2024

Research And Explain 10 Security Hardening Best Practices For The Windows Operating System

MOSSÉ CYBERSECURITY INSTITUTE

AARON AMRAN

Student ID: nxCLnZGLgyOUMpnDw16rtDvYuTF2

1. Organizational Security

1.1 Develop and Enforce Security Policies

- **Define and Document Policies**: Create comprehensive security policies tailored to your organization's needs. These policies should define acceptable use of resources, password requirements (e.g., complexity, length, rotation), access control guidelines, and incident response procedures. Include detailed steps for handling common scenarios like suspected phishing emails or a detected malware outbreak.
- **Enforce Policies with Group Policy Objects (GPOs)**: Use Active Directory's GPOs to automate enforcement of these policies across all computers and users. For instance, you can mandate password length, disable USB access, or enforce software installation restrictions organization-wide.
- **Security Awareness Training**: Regularly educate employees on recognizing threats like phishing emails, malicious attachments, and social engineering attacks. Use real-world simulations and follow-up discussions to reinforce learning. Training should be conducted quarterly or biannually.

1.2 Patch Management

- **Centralized Update System**: Use tools like Windows Server Update Services (WSUS) or Microsoft Endpoint Configuration Manager to manage updates. These tools allow you to approve, schedule, and deploy patches for both Windows and third-party software to ensure all devices are up to date.
- **Regular Patching Schedule**: Schedule patching during off-peak hours to minimize disruptions. Test updates on a few machines in a controlled environment before a full rollout to prevent compatibility issues.
- **Third-Party Software Updates**: Don't overlook non-Microsoft software. Use tools like Chocolatey or third-party patching solutions to keep applications like Adobe Reader, Java, or web browsers up to date, as they're common entry points for attackers.

1.3 Role-Based Access Control (RBAC)

- **Principle of Least Privilege (PoLP)**: Assign only the permissions users need for their specific roles. For instance, a marketing team member shouldn't have access to financial data. This minimizes the impact if an account is compromised.
- **Role Management via Active Directory (AD)**: Organize users into groups in AD based on their job roles (e.g., HR, IT, Finance) and assign permissions at the group level. Avoid granting access directly to individual accounts to make auditing and role changes easier.
- **Regular Access Reviews**: Periodically review user roles and permissions to ensure they align with current job responsibilities. Use automated tools or scripts to detect and report excessive or unused privileges.

2. Windows Server Security

2.1 Enable Secure Boot and Trusted Boot

- **Secure Boot**: This UEFI-based feature validates that the OS is booting with trusted software, blocking unauthorized changes to firmware or bootloaders. Configure it in the system's BIOS/UEFI settings and ensure only signed drivers and boot files are loaded.
- **Trusted Boot**: After Secure Boot completes, Trusted Boot ensures that the integrity of Windows components is checked during startup. Configure it using Group Policy or local security policies to ensure malware can’t tamper with system files.

2.2 Harden Remote Desktop Protocol (RDP)

- **Restrict RDP Access**: Use Windows Firewall or network firewalls to allow RDP access only from specific IP addresses or VPNs. Avoid exposing RDP directly to the internet.
- **Network-Level Authentication (NLA)**: Enable NLA to require authentication before an RDP session is established. This protects against attackers attempting to brute-force credentials on exposed machines.
- **RDP Gateway**: Use an RDP gateway server as a secure entry point to manage RDP connections. This adds encryption and additional layers of authentication.
- **Disable RDP When Not Needed**: If RDP is not in active use, disable it completely to eliminate potential attack vectors. This can be done through the system settings or Group Policy.

2.3 Enable Windows Defender Credential Guard

- **Credential Protection**: Windows Defender Credential Guard protects sensitive credentials like Kerberos tickets and NTLM hashes by isolating them in a secure virtualized environment. This ensures that even if malware runs on the system, it cannot access these secrets.
- **Requirements**: This feature requires hardware support for virtualization, such as Hyper-V and a compatible processor. Enable it via Group Policy (Computer Configuration > Administrative Templates > System > Device Guard > Turn On Virtualization Based Security).

3. User Account Security

3.1 Enforce Strong Password Policies

- **Complexity and Length**: Require passwords to be at least 12-16 characters, including uppercase letters, lowercase letters, numbers, and special characters. Avoid allowing users to use easily guessable information like dictionary words or names.
- **Password Rotation**: Set policies to require users to change passwords every 60-90 days. Prevent reuse of the last 5-10 passwords to discourage cycling through old passwords.
- **Multi-Factor Authentication (MFA)**: Require MFA for all accounts, especially administrator and remote access accounts. MFA combines something the user knows (password) with something they have (a mobile device or hardware token) for better security.

3.2 Disable Unused Accounts

- **Regular Audits**: Use PowerShell scripts (Get-ADUser or Get-LocalUser) to identify inactive or unused accounts. Accounts belonging to former employees or default accounts like “Guest” should be disabled or deleted.
- **Automation**: Configure scripts or identity management solutions to automatically disable accounts after a defined period of inactivity (e.g., 30 days) to minimize manual intervention.

3.3 Implement Account Lockout Policies

- **Failed Attempt Thresholds**: Configure account lockout policies to lock an account after 3-5 failed login attempts. This deters brute-force attacks while allowing legitimate users to recover easily.
- **Lockout Duration**: Set a temporary lockout duration (e.g., 15-30 minutes) rather than indefinite locking. This ensures legitimate users can retry without requiring IT intervention.
- **GPO Configuration**: Use Group Policy to configure these settings (Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Account Lockout Policy).

4. Network Security

4.1 Enable Windows Firewall with Advanced Security

- **Define Rules**: Windows Firewall is a built-in feature that controls incoming and outgoing traffic. To secure your network, configure **inbound rules** to allow traffic only for essential services (e.g., web server or file sharing) and block everything else. Similarly, set **outbound rules** to limit applications that can send data outside the network, preventing unauthorized exfiltration.
- **Logging Traffic**: Enable logging for Windows Firewall to monitor allowed and blocked traffic. Logs can be configured in the Advanced Security snap-in (Windows Firewall with Advanced

Security > Monitoring > Firewall). Regularly review logs to identify unusual traffic patterns, which may indicate malicious activity.

4.2 Use IPsec for Encryption

- **What is IPsec**: IPsec (Internet Protocol Security) secures communication between devices by encrypting data packets. This ensures that even if traffic is intercepted, it cannot be read without the decryption keys.
- **Policies for Ports and Protocols**: Use the IPsec policy settings in Group Policy to define which traffic should be encrypted. For example, secure communication between critical servers by applying IPsec to TCP ports used by sensitive services like database or file transfer.
- **Authentication**: Combine IPsec with Active Directory integration for mutual authentication between endpoints, further enhancing security.

4.3 Disable Unused Network Protocols

- **Legacy Protocols**: Outdated protocols like SMBv1, Telnet, or NetBIOS are often exploited by attackers. For example, SMBv1 was used in the infamous WannaCry ransomware attack. Disable these protocols unless absolutely necessary.
- **How to Disable**: Use PowerShell commands (e.g., Set-SmbServerConfiguration -EnableSMB1Protocol $false) or the **Windows Features** control panel to turn off these protocols. Ensure replacements, like SMBv2 or SMBv3, are correctly configured.
- **Secure Alternatives**: Always prefer secure protocols like HTTPS instead of HTTP and SSH instead of Telnet for remote management. Enforce these through policy or configuration management tools.

5. Registry Security

5.1 Restrict Access to the Registry

- **What is the Registry**: The Windows Registry contains configuration data for the operating system and installed software. If compromised, attackers can modify critical settings or persist malicious code.
- **Restrict Permissions**: Use the Registry Editor (regedit.exe) or Group Policy to restrict permissions on sensitive keys like HKLM\SAM, which stores account information. Grant access only to administrators and system accounts to prevent unauthorized changes.
- **Automation**: Automate this process using scripts like PowerShell to ensure consistent enforcement across multiple machines.

5.2 Enable Registry Auditing

- **Purpose**: Registry auditing logs changes to specified keys, helping administrators detect unauthorized modifications.

- **How to Configure**: Open Local Security Policy (secpol.msc), navigate to Advanced Audit Policy Configuration > Object Access, and enable auditing for "Registry." Then, specify keys to audit (e.g., HKLM\SYSTEM) by setting audit permissions in the registry editor.
- **Log Review**: Regularly review logs in the Event Viewer under the "Security" log to identify suspicious changes.

5.3 Back Up the Registry Regularly

- **Why Backups Matter**: The registry is crucial for system functionality. Corruption or malicious changes can render a system unstable. Regular backups ensure quick recovery.
- **Manual Backup**: Use the Registry Editor's **Export** feature to save a copy of the registry to a safe location. This can also be done with the command reg export HKLM\SOFTWARE C:\Backup\Registry.bak in PowerShell or Command Prompt.
- **Automated Backup**: Configure a script or third-party tool to schedule regular backups. Store these backups securely, using encryption if needed.

6. General Security

6.1 Implement Disk Encryption

- **Why Encrypt**: Disk encryption prevents unauthorized access to data on a system, especially if the device is lost or stolen. BitLocker is a native Windows tool for full-disk encryption.
- **BitLocker Configuration**: Enable BitLocker via the **Control Panel** or PowerShell (Enable-BitLocker -MountPoint "C:"). Store recovery keys securely, either in Active Directory or a physical safe.
- **Pre-Boot Authentication**: For added security, configure BitLocker with pre-boot authentication (e.g., PIN or USB key). This ensures that encryption keys are not loaded until proper authentication is provided.

6.2 Disable Unnecessary Services

- **Minimize Attack Surface**: Each running service represents a potential vulnerability. For example, leaving the **Print Spooler** service running on a server that doesn’t need it can expose the system to exploits like PrintNightmare.
- **How to Disable**: Use the **Services Management Console** (services.msc) or PowerShell (Set-Service -Name "Spooler" -StartupType Disabled) to disable unnecessary services.
- **Audit Services**: Regularly review running services using tools like PowerShell (Get-Service) and cross-reference them with your organization's baseline of required services.

6.3 Secure System Backups

- **Regular Backups**: Schedule automatic backups of critical files and system states. Use tools like Windows Backup or third-party solutions that integrate with the OS.
- **Offsite Storage**: Store backups in a secure offsite location, such as a dedicated backup server or cloud storage. This protects against disasters like ransomware or physical theft.
- **Encrypt Backup Files**: Use AES-256 encryption or similar standards to ensure backup data is secure. Most modern backup tools include encryption options during the backup process.

7. Audit Policy

7.1 Configure Advanced Audit Policies

- **Why It's Important**: Advanced Audit Policies provide granular control over what events are logged, enabling administrators to monitor critical activities like logins, privilege escalations, and unauthorized file access.
- **How to Enable**:
    - Open the **Local Security Policy** tