Assignment 4.1: Risks/Threats/Vulnerabilities

Joshua A. Wortz

University of San Diego

CSOL-560

Dr Varma

11/17/2025

Hardening a Windows Server environment requires a structured, multi-layered approach that addresses risks, threats, and vulnerabilities across organizational, architectural, network, identity, software, and auditing domains. Modern guidance, including Microsoft's Security Baselines (Microsoft, 2024), DISA's Windows 11 STIG (Defense Information Systems Agency [DISA], 2024), and NIST SP 800-53 (NIST, 2020), emphasizes governance-driven, defense-in-depth strategies that integrate both technical and administrative controls. These frameworks collectively demonstrate that hardening is not only a matter of configuration but also of consistent lifecycle management and monitoring (Alsaadi & Niazi, 2020).

Organizational Security

Organizational security establishes the governance foundation upon which all technical security measures rely. Centralized baselines enforced through Group Policy prevent configuration drift and ensure servers begin from a consistent security posture (NIST, 2020). Segregation of duties among administrators, auditors, and analysts reduces the potential for insider threats and aligns with the principle of least privilege (Wang et al., 2021). Lifecycle governance, including documented change control and patch verification, ensures that operational updates do not reintroduce vulnerabilities. The STIG repeatedly emphasizes the importance of centralized oversight, particularly in areas such as privilege management, log protection, and configuration integrity (DISA, 2024).

Windows Server Preparation

Pre-installation hardening focuses on ensuring firmware integrity, implementing trusted boot processes, and configuring devices securely. Implementing Secure Boot, TPM 2.0, and

firmware updates aligns with core system integrity controls in NIST SP 800-53 and STIG baseline expectations (NIST, 2020; DISA, 2024). Disabling unnecessary hardware components reduces the attack surface and prevents potential exploitation at the firmware or bus level. Pre-installation cryptographic configuration, such as disabling legacy cipher suites, ensures secure defaults before the OS is deployed (Alsaadi & Niazi, 2020). Validating installation media protects against supply-chain attacks that could otherwise introduce malicious binaries into the system before hardening begins.

Windows Server Installation

Server installation requires the use of hardened images that enforce the least functionality by removing unnecessary roles and features (Alsaadi & Niazi, 2020). Enabling early protections such as virtualization-based security (VBS), Credential Guard, and hypervisor-enforced code integrity aligns with Microsoft's secure configuration guidance (Microsoft, 2023). Securing remote management defaults such as WinRM over HTTPS prevents insecure administrative channels from becoming operational norms. The STIG's emphasis on controlling service behavior and protecting core system processes reinforces the requirement to configure these protections at installation time (DISA, 2024).

User Account Security Hardening

User account hardening prevents unauthorized access and lateral movement. Enforcing separate administrative accounts with MFA aligns with NIST identity assurance principles (NIST, 2020). Disabling legacy protocols such as NTLMv1 and anonymous logon mitigates credential interception risks (Wang et al., 2021). Credential Guard protects LSASS and

authentication material using virtualization-based isolation (Microsoft, 2023). Registry-level protections against credential dumping attacks further strengthen identity boundaries (Sufatrio et al., 2018). Managing privileged account scope using tiered access models reduces opportunities for misuse or escalation (DISA, 2024).

Network Security Configuration

Network security configuration addresses remote attack vectors and protects servers from protocol abuse, credential interception, and unauthorized access. Enforcing a default-deny firewall posture and restricting inbound/outbound traffic aligns with system hardening research, which shows that reducing exposed services significantly lowers the attack probability (Alsaadi & Niazi, 2020). DISA STIG requirements emphasize disabling Basic authentication for WinRM and HTTP-based services, mandating the use of encrypted channels to prevent credential disclosure (DISA, 2024). Secure LDAP and SMB signing requirements further protect directory and file service operations from relay attacks. Minimizing legacy protocols such as SMBv1 aligns with Microsoft's secure baseline guidance and reduces susceptibility to widely exploited vulnerabilities (Microsoft, 2024). Network segmentation and restricting administrative traffic to dedicated management networks help prevent lateral movement, a core defense-in-depth principle outlined in NIST SP 800-53 (NIST, 2020).

Registry Security Configuration

Registry hardening safeguards the configuration store that controls authentication, privilege usage, and core system behaviors. STIG controls require restricting permissions on sensitive hives, including SYSTEM, SECURITY, and SAM, to prevent unauthorized users from

modifying core configuration values (DISA, 2024). Research shows that registry-based privilege escalation remains a high-risk attack vector when ACLs are improperly configured (Sufatrio et al., 2018). Enforcing registry-backed cryptographic and protocol settings, such as TLS versions and SMB signing, ensures alignment with enterprise security standards (NIST, 2020). Restricting remote registry access and monitoring registry paths associated with services and startup behavior decreases opportunities for persistence and unauthorized configuration drift (Wang et al., 2021).

General Security Settings

General system protections apply across all workloads and form the backbone of OS integrity. Enabling exploit mitigations such as DEP, ASLR, SEHOP, and HVCI prevents memory corruption, code injection, and kernel tampering (Alsaadi & Niazi, 2020). DISA STIG requirements emphasize the need to enable structured exception handling protections and ensure tamper-resistant process isolation (DISA, 2024). Least-functionality principles, such as disabling unused Windows components and legacy subsystems, align with research demonstrating that unnecessary functionality increases exploit surface area (Wang et al., 2021). System-wide cryptographic defaults, including enforcing minimum TLS versions, support secure communication standards recommended by NIST SP 800-53 (NIST, 2020). Continuous monitoring and configuration enforcement prevent drift from the approved system baseline.

Audit Policy Settings

Configuring audit policy settings ensures the system logs security-relevant actions consistently and comprehensively. NIST SP 800-53 and DISA STIG both require the use of

Advanced Audit Policy Configuration to produce granular, actionable telemetry (NIST, 2020; DISA, 2024). Logging process creation, including command-line arguments, is essential for detecting script-based attacks and "living off the land" behaviors (Alsaadi & Niazi, 2020). Capturing success and failure events for authentication, privilege use, policy changes, and account modifications supports behavioral analytics and anomaly detection used in SIEM systems. Ensuring appropriate log retention and preventing overwriting of critical audit data aligns with STIG controls designed to maintain forensic integrity (DISA, 2024).

Software Security Guide

Software hardening addresses the introduction, execution, and lifecycle of applications within Windows Server environments. Research has emphasized that restricting installation privileges and validating software sources can dramatically reduce risks from malicious code and supply-chain attacks (Wang et al., 2021). Application control technologies, such as Windows Defender Application Control and AppLocker, enforce the execution of signed code, providing strong defenses against ransomware and fileless malware (Microsoft, 2024). Patch management processes aligned with NIST and DISA requirements ensure timely mitigation of vulnerabilities (NIST, 2020; DISA, 2024). Defender for Endpoint and enterprise anti-malware tools provide behavioral analysis and real-time threat detection capabilities. Restricting script execution to signed PowerShell scripts limits misuse of automation tools often leveraged in adversary operations (Alsaadi & Niazi, 2020).

Audit Policy Best Practices

Audit policy best practices ensure audit data remains trustworthy, tamper-resistant, and operationally meaningful. Centralizing logs via SIEM or Windows Event Forwarding aligns with DISA STIG requirements for protecting logs from local modification (DISA, 2024). Maintaining retention periods that support long-term investigations reflects NIST SP 800-53 expectations for forensic readiness (NIST, 2020). Enforcing strict access controls on audit logs helps preserve confidentiality and prevents unauthorized users from tampering with them. Regular review cycles and automated correlation rules help detect anomalies earlier in the intrusion chain (Alsaadi & Niazi, 2020). Continuous compliance monitoring ensures audit configurations remain effective and consistent across the environment.

Types of Events You Can Audit

Windows Server provides auditing across various categories, including logon events, privilege use, account management, object access, directory service access, process tracking, and system events. These categories align with adversary behaviors identified in MITRE ATT&CK and are reinforced by DISA STIG's comprehensive auditing requirements (DISA, 2024). Identity-related events, such as authentication and Kerberos ticket activity, support the detection of credential theft attempts. Privilege use and policy change events help identify unauthorized elevation or tampering with configuration. Object access events provide visibility into attempts to access sensitive or protected resources. Research on system hardening emphasizes that comprehensive event coverage is essential for early breach detection (Wang et al., 2021).

Recommended Audit Policy Settings

Recommended audit settings involve capturing both success and failure events for high-value categories. Logging success and failure for logon events reveals brute-force attempts and legitimate identity usage patterns (NIST, 2020). Monitoring account management and privilege use events provides insight into attempted or successful administrative actions (Alsaadi & Niazi, 2020). Auditing policy changes allows for the detection of attempts to weaken the security posture or disable auditing, which STIG identifies as high-severity indicators of compromise (DISA, 2024). Successful process creation logs with command-line parameters are essential for visibility into script execution and attacker tradecraft (Microsoft, 2024). System events related to startup, shutdown, and service failures also provide valuable detection signals.

Best Practices for Auditing

Best practices for auditing ensure that logs maintain integrity, availability, and evidentiary value. STIG controls require protecting Security, System, and Application log permissions to prevent unauthorized access (DISA, 2024). Preventing log overwriting and ensuring adequate storage preserves critical events for forensic analysis and investigation. Integrity-monitoring solutions help detect unauthorized changes to audit data. Ensuring the Event Log service remains operational and protected from tampering supports continuous monitoring, a core requirement of NIST SP 800-53 (NIST, 2020). Integrating log data with automated analytics and security incident workflows ensures that the information collected leads to actionable detection and response.

Conclusion

Windows Server hardening requires a cohesive strategy spanning governance, configuration, identity management, network protection, software control, and auditing. Each of the thirteen categories contributes to defense-in-depth by reducing attack surface, enforcing least privilege, strengthening system integrity, and ensuring security-relevant activity is captured and analyzed. When implemented together and aligned with authoritative frameworks such as DISA STIG, NIST SP 800-53, and Microsoft's secure baselines, these controls create a resilient server environment capable of resisting modern cyber threats. Scholarly research consistently reinforces the effectiveness of these techniques, demonstrating that hardening, when properly governed and applied, remains one of the most effective defenses against system compromise.

References

Alsaadi, I. M., & Niazi, M. (2020). System hardening approaches for operating systems security: A systematic literature review. *Computer Standards & Interfaces, 71*, 103431. https://doi.org/10.1016/j.csi.2020.103431

Defense Information Systems Agency. (2024). *Windows 11 Security Technical Implementation Guide (STIG), Release 5*. https://public.cyber.mil/stigs/

Microsoft. (2023). *Credential Guard and virtualization-based security overview*. https://learn.microsoft.com/windows/security/identity-protection/credential-guard/

Microsoft. (2024). *Windows security baseline documentation*. https://learn.microsoft.com/windows/security

National Institute of Standards and Technology. (2020). *Security and privacy controls for information systems and organizations (SP 800-53 Rev. 5)*. https://doi.org/10.6028/NIST.SP.800-53r5

Sufatrio, S., Saxena, P., & Liang, Z. (2018). Preventing registry-based privilege escalation through integrity policy enforcement. *Digital Investigation, 26*, S1–S10. https://doi.org/10.1016/j.diin.2018.04.015

Wang, T., Li, X., & Sun, H. (2021). Enhancing system resilience through privilege separation and secure configuration baselines. *Journal of Information Security and Applications, 58*, 102788. https://doi.org/10.1016/j.jisa.2021.102788

Appendix A — Windows Server Hardening Controls Itemized by Category

1. Organizational Security

- Maintain and centrally enforce server configuration baselines through GPO.
- Implement formal change management and documentation procedures for all server modifications.
- Enforce separation of duties between administrators, auditors, and security analysts. Conduct regular configuration drift monitoring and baseline comparison.
- Maintain asset inventories documenting server purpose, baseline, and lifecycle state.
- Implement privileged access management (PAM) for administrative credential control.

Windows Server Preparation

- Enable Secure Boot and TPM 2.0 to ensure hardware-rooted trust.
- Disable unused hardware interfaces such as Bluetooth, Wi-Fi, and secondary NICs.
- Configure BIOS/UEFI firmware passwords to prevent unauthorized boot configuration changes.
- Validate installation media hash values to prevent supply chain tampering.
- Disable legacy cipher suites and enforce secure cryptographic algorithms before installation.
- Restrict physical console access to authorized provisioning personnel only.

Windows Server Installation

- Use hardened, pre-approved server images aligned to enterprise baselines.
- Enable virtualization-based security (VBS) and hypervisor-enforced code integrity (HVCI).
- Configure WinRM to use HTTPS-only management channels.
- Install only the required server roles and features based on least-functionality principles.
- Harden initial service startup types and remove unnecessary default services.
- Apply restricted ACLs to system directories at installation time.

User Account Security Hardening

- Use separate privileged and non-privileged accounts for administrators.
- Enforce multi-factor authentication for all administrative accounts.
- Disable legacy authentication protocols such as NTLMv1 and anonymous logon.
- Enable Credential Guard to isolate credential material from LSASS.
- Randomize local administrator passwords via LAPS or gMSA.
- Restrict which accounts can log on locally, remotely, or as services.

Network Security Configuration

- Enforce a default-deny Windows Firewall posture with explicit allow rules.
- Require encrypted WinRM management channels and disable Basic authentication.
- Enable LDAP signing and channel binding to prevent credential relay attacks.
- Require SMB signing and disable SMBv1.

- Enforce TLS 1.2+ and disable weak cipher suites.
- Implement network segmentation and place servers on restricted management subnets.
- Restrict administrative protocols (RDP, WinRM) to authorized jump hosts only.

Registry Security Configuration

- Apply restrictive ACLs to security-sensitive registry hives (SAM, SYSTEM, SECURITY).
- Disable remote registry access unless explicitly required.
- Enforce cryptographic, authentication, and protocol settings through registry-based policies.
- Monitor registry paths controlling service startup behavior to prevent persistence.
- Disable legacy protocols (e.g., LSA anonymous logon) through registry security keys.
- Use registry auditing to detect unauthorized modification attempts.

General Security Settings

- Enable exploit mitigations such as DEP, ASLR, SEHOP, and CFG.
- Remove unnecessary Windows components and legacy subsystems.
- Enforce file integrity protections for system binaries and configuration data.
- Require minimum TLS versions and strong cipher suites system-wide.
- Disable guest access features and anonymous enumeration methods.
- Enforce tamper protection for Windows Defender and security agents.

Audit Policy Settings

- Enable Advanced Audit Policy Configuration for granular logging.
- Audit logon/logoff (success and failure) events for identity monitoring.
- Audit privilege use (success and failure) to detect escalation attempts.
- Audit account management (success and failure) for unauthorized changes.
- Audit policy change events to detect tampering.
- Enable process creation auditing with command-line visibility.
- Configure log retention and prevent audit logs from being overwritten.

Software Security Guide

- Restrict software installation privileges to authorized administrators.
- Enforce allow-listed software execution via WDAC or AppLocker.
- Require signed PowerShell scripts and restrict script execution policies.
- Deploy enterprise anti-malware with real-time protection and cloud-based analysis.
- Maintain a full software inventory and remove unused or outdated applications.
- Use WSUS or endpoint management tools to enforce timely patching.

Audit Policy Best Practices

- Centralize log collection via SIEM or Windows Event Forwarding.
- Define long-term retention periods for compliance and forensic readiness.
- Enforce strict access controls on Security, System, and Application logs.
- Synchronize system time via a trusted NTP hierarchy for log correlation.
- Conduct regular log review cycles with documented escalation procedures.

- Monitor log health, size thresholds, and forwarding channel integrity.

Types of Events You Can Audit

- Logon/logoff and authentication events.
- Privilege use and escalation-related actions.
- Account creation, modification, and deletion.
- Object access events for files, folders, and registry keys.
- Process creation, termination, and command-line activity.
- System startup, shutdown, and crash events.
- Directory service access (for domain-joined systems).
- Policy change and configuration modification events.

Recommended Audit Policy Settings

- Audit Logon: Success and Failure.
- Audit Account Management: Success and Failure.
- Audit Privilege Use: Success and Failure.
- Audit Policy Change: Success and Failure.
- Audit Object Access: Success and Failure (on sensitive assets).
- Audit Process Creation: Success (with command-line parameters).
- Audit System Events: Success.

Best Practices for Auditing

- Prevent audit logs from being overwritten by configuring “Do not overwrite events.”
- Enforce permissions preventing non-privileged users from viewing or clearing logs.
- Enable file integrity monitoring for log tamper detection.
- Ensure the Event Log service cannot be disabled by normal administrators.
- Validate log forwarding channels and SIEM connectivity continuously.
- Perform periodic audit configuration reviews to detect drift.