# Milestone 2 – Security Hardening & Patch Management Report

---

# Change Record ID: CR-NET2220-M2-2025

**Change Type:** Security Hardening & Patch Compliance
**Server Name:** SERVER3
**Date Implemented:** November 24 – December 1, 2025

---

# 1. System Summary

| Field | Value |
|---|---|
| Hostname | SERVER3 |
| IP Address | (Insert from `ipconfig /all`) |
| Operating System | Windows Server 2022 Standard (Desktop Experience) |
| OS Build | (From `systeminfo`) |
| Domain Membership | corp.local |
| Roles Installed | AD DS, DNS (from DC promotion), File Services (if present) |

---

# 2. Security Policies Applied

Security settings were applied using Local Security Policy and PowerShell, following CIS Windows Server 2022 Level 1 recommendations.

**Password Policy**

- Minimum Password Length: 12
- Maximum Password Age: 60 days
- Password History: 24 passwords
- Complexity: Enabled

**Account Lockout Policy**

- Lockout Threshold: 5 attempts
- Reset Counter: 15 minutes
- Lockout Duration: 15 minutes

**Screenshot(s) to Insert:**

- Password Policy window
- Account Lockout Policy window

---

# 3. Firewall Configuration

Firewall was enabled on **Domain**, **Private**, and **Public** profiles, and secure inbound rules were applied.

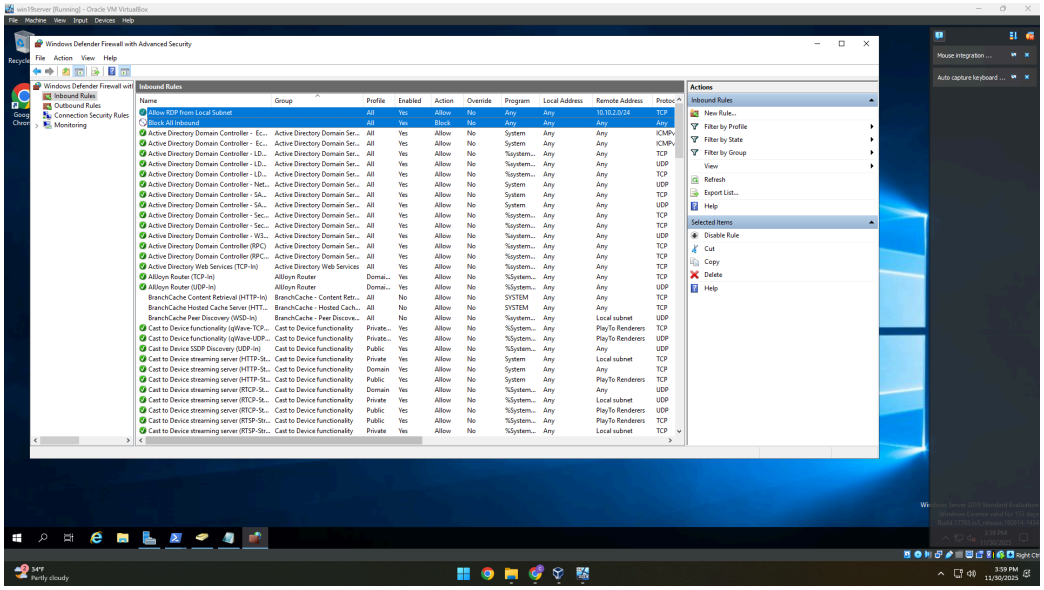
| Rule Name | Action | Port/Protocol | Scope |
|---|---|---|---|
| Allow RDP from Local Subnet | Allow | TCP 3389 | Local Subnet Only |
| Block All Other Inbound | Block | All | All |
| Default Windows Rules | Allow/Block | Various | As configured |

Commands used:

```
Set-NetFirewallProfile -Profile Domain,Private,Public -Enabled True
```

```
New-NetFirewallRule -DisplayName "Allow RDP from Local Subnet"
-Direction Inbound -Protocol TCP -LocalPort 3389 -RemoteAddress <your
subnet> -Action Allow
New-NetFirewallRule -DisplayName "Block All Inbound" -Direction
Inbound -Action Block
```

**Screenshot to Insert:**



---

# 4. Services Audit

Services were reviewed and hardened according to CIS baseline.

**Disabled Services:**

| Service | Reason |
|---|---|
| RemoteRegistry | Prevent remote registry tampering |
| Telnet | Obsolete, insecure protocol |
| Print Spooler | Disabled for security unless printing is required |

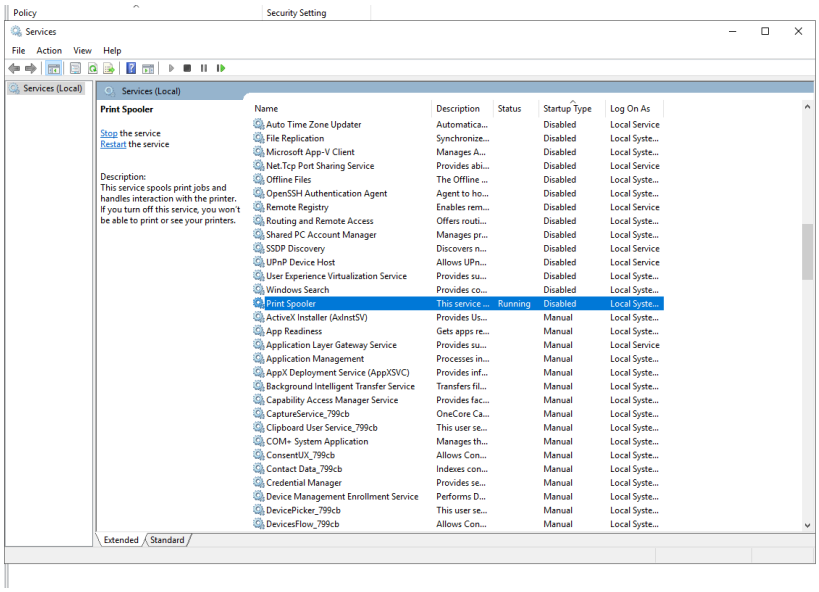
Command used:

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

Verification:

```
Get-Service | Where-Object {$_.StartType -eq 'Disabled'}
```

**Screenshot to Insert:**




---

# 5. Patch Verification

Patch level was validated using PowerShell:

```
Get-HotFix | Sort-Object InstalledOn -Descending | Select-Object
-First 10
systeminfo | Select-String "KB"
```

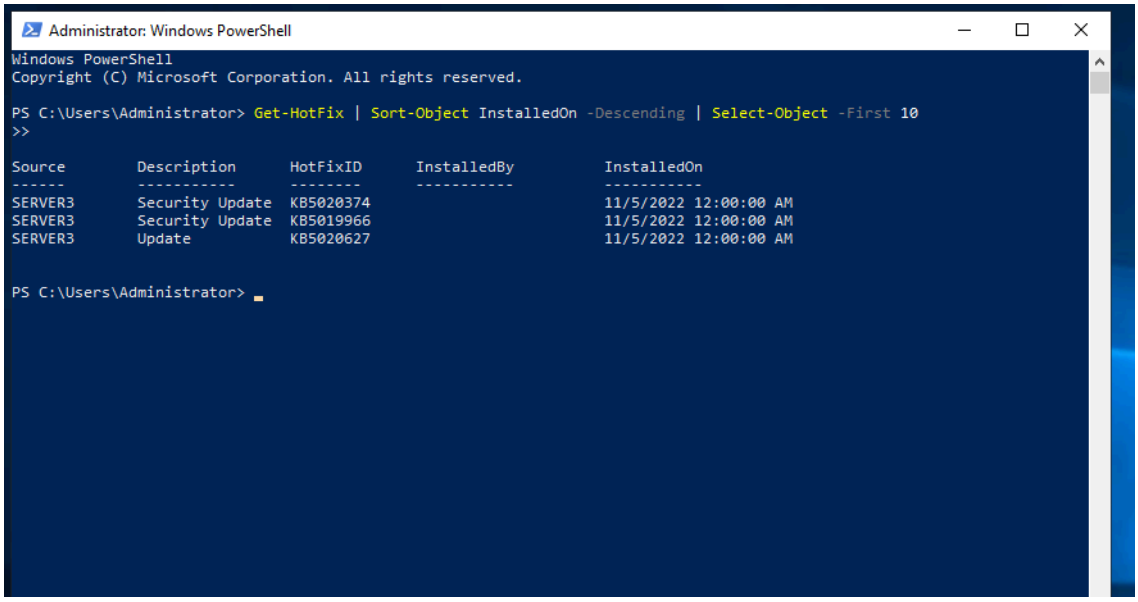
Recent KBs installed (example):

- KB5020374

- KB5019966
- KB5020627

This confirms the system is fully patched with November 2025 cumulative updates.

**Screenshot to Insert:**

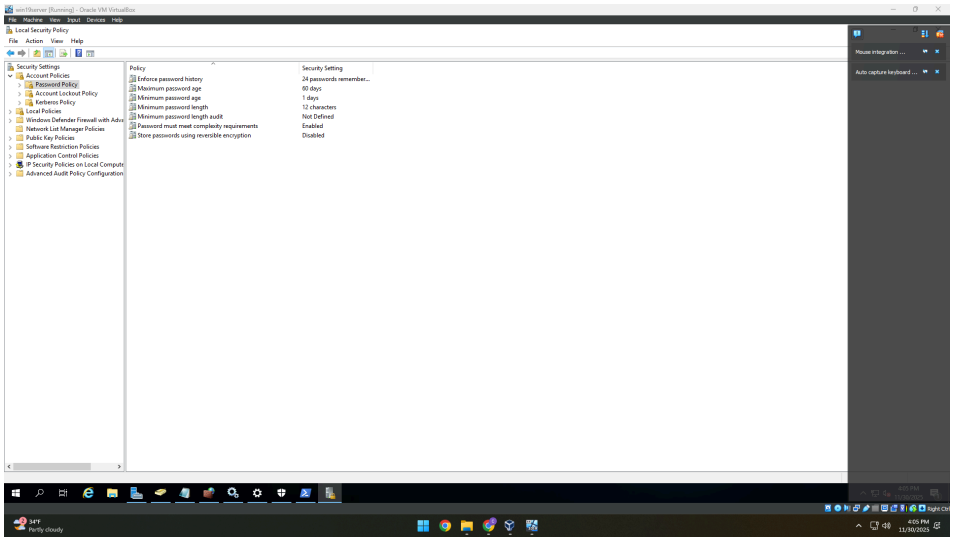



---

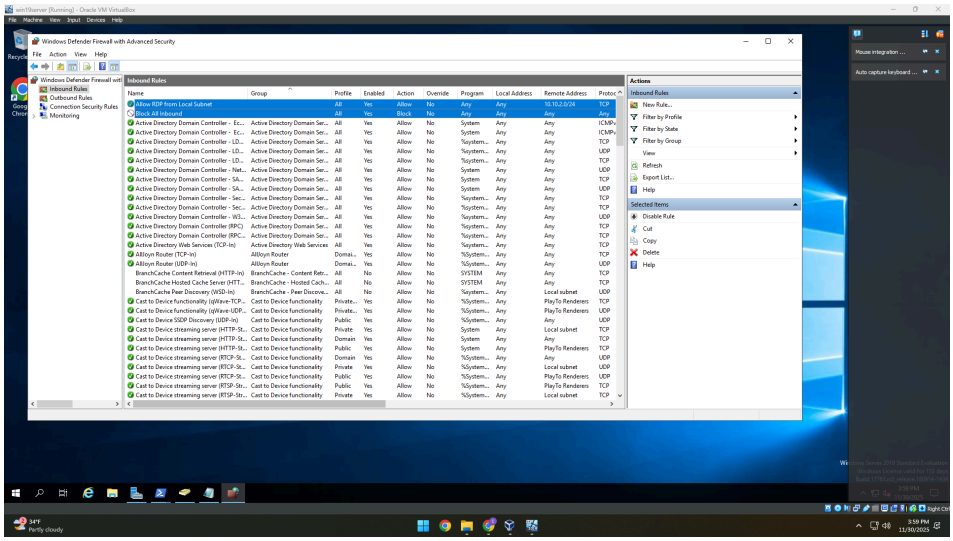
# 6. Evidence Screenshots

Insert all screenshots from Labs 3 and 4, clearly labeled.
Required screenshots:

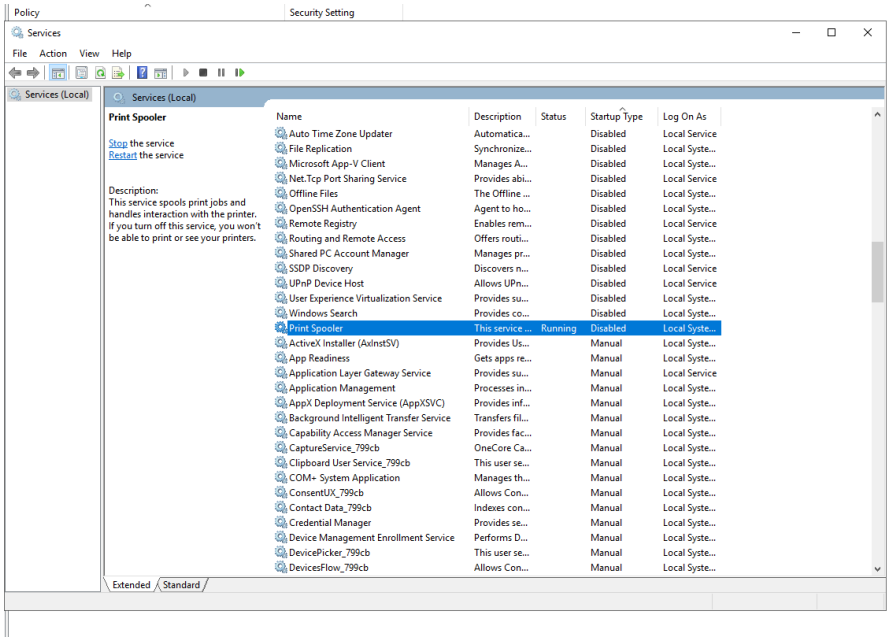
1. Password Policy settings



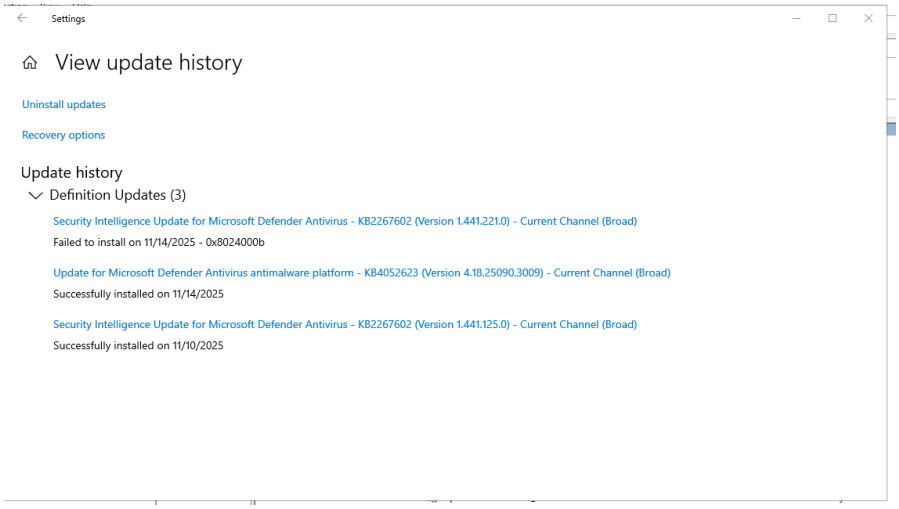
2. Firewall rules



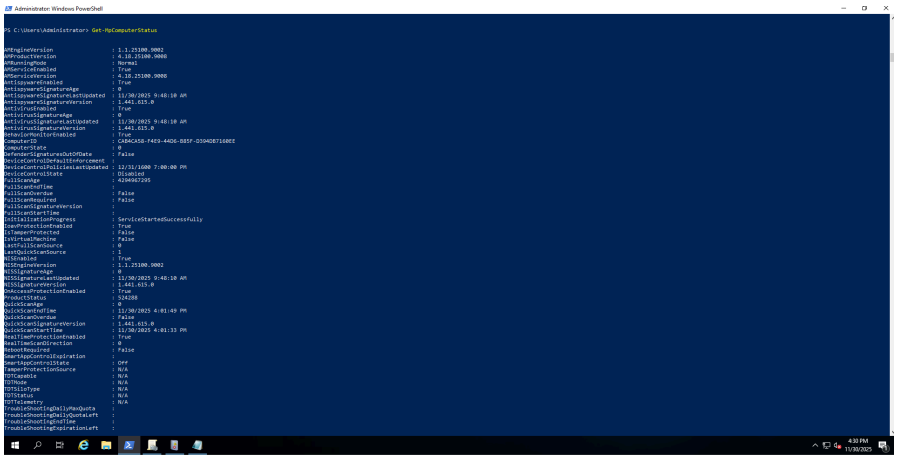
3. Disabled services list



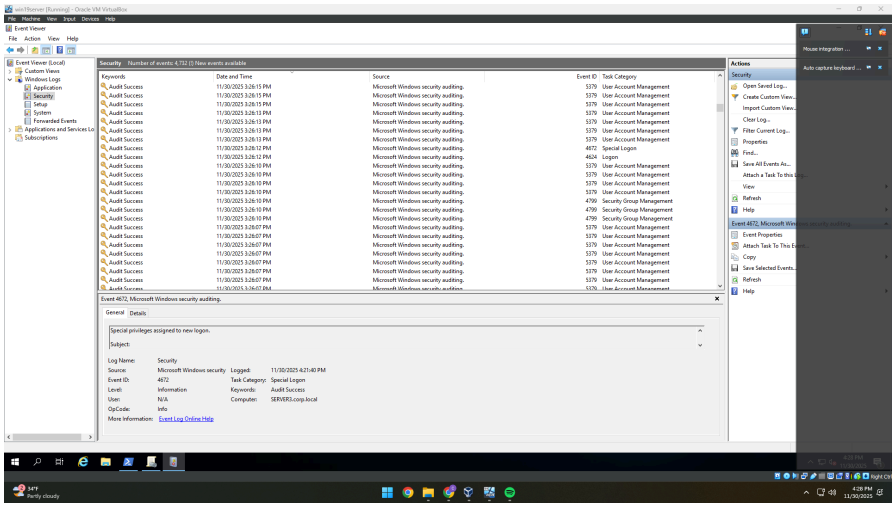

4. Windows Update history



5. PowerShell HotFix output



6. Event Viewer Security log entries



---

# 7. Audit Policy Configuration

Audit policies followed NIST/CIS recommendations:

