Lab 3 – Server Hardening & Baseline Security

Course: NET-2220 – Server Management
Student: Clayton Holden
Date Completed:

---

1. Purpose

The goal of this lab was to harden a Windows Server 2022 system using standard security controls aligned with CIS and NIST guidelines. The lab focused on applying password and account lockout baselines, configuring secure firewall rules, disabling unnecessary services, verifying Defender and update settings, and validating changes through PowerShell.

---

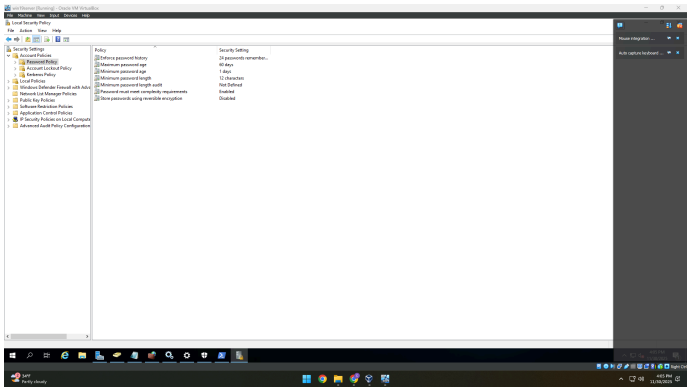
2. Hardening Tasks Performed

A. Account Policies (CIS Baseline)

Using *Local Security Policy* (`secpol.msc`):

- Minimum password length set to **12**
- Maximum password age set to **60 days**
- Enforce password history set to **24**
- Account lockout threshold set to **5 attempts**
- Lockout window and duration set to **15 minutes**

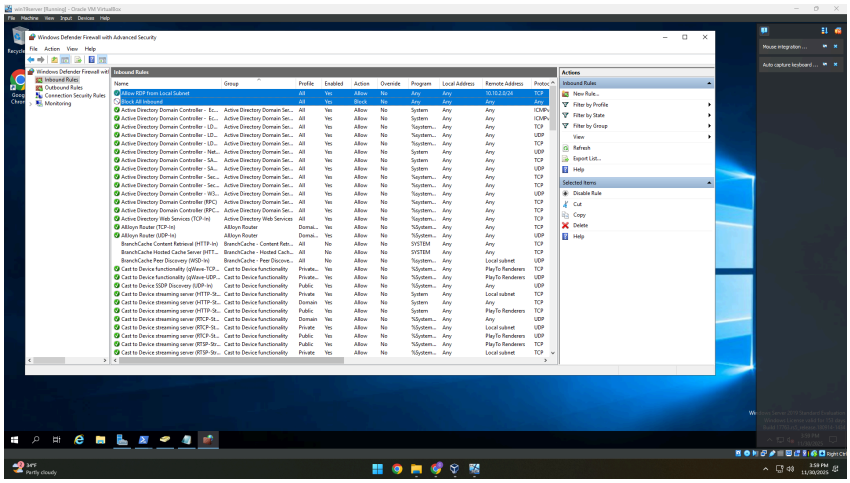
Evidence:



B. Windows Firewall Configuration

- Enabled firewall on all profiles (Domain, Private, Public)
- Created inbound rule allowing **RDP (TCP 3389)** only from the internal subnet
- Created rule to block all remaining inbound traffic

Evidence:



C. Disable Unused/Unsafe Services

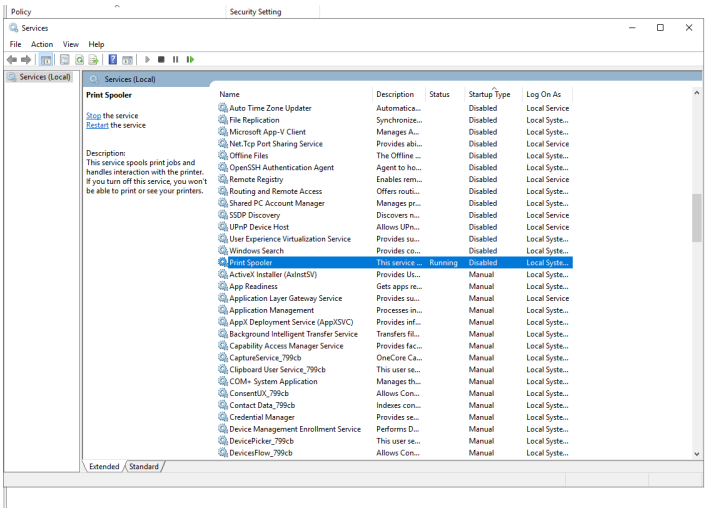
Disabled unnecessary services using PowerShell:

```
Set-Service RemoteRegistry -StartupType Disabled
```

```
Set-Service TlntSvr -StartupType Disabled
Set-Service Spooler -StartupType Disabled
```

Restarted server to apply service changes.

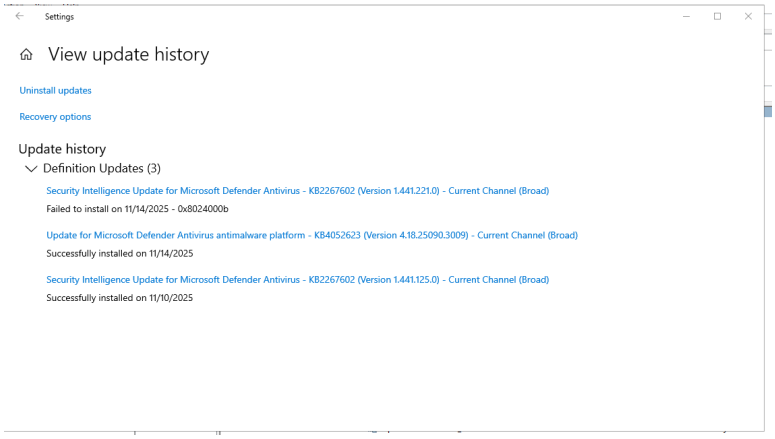
Evidence:

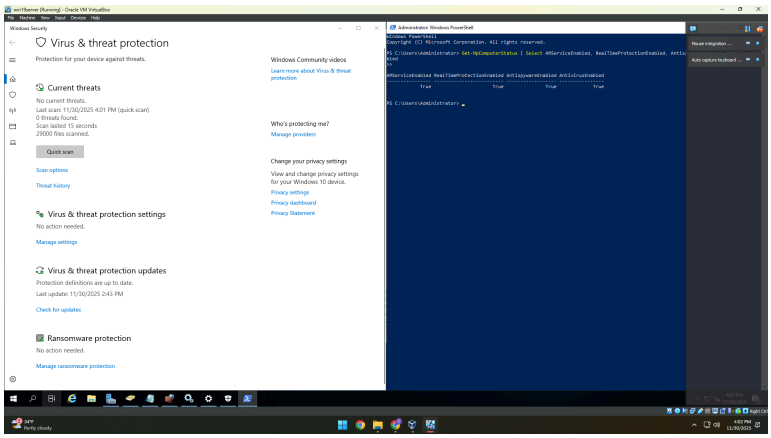


D. Windows Defender & Update Configuration

- Verified Defender real-time protection is **ON**
- Confirmed AV and AS engines enabled in PowerShell (`Get-MpComputerStatus`)
- Configured Windows Update to **Automatically Download and Install**
- Installed all pending security updates

Evidence:





---

3. Validation Commands Executed

(Outputs stored in screenshots or text attachments)

```
Get-Service | Where-Object {$_.StartType -eq 'Disabled'}
Get-WindowsFeature | Where-Object {$_.InstallState -eq 'Installed'}
(Get-ItemProperty
"HKLM:\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile").Ena
bleFirewall
```

These confirmed:

- Required services are disabled
- AD DS and other required roles installed

- Firewall is fully enabled

---

4. Results Summary

All baseline requirements from the lab were successfully implemented:

- Password, lockout, and local security policies meet CIS Level 1
- All firewall profiles enabled and RDP restricted to local subnet
- Remote Registry, Telnet, and Print Spooler disabled
- Defender active with real-time protection
- Server fully patched and up to date

---

5. Reflection

Completing this lab showed how essential baseline hardening is to securing any Windows Server deployment. Applying CIS password and lockout policies reduces the risk of weak credentials and brute-force attacks. Restricting RDP and enabling all firewall profiles drastically limits the attack surface. Disabling unnecessary services and keeping Defender and Windows Update active ensures the server is protected against common vulnerabilities. This baseline sets the foundation for secure domain operations and supports future GPO-based hardening.