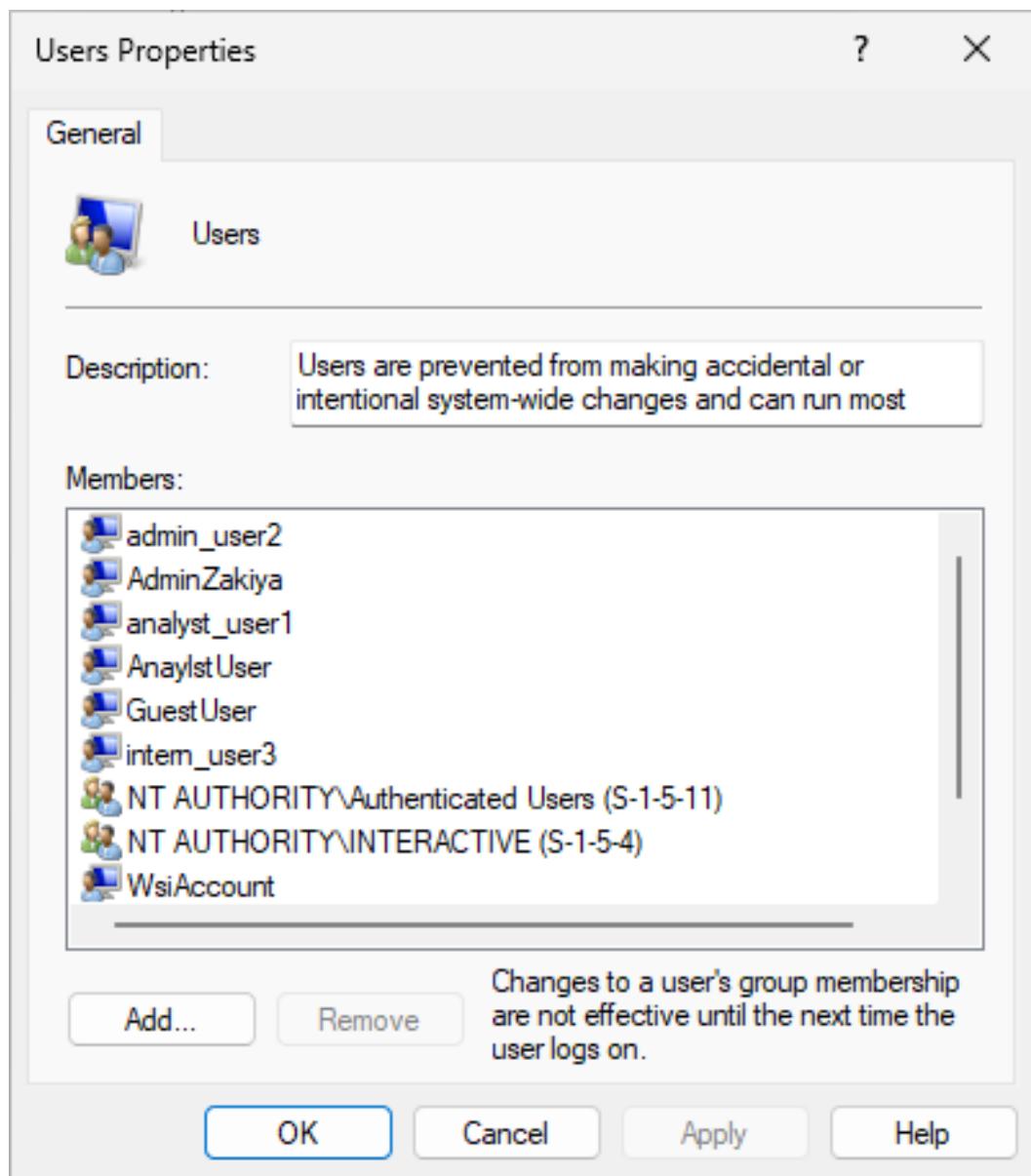


Figure 3: AnalystUser assigned to the Users group for least privilege access.

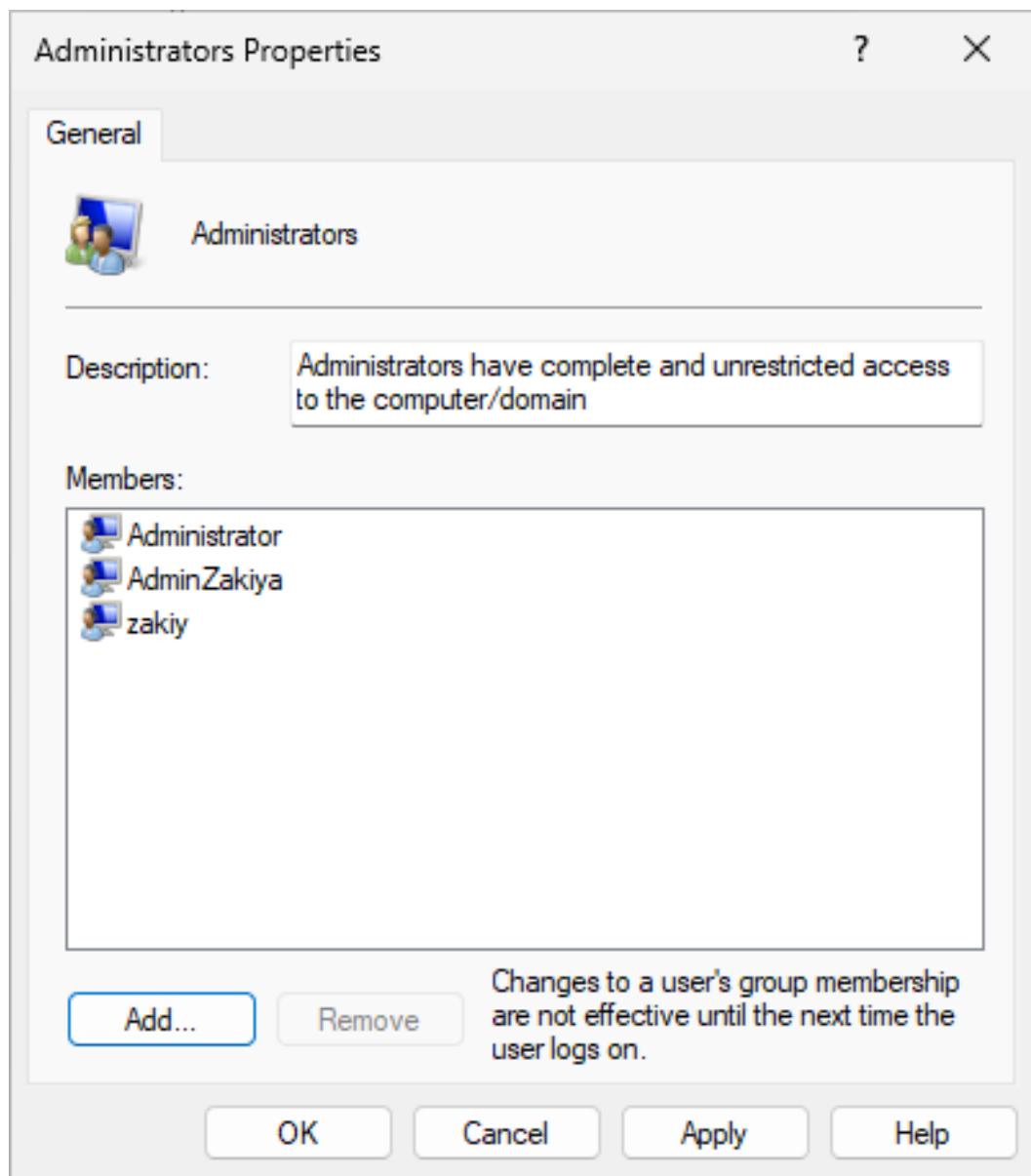


Figure 4: AdminZakiya assigned to the Administrators group with elevated privileges.

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

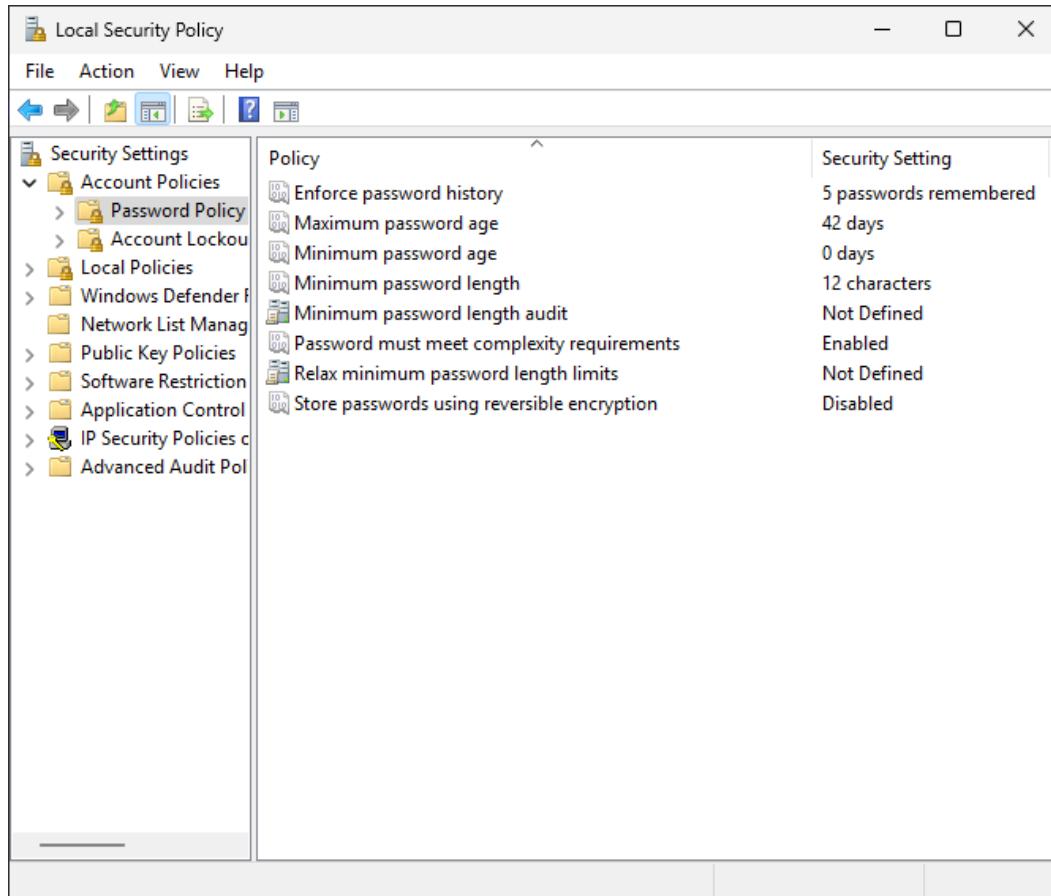


Figure 5: Password policy settings applied using Local Security Policy.

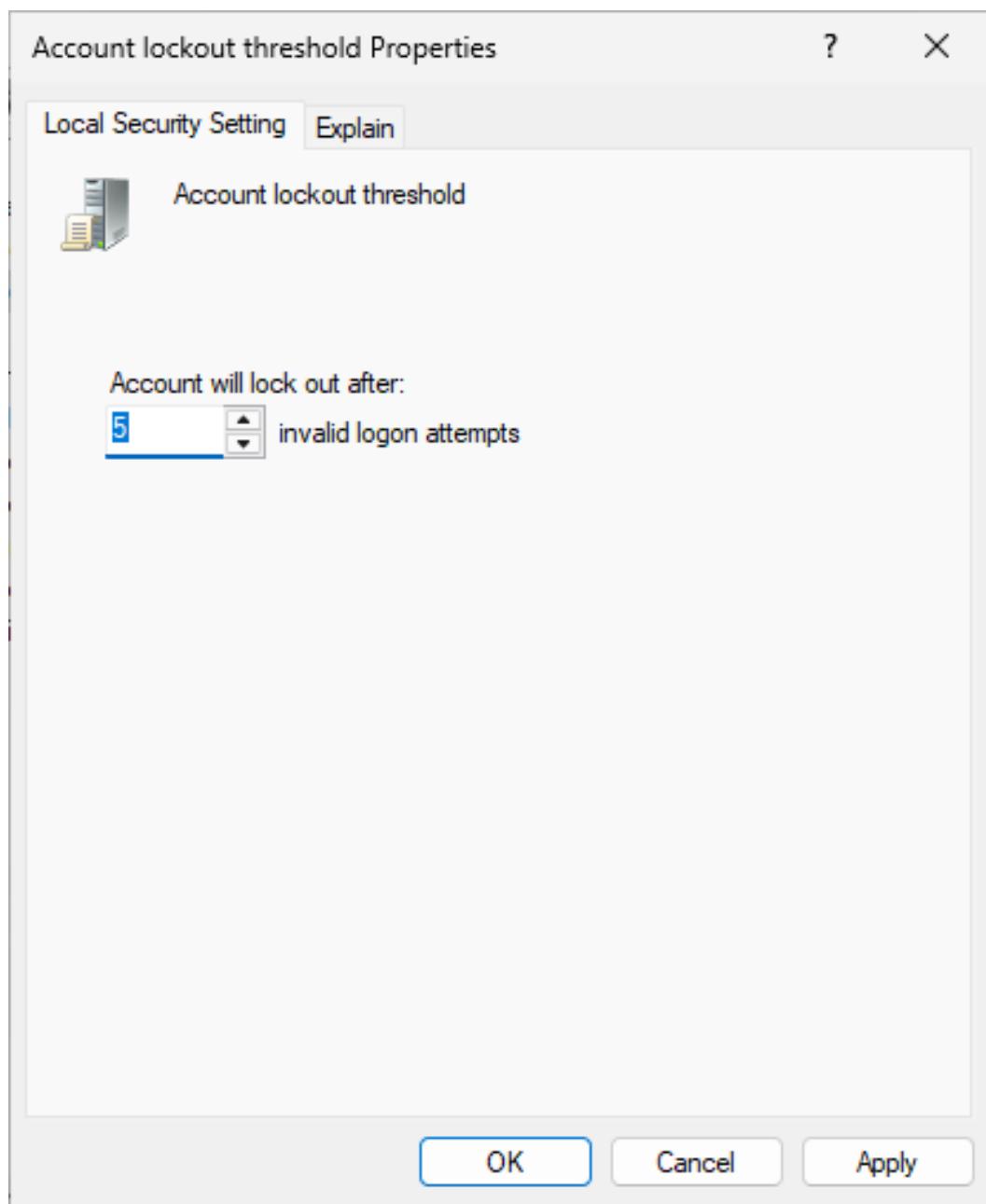


Figure 6: Account lockout threshold set to 5 invalid login attempts.

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.

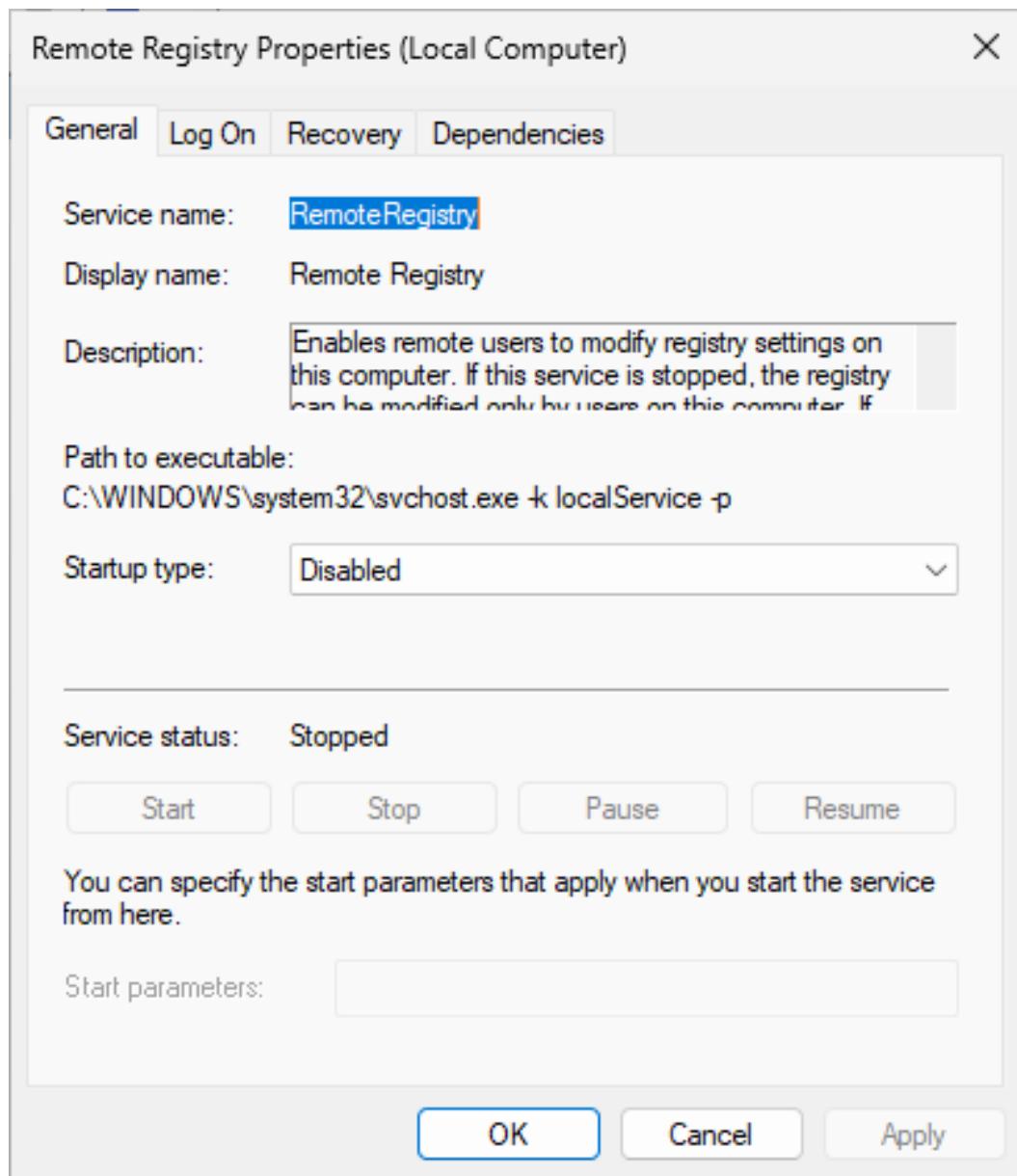


Figure 7: Remote Registry service disabled to prevent remote editing vulnerabilities.

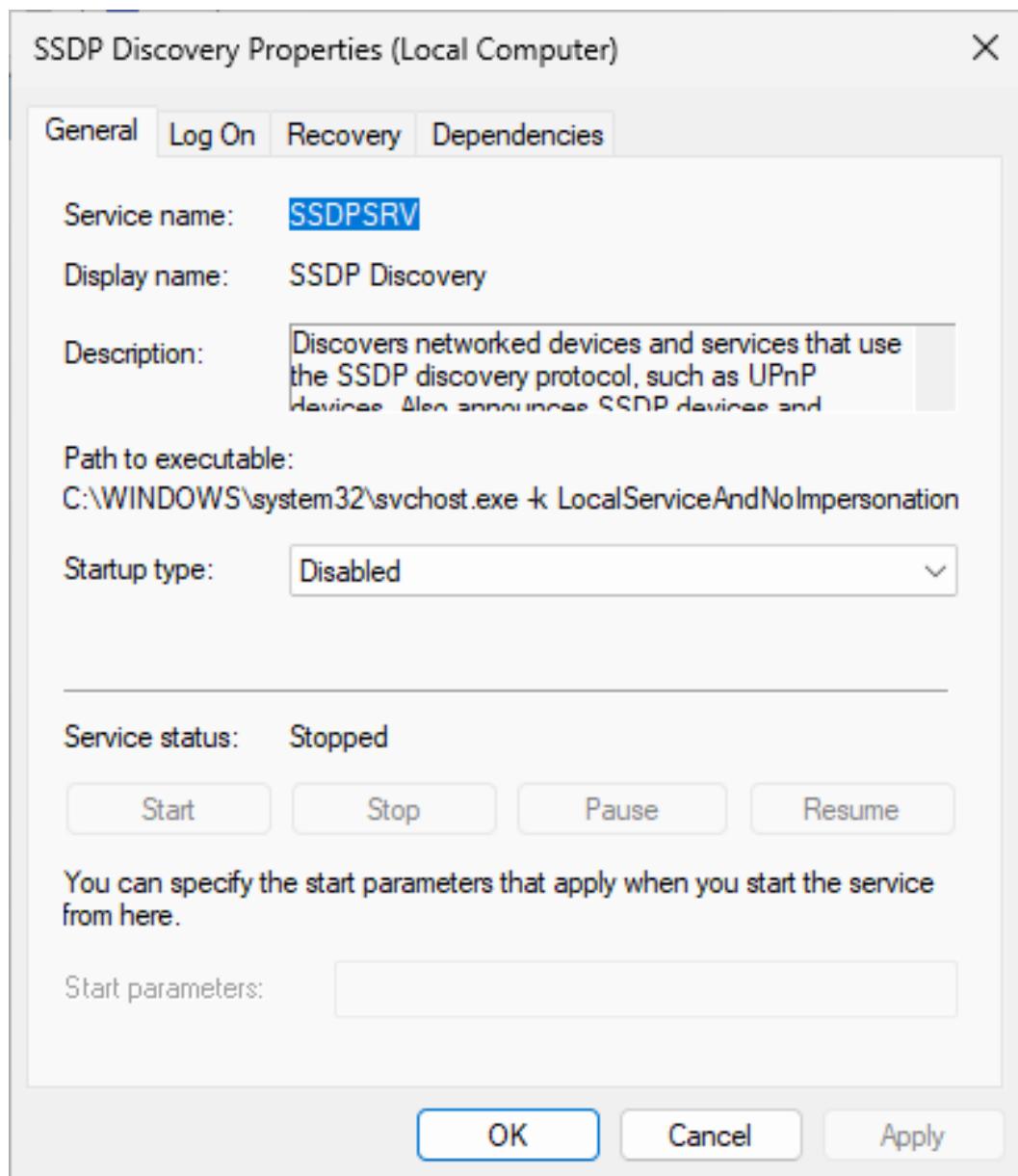


Figure 8: SSDP Discovery service disabled to reduce exposure to UPnP vulnerabilities.

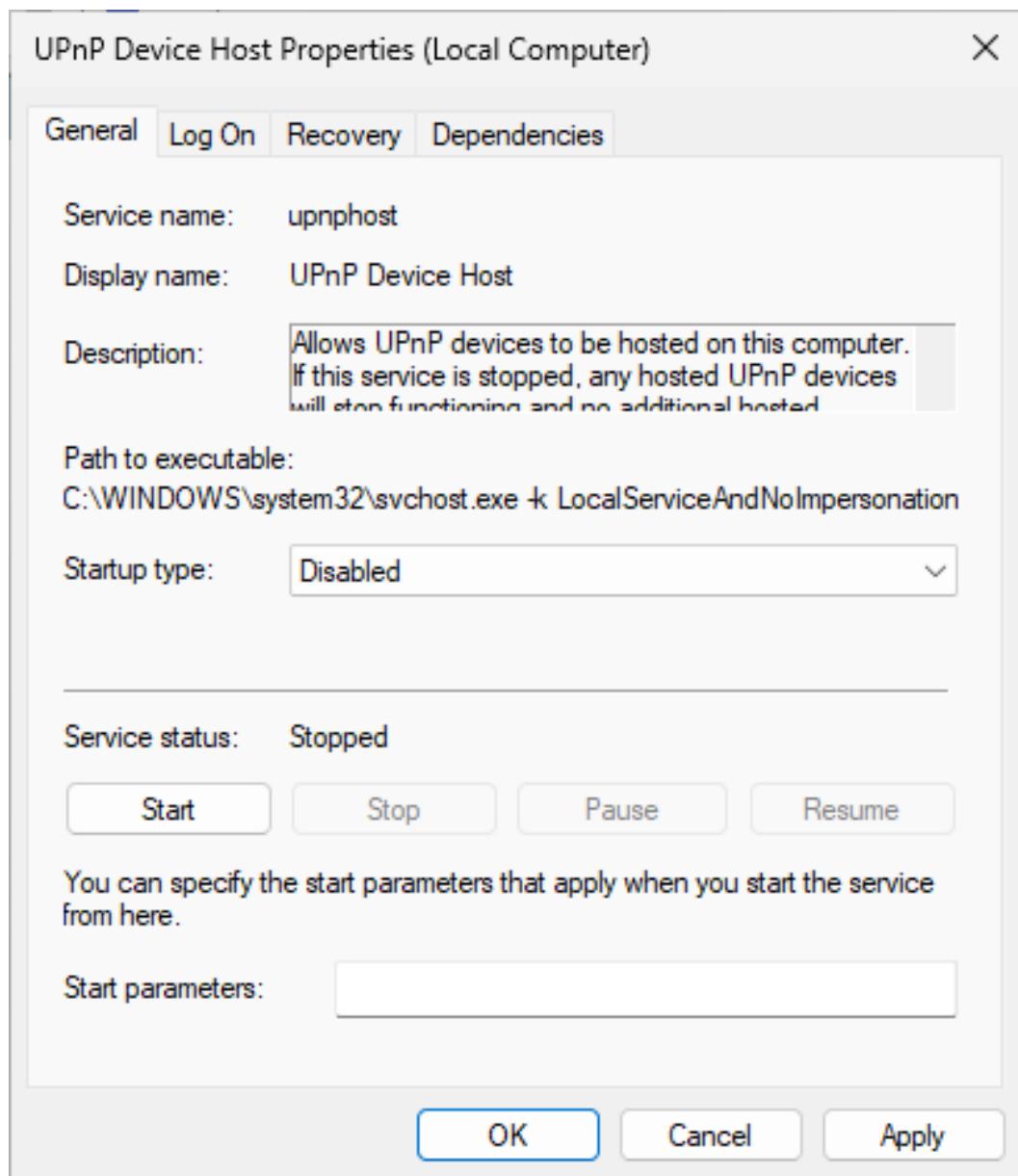


Figure 9: UPnP Device Host service disabled to mitigate auto-discovery risks.

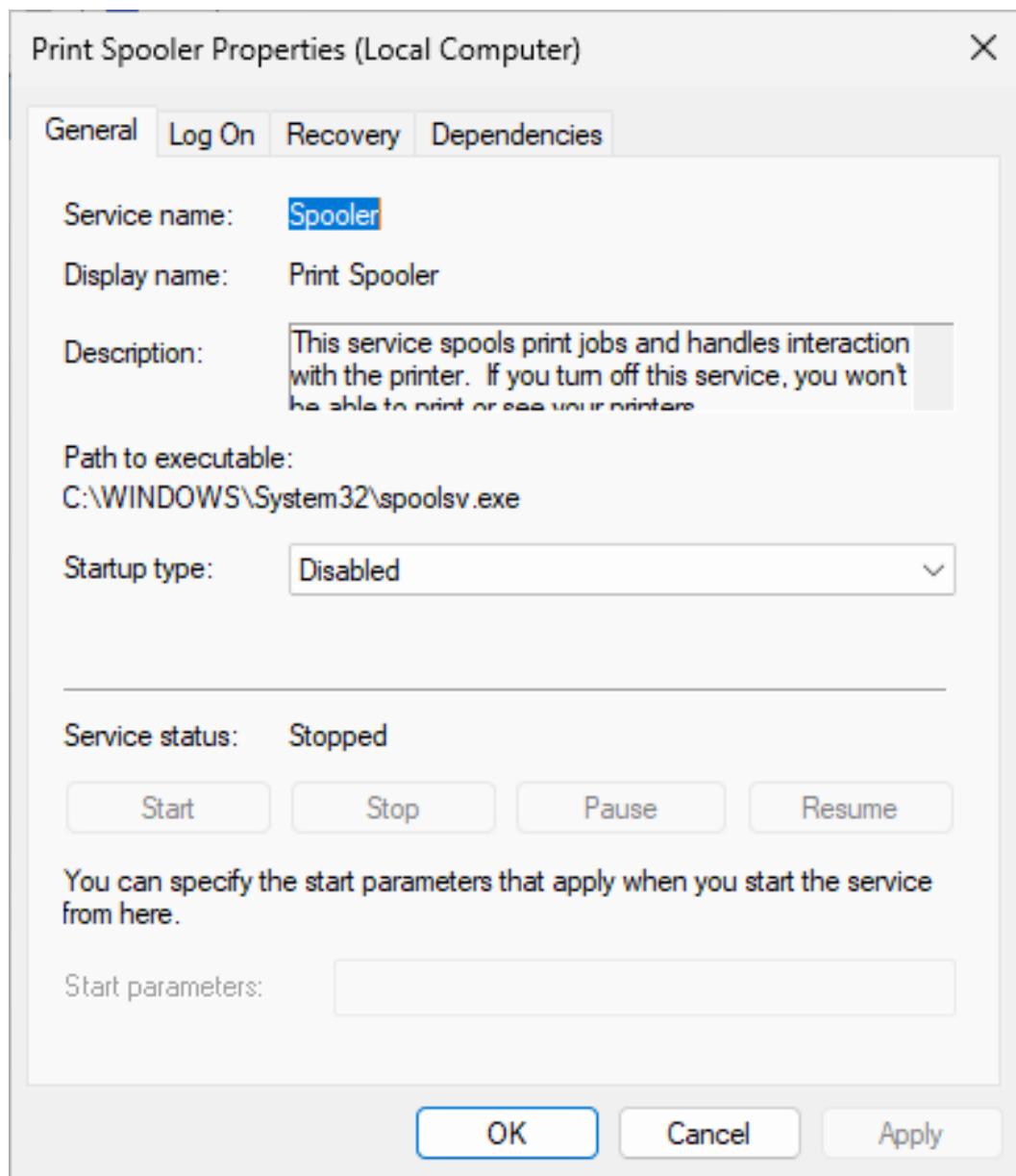


Figure 10: Print Spooler service disabled to reduce risk when printing is not needed.

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

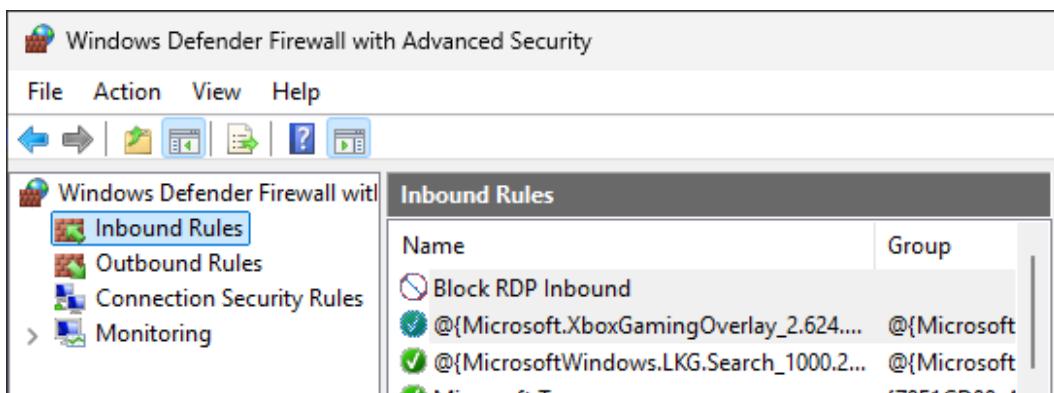


Figure 11: Firewall rule created to block RDP connections.

```
Administrator: Windows PowerShell
RemoteDynamicKeywordAddresses : {}
PolicyAppId                   :
PackageFamilyName             :

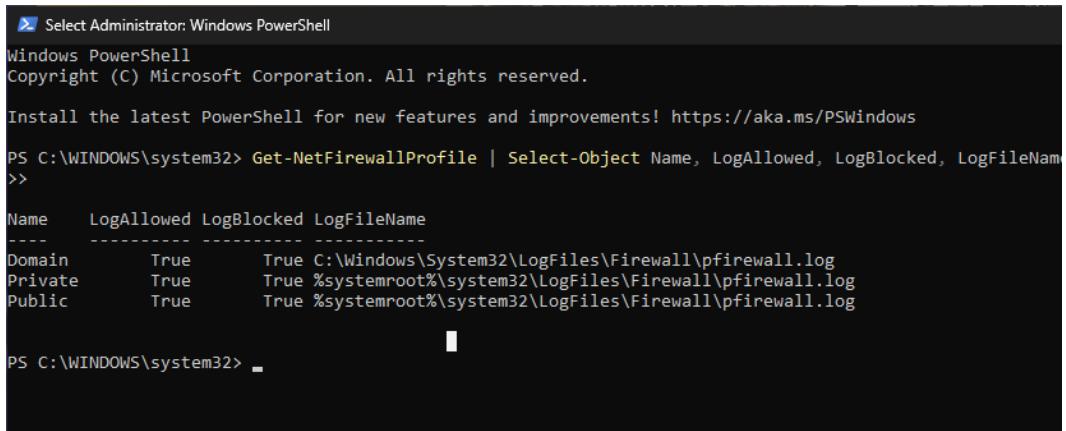
Name                          : {E35E8FA2-C1D7-4224-AF34-B72749B09E47}
DisplayName                   : Block Powershell Remoting
Description                   :
DisplayGroup                 :
Group                         :
Enabled                       : True
Profile                       : Any
Platform                      : {}
Direction                     : Inbound
Action                        : Block
EdgeTraversalPolicy           : Block
LooseSourceMapping            : False
LocalOnlyMapping              : False
Owner                         :
PrimaryStatus                : OK
Status                        : The rule was parsed successfully from the store. (65536)
EnforcementStatus            : NotApplicable
PolicyStoreSource             : PersistentStore
PolicyStoreSourceType          : Local
RemoteDynamicKeywordAddresses : {}
PolicyAppId                   :
PackageFamilyName             :

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

A screenshot of an Administrator: Windows PowerShell window. The command entered is ".\". The output shows a custom firewall rule named "Block Powershell Remoting" with the following properties:

- Name: {E35E8FA2-C1D7-4224-AF34-B72749B09E47}
- DisplayName: Block Powershell Remoting
- Description:
- DisplayGroup:
- Group:
- Enabled: True
- Profile: Any
- Platform: {}
- Direction: Inbound
- Action: Block
- EdgeTraversalPolicy: Block
- LooseSourceMapping: False
- LocalOnlyMapping: False
- Owner:
- PrimaryStatus: OK
- Status: The rule was parsed successfully from the store. (65536)
- EnforcementStatus: NotApplicable
- PolicyStoreSource: PersistentStore
- PolicyStoreSourceType: Local
- RemoteDynamicKeywordAddresses: {}
- PolicyAppId:
- PackageFamilyName:

Figure 12: PowerShell Remoting blocked via custom firewall rule.



```
PS 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
>>

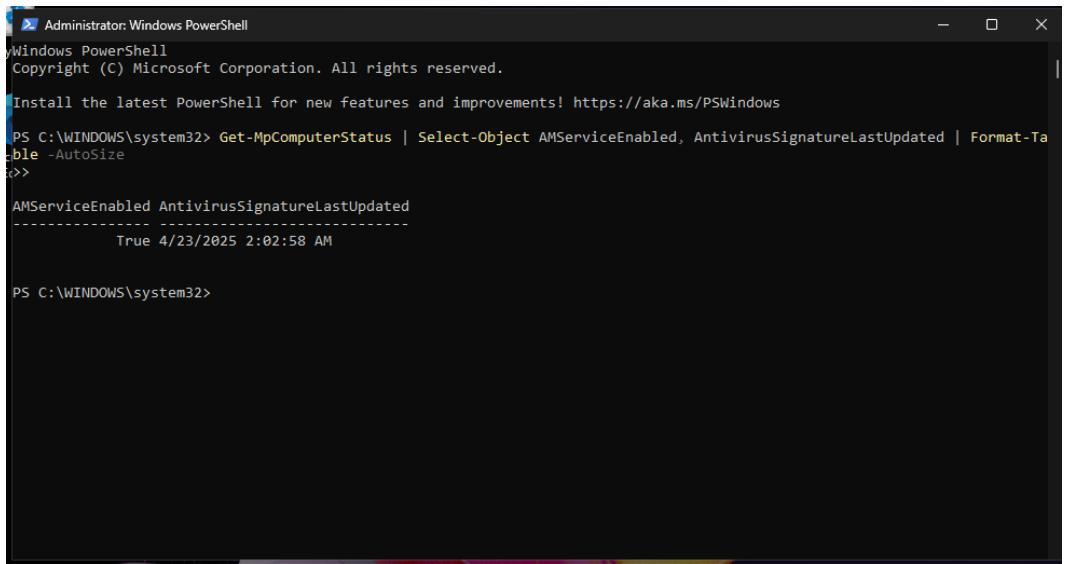
Name      LogAllowed LogBlocked LogFileName
----      -----     -----      -----
Domain    True       True       C:\Windows\System32\LogFiles\Firewall\pfirewall.log
Private   True       True       %systemroot%\system32\LogFiles\Firewall\pfirewall.log
Public    True       True       %systemroot%\system32\LogFiles\Firewall\pfirewall.log

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.

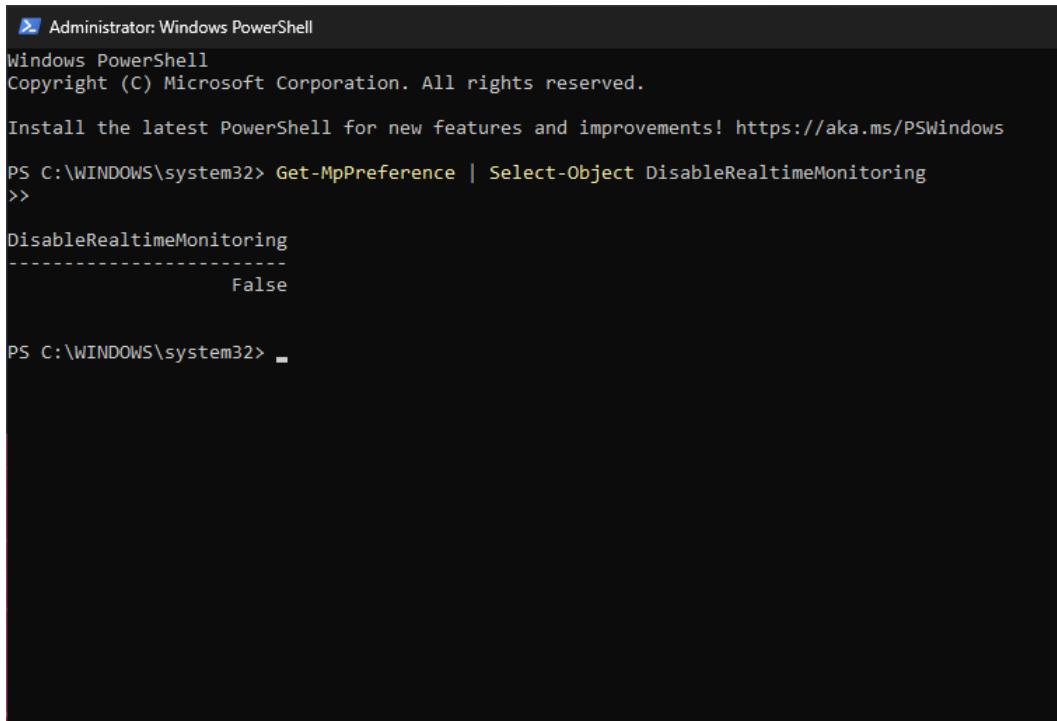
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

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
xception
+ 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

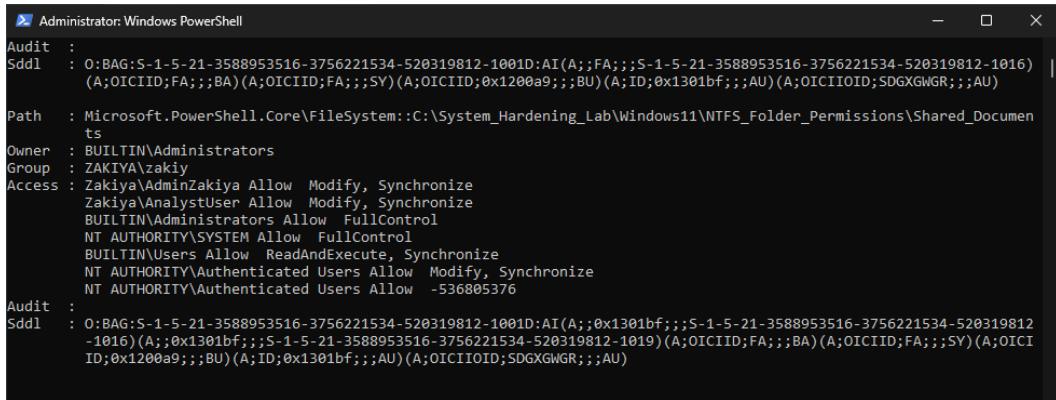
Mode                LastWriteTime        Length Name
----                -----        ---- 
d----    4/27/2025 11:22 AM            Admin_Tools
d----    4/27/2025 11:27 AM            Security_Logs
d----    4/27/2025 11:22 AM            Shared_Documents

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;OICII OID;SDGXGWGR;;;AU)
Path : Microsoft.PowerShell.Core\FileSystem::C:\System_Hardening_Lab\Windows11\NTFS_Folder_Permissions\Shared_Documen ts
Owner : BUILTIN\Administrators
Group : ZAKIYAZakiy
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;OICII OID;SDGXGWGR;;;AU)
```

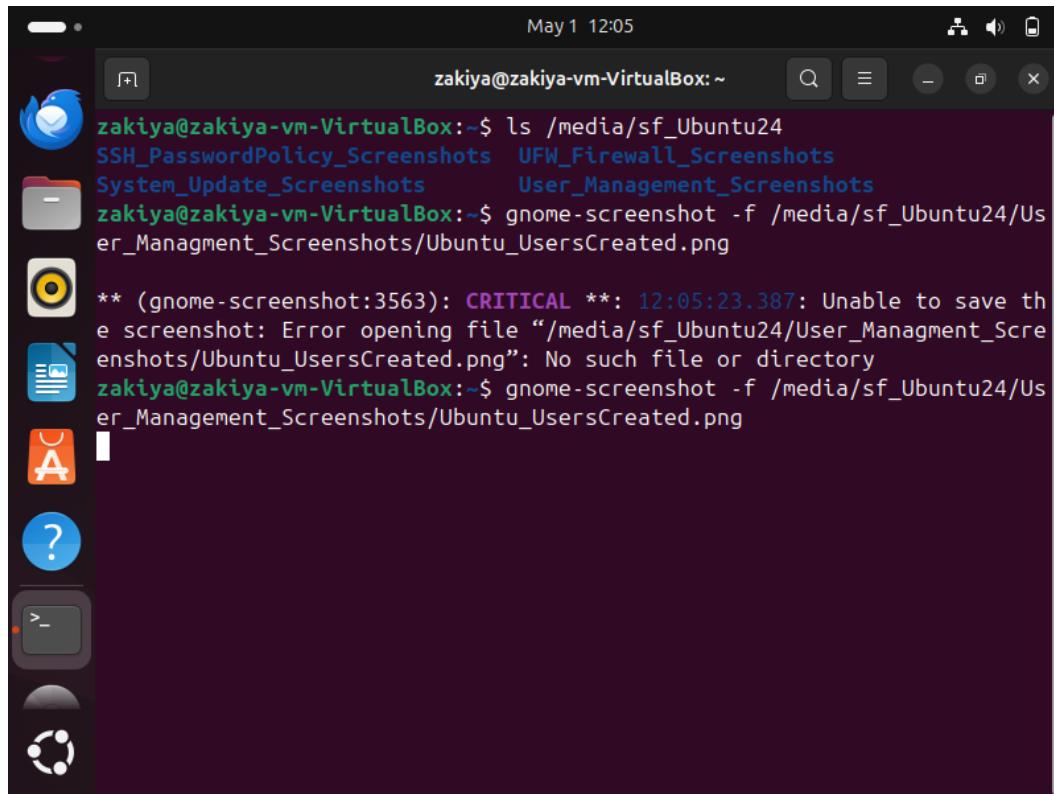
Figure 18: NTFS permissions for Shared_Documents.

4. Ubuntu 24.04 System Hardening

4.1 User and Group Management

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

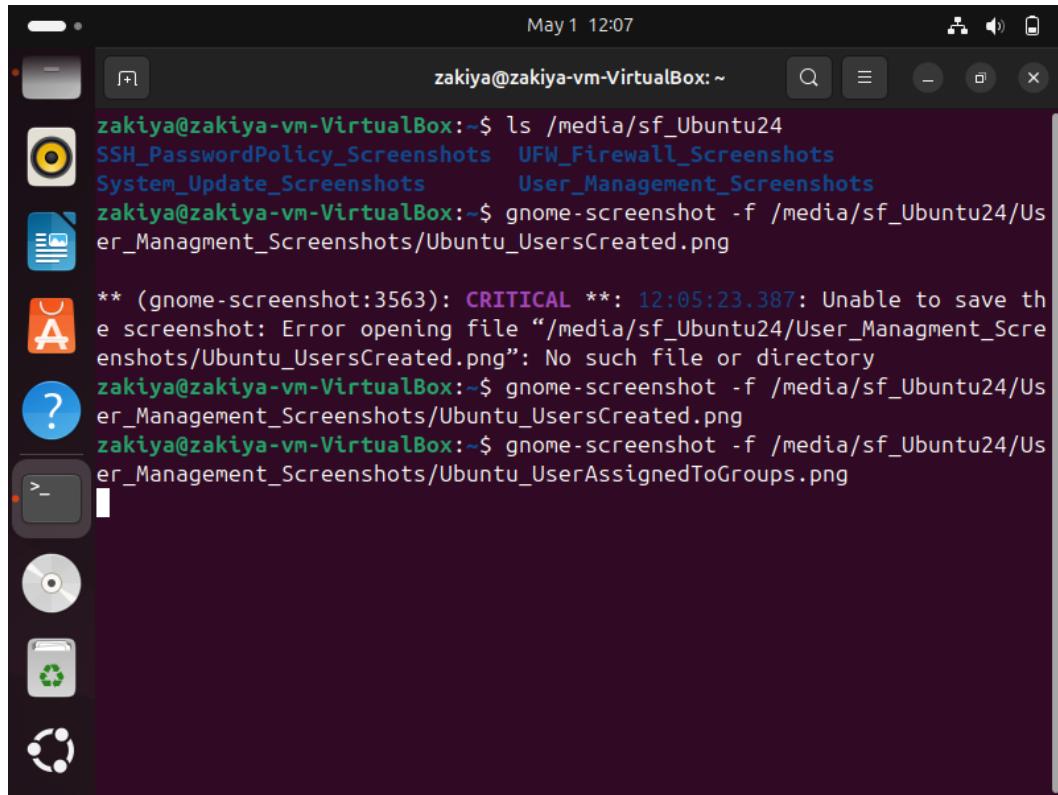
- adminzakiya (sudo/admin)
- analystuser (secops)
- guestuser (guests)



The screenshot shows a terminal window with a dark theme. The terminal title bar displays "zakiya@zakiya-vm-VirtualBox: ~". The terminal window contains the following text:

```
May 1 12:05
zakiya@zakiya-vm-VirtualBox:~$ ls /media/sf_Ubuntu24
SSH_PasswordPolicy_Screenshots  UFW_Firewall_Screenshots
System_Update_Screenshots      User_Management_Screenshots
zakiya@zakiya-vm-VirtualBox:~$ gnome-screenshot -f /media/sf_Ubuntu24/User_Managment_Screenshots/Ubuntu_UsersCreated.png
** (gnome-screenshot:3563): CRITICAL **: 12:05:23.387: Unable to save the screenshot: Error opening file “/media/sf_Ubuntu24/User_Managment_Screenshots/Ubuntu_UsersCreated.png”: No such file or directory
zakiya@zakiya-vm-VirtualBox:~$ gnome-screenshot -f /media/sf_Ubuntu24/User_Management_Screenshots/Ubuntu_UsersCreated.png
```

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

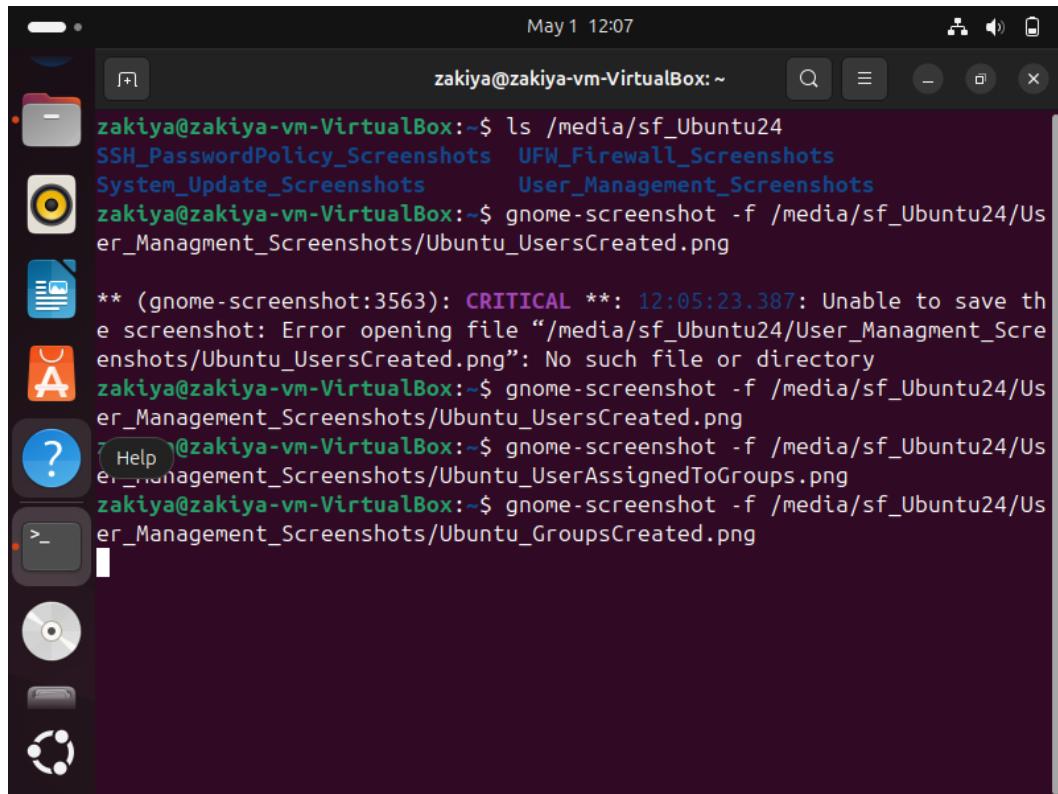


May 1 12:07

```
zakiya@zakiya-vm-VirtualBox:~$ ls /media/sf_Ubuntu24
SSH_PasswordPolicy_Screenshots  UFW_Firewall_Screenshots
System_Update_Screenshots      User_Management_Screenshots
zakiya@zakiya-vm-VirtualBox:~$ gnome-screenshot -f /media/sf_Ubuntu24/User_Managment_Screenshots/Ubuntu_UsersCreated.png

** (gnome-screenshot:3563): CRITICAL **: 12:05:23.387: Unable to save the screenshot: Error opening file "/media/sf_Ubuntu24/User_Managment_Screenshots/Ubuntu_UsersCreated.png": No such file or directory
zakiya@zakiya-vm-VirtualBox:~$ gnome-screenshot -f /media/sf_Ubuntu24/User_Management_Screenshots/Ubuntu_UsersCreated.png
zakiya@zakiya-vm-VirtualBox:~$ gnome-screenshot -f /media/sf_Ubuntu24/User_Management_Screenshots/Ubuntu_UserAssignedToGroups.png
```

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



May 1 12:07

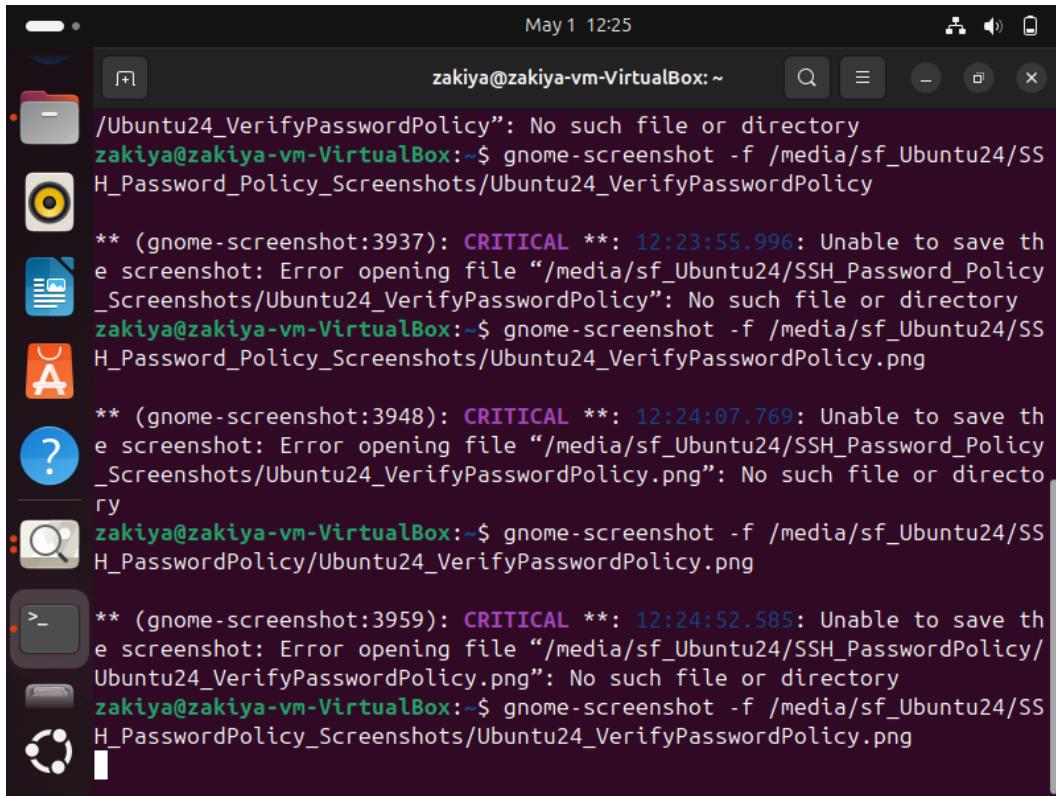
```
zakiya@zakiya-vm-VirtualBox:~$ ls /media/sf_Ubuntu24
SSH_PasswordPolicy_Screenshots  UFW_Firewall_Screenshots
System_Update_Screenshots      User_Management_Screenshots
zakiya@zakiya-vm-VirtualBox:~$ gnome-screenshot -f /media/sf_Ubuntu24/User_Managment_Screenshots/Ubuntu_UsersCreated.png

** (gnome-screenshot:3563): CRITICAL **: 12:05:23.387: Unable to save the screenshot: Error opening file "/media/sf_Ubuntu24/User_Managment_Screenshots/Ubuntu_UsersCreated.png": No such file or directory
zakiya@zakiya-vm-VirtualBox:~$ gnome-screenshot -f /media/sf_Ubuntu24/User_Management_Screenshots/Ubuntu_UsersCreated.png
zakiya@zakiya-vm-VirtualBox:~$ gnome-screenshot -f /media/sf_Ubuntu24/User_Management_Screenshots/Ubuntu_UserAssignedToGroups.png
zakiya@zakiya-vm-VirtualBox:~$ gnome-screenshot -f /media/sf_Ubuntu24/User_Management_Screenshots/Ubuntu_GroupsCreated.png
```

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



The screenshot shows a terminal window titled "zakiya@zakiya-vm-VirtualBox:~". The terminal output is as follows:

```
/Ubuntu24_VerifyPasswordPolicy": No such file or directory
zakiya@zakiya-vm-VirtualBox:~$ gnome-screenshot -f /media/sf_Ubuntu24/SSH_Password_Policy_Screenshots/Ubuntu24_VerifyPasswordPolicy

** (gnome-screenshot:3937): CRITICAL **: 12:23:55.996: Unable to save the screenshot: Error opening file "/media/sf_Ubuntu24/SSH_Password_Policy_Screenshots/Ubuntu24_VerifyPasswordPolicy": No such file or directory
zakiya@zakiya-vm-VirtualBox:~$ gnome-screenshot -f /media/sf_Ubuntu24/SSH_Password_Policy_Screenshots/Ubuntu24_VerifyPasswordPolicy.png

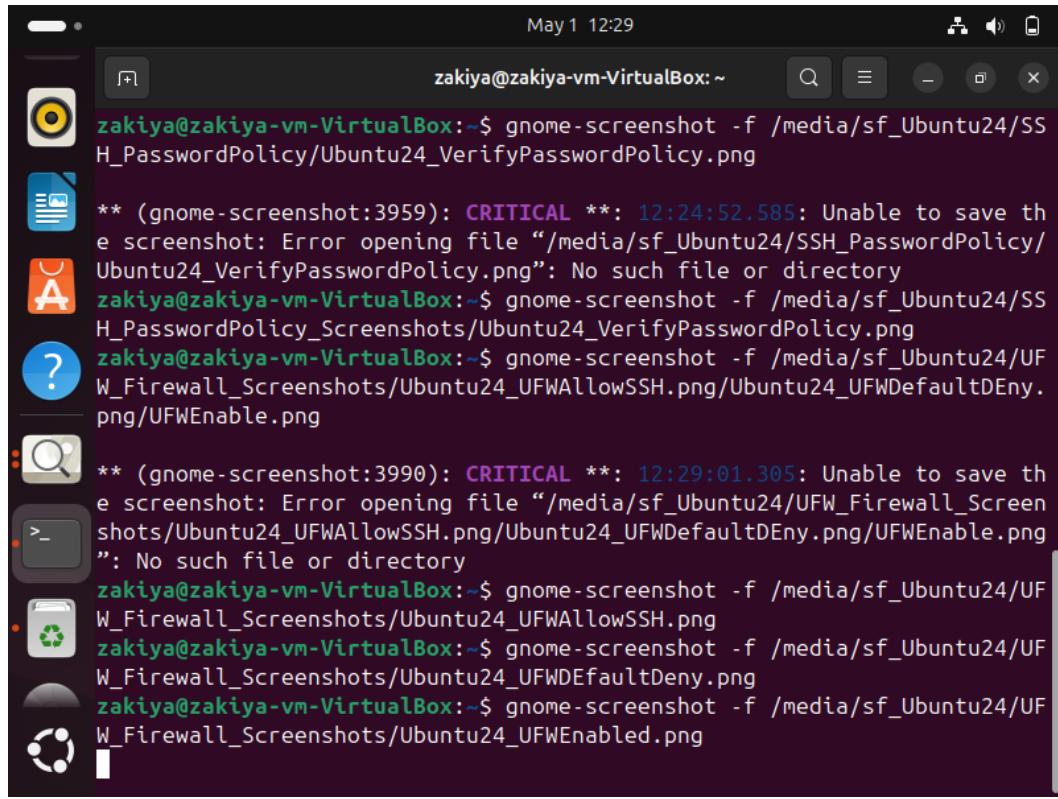
** (gnome-screenshot:3948): CRITICAL **: 12:24:07.769: Unable to save the screenshot: Error opening file "/media/sf_Ubuntu24/SSH_Password_Policy_Screenshots/Ubuntu24_VerifyPasswordPolicy.png": No such file or directory
zakiya@zakiya-vm-VirtualBox:~$ gnome-screenshot -f /media/sf_Ubuntu24/SSH_PasswordPolicy/Ubuntu24_VerifyPasswordPolicy.png

** (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
```

Figure 22: Password complexity enforced via pam_pwquality.

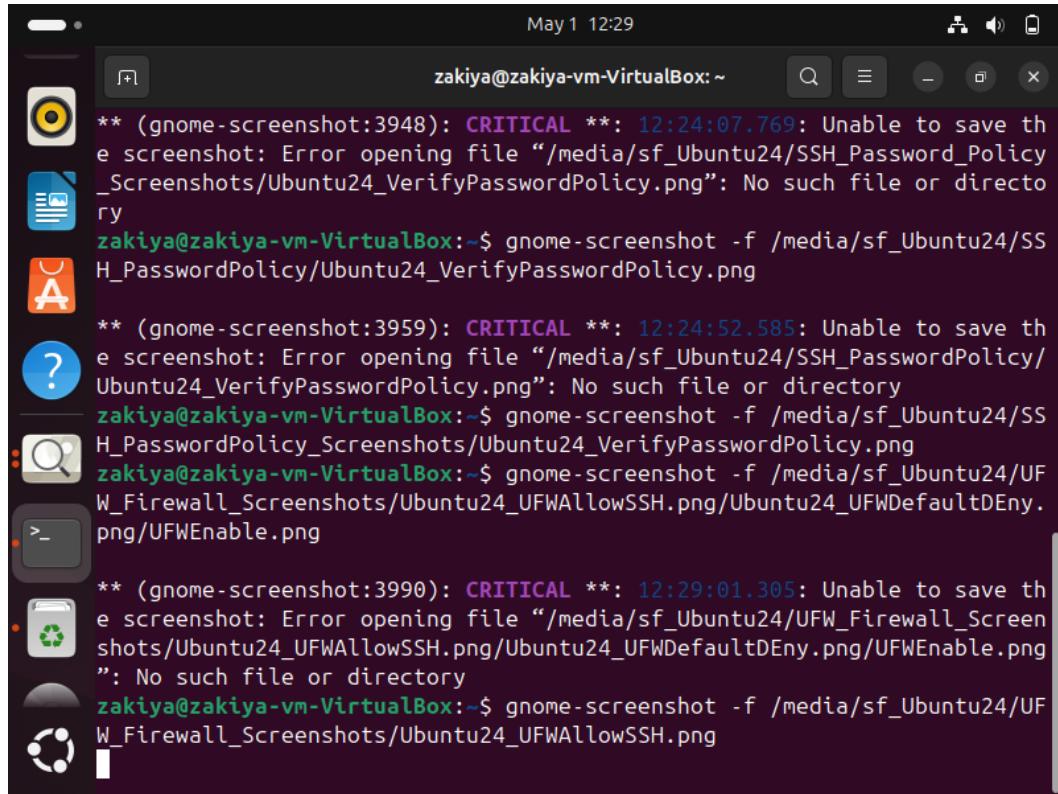
4.3 Firewall (UFW) Configuration

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



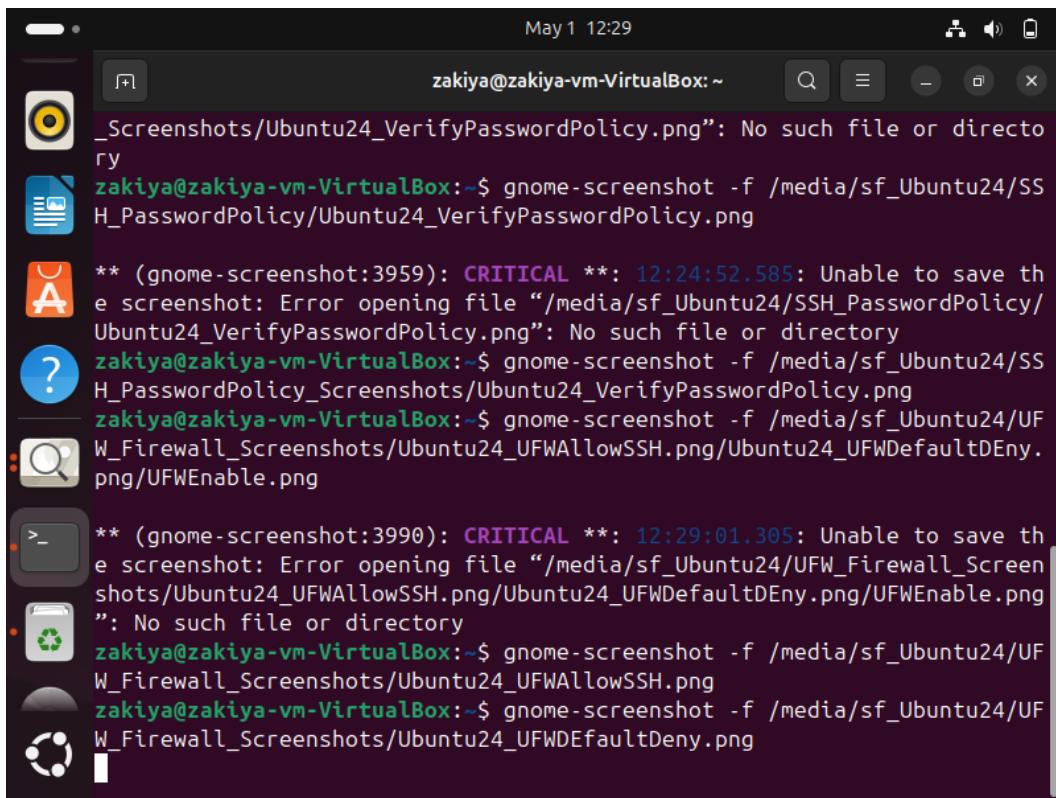
```
zakiya@zakiya-vm-VirtualBox:~$ gnome-screenshot -f /media/sf_Ubuntu24/SSH_PasswordPolicy/Ubuntu24_VerifyPasswordPolicy.png
** (gnome-screenshot:3959): CRITICAL **: 12:24:52.585: Unable to save the screenshot: Error opening file "/media/sf_Ubuntu24/SSH_PasswordPolicy/Ubuntu24_VerifyPasswordPolicy.png": 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.



```
zakiya@zakiya-vm-VirtualBox:~$ gnome-screenshot -f /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.



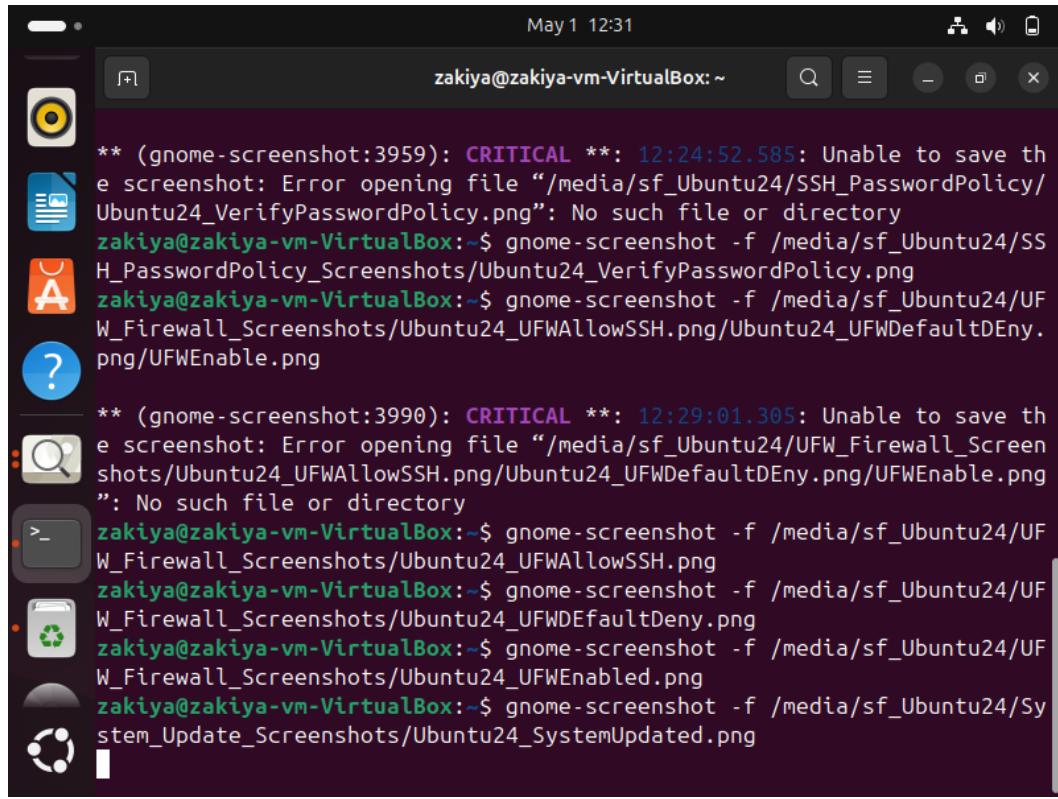
The screenshot shows a terminal window titled 'zakiya@zakiya-vm-VirtualBox: ~'. The terminal output is as follows:

```
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.



The screenshot shows a terminal window titled "zakiya@zakiya-vm-VirtualBox: ~". The window contains a series of log entries from the "gnome-screenshot" command, indicating errors while saving screenshots. The log entries are:

```
** (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_UFWDefaultDeny.png
zakiya@zakiya-vm-VirtualBox:~$ gnome-screenshot -f /media/sf_Ubuntu24/UFW_Firewall_Screenshots/Ubuntu24_UFWEabled.png
zakiya@zakiya-vm-VirtualBox:~$ gnome-screenshot -f /media/sf_Ubuntu24/System_Update_Screenshots/Ubuntu24_SystemUpdated.png
```

Figure 26: Screenshot showing Ubuntu system updates applied.