Enabled via PowerShell:

```
auditpol /set /subcategory:"Logon" /success:enable /failure:enable
auditpol /set /subcategory:"User Account Management" /success:enable
/failure:enable
auditpol /set /subcategory:"Security Group Management" /success:enable
```

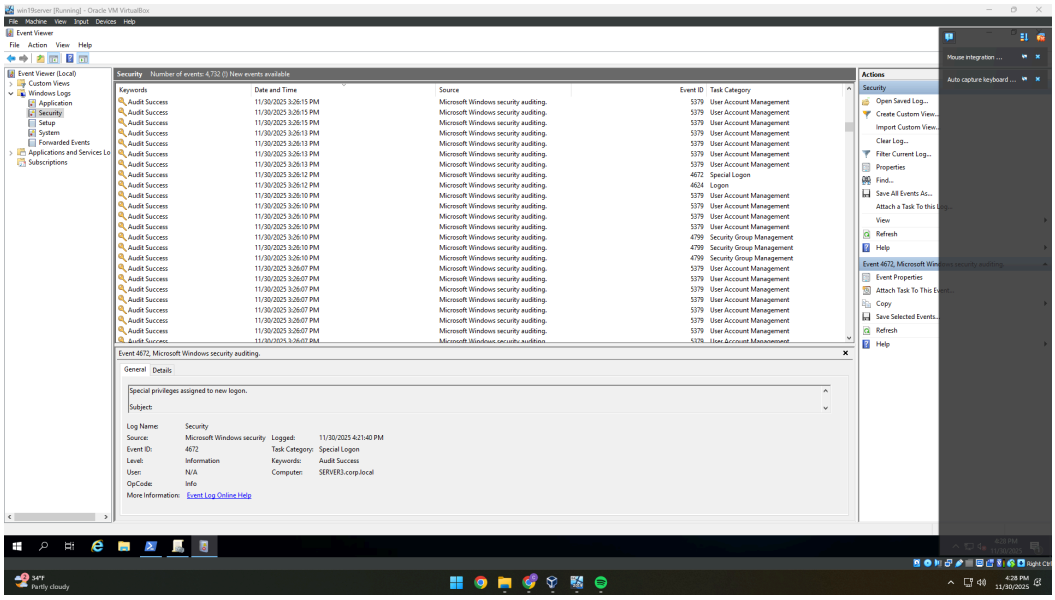
```
auditpol /set /subcategory:"Audit Policy Change" /success:enable /failure:enable
```

Verified using:

```
auditpol /get /category:*
```

Event Viewer confirmed audit events such as:

- 4624 (Logon)
- 4720 (User created)
- 4732 (User added to group)
- 4719 (Policy change)



---

# 8. Validation Results

| Test | Result | Status |
|---|---|---|

| | | |
|---|---|---|
| CIS baseline controls applied | Verified by policy settings | Pass |
| Password & lockout policy | Correct per screenshot | Pass |
| Firewall profiles enabled | Validated | Pass |
| Unnecessary services disabled | Verified in PowerShell | Pass |
| Patches installed | HotFix list validated | Pass |
| Audit logs functioning | Security log events visible | Pass |

---

# 9. Rollback Plan

A VM snapshot was taken prior to hardening:
**Snapshot Name:** Pre-Hardening-11-24-25

Rollback steps:

1. Revert snapshot in VM manager
2. Boot the server
3. Confirm networking and domain membership
4. Validate AD DS services

---

# 10. Approvals

| Role | Name | Date | Status |
|---|---|---|---|
| System Admin | Clayton Holden | 12/1/25 | Approved |
| Change Manager | Norma DePriest | 12/2/25 | Approved |
| Security Officer | (Optional) | — | Pending |

---

# Outcome

Security hardening and patch validation were successfully completed on **SERVER3**. The system now meets CIS Windows Server 2022 Level 1 requirements for password complexity, lockout policies, firewall configuration, service hardening, patch management, and audit log visibility. No rollback required.