cyber.encse

CIS MICROSOFT WINDOWS SERVER 2022 BENCHMARK — ALIGNED

Windows Server 2022 Hardening Guide

CIS Benchmark–aligned hardening guide with rationale, registry paths, and PowerShell verification commands.

This guide provides hardening rationale, registry paths, and verification commands for a security baseline. Always test in a non-production environment first — some settings can break application compatibility or legacy integrations. Not every control applies to every environment; assess against your own risk tolerance.

Published by eNeoteric Consultancy Services · cyber.encse.com · v1.0, August 2026

1. Account & Password Policy

Setting	Recommended Value	Verify (PowerShell)
Minimum password length	14 characters	(Get-ADDefaultDomainPasswordPolicy).MinPasswordLength
Password complexity	Enabled	(Get-ADDefaultDomainPasswordPolicy).ComplexityEnabled
Account lockout threshold	5 invalid attempts	(Get-ADDefaultDomainPasswordPolicy).LockoutThreshold
Account lockout duration	15 minutes minimum	(Get-ADDefaultDomainPasswordPolicy).LockoutDuration
Maximum password age	60–90 days	(Get-ADDefaultDomainPasswordPolicy).MaxPasswordAge
Reversible encryption	Disabled	(Get-ADDefaultDomainPasswordPolicy).ReversibleEncryptionEnabled

Rationale: CIS and NIST both recommend length over forced complexity/rotation for resisting brute-force and credential-stuffing attacks, while lockout thresholds slow online guessing without enabling denial-of-service against legitimate users.

2. Local Security Policy

2.1 Disable weak authentication protocols

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name
"LmCompatibilityLevel" -Value 5
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name "NoLMHash" -Value 1
```

LmCompatibilityLevel=5 forces NTLMv2-only and refuses LM/NTLMv1, closing off pass-the-hash and relay attacks that rely on the legacy protocol downgrade.

2.2 Enable LSA Protection (credential guard against dumping)

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa" -Name "RunAsPPL" -Value 1
```

Runs LSASS as a Protected Process, blocking common credential-dumping tools (e.g. Mimikatz) from reading its memory without a signed, Microsoft-trusted driver.

2.3 Disable SMBv1

```
Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol -NoRestart
Set-SmbServerConfiguration -EnableSMB1Protocol $false -Force
```

SMBv1 has no integrity protection and was the vector for WannaCry/NotPetya via EternalBlue. Disable unless a legacy device genuinely requires it, and isolate that device on a separate segment if so.

3. Windows Firewall & Network

- Enable Windows Firewall on all three profiles (Domain, Private, Public) — verify with `Get-NetFirewallProfile | Select Name,Enabled`.
- Block inbound by default; only explicitly allow required ports (RDP 3389 restricted to jump-host IPs only, never open to 0.0.0.0/0).
- Disable NetBIOS over TCP/IP and LLMNR/mDNS where not required — both are common lateral-movement/credential-relay vectors (Responder-style attacks).
- Restrict RDP to a jump host or VPN-only access; enforce Network Level Authentication (NLA).

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Terminal
Server\WinStations\RDP-Tcp" -Name "UserAuthentication" -Value 1
```

4. Auditing & Logging

Audit Category	Setting	Why
Logon/Logoff	Success and Failure	Detects brute-force and account compromise
Account Management	Success and Failure	Detects unauthorised account/group changes
Privilege Use	Success and Failure	Detects privilege escalation attempts
Process Creation	Success (with command-line auditing)	Enables detection of malicious tooling execution
Object Access (file share)	Success and Failure on sensitive shares	Detects unauthorised data access

```
auditpol /set /category:"Logon/Logoff" /success:enable /failure:enable
auditpol /set /subcategory:"Process Creation" /success:enable
Set-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Audit"
-Name "ProcessCreationIncludeCmdLine_Enabled" -Value 1
```

Ensure the Security event log size is increased from the 20MB default (e.g. 1GB+) and forwarded to a central SIEM — the default size rotates out evidence within hours on a busy server.

5. Services & Attack Surface Reduction

- Disable unused services: Print Spooler on non-print servers (PrintNightmare, CVE-2021-34527), Remote Registry, Telnet Client/Server, Fax.
- Uninstall unused Windows Features/Roles — every installed role expands the attack surface, whether or not it's actively used.
- Enable Windows Defender Attack Surface Reduction (ASR) rules, particularly the rules blocking Office child-process creation and credential stealing from LSASS.
- Enable Controlled Folder Access to protect against ransomware encryption of protected directories.

```
Stop-Service -Name Spooler -Force; Set-Service -Name Spooler -StartupType Disabled
Set-MpPreference -EnableControlledFolderAccess Enabled
Add-MpPreference -AttackSurfaceReductionRules_Ids 9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2
-AttackSurfaceReductionRules_Actions Enabled
```

6. Patch Management

- Apply security updates within 14 days of release for critical/exploited-in-the-wild CVEs; 30 days for high severity.
- Subscribe to CISA's Known Exploited Vulnerabilities (KEV) catalog and prioritise any listed CVE affecting Windows Server immediately.
- Test patches in a staging ring before production rollout, but do not let staging delay critical/actively-exploited patches beyond the target SLA.
- Maintain an accurate inventory of installed roles/features so patch impact can be assessed quickly.

7. Verification Checklist

Control	Verified
SMBv1 disabled	
LSA Protection (RunAsPPL) enabled	
NTLMv1/LM disabled (LmCompatibilityLevel=5)	
Firewall enabled on all profiles, default-deny inbound	
RDP restricted + NLA enforced	
Audit policy configured for logon, account mgmt, privilege use, process creation	
Security log size increased and forwarded to SIEM	
Unused services disabled (Spooler, Remote Registry, etc.)	
ASR rules and Controlled Folder Access enabled	
Patch SLA defined and tracked (14d critical / 30d high)	

Based on the CIS Microsoft Windows Server 2022 Benchmark. This guide is a starting baseline, not a complete hardening programme — validate against the full CIS Benchmark and your organisation's specific requirements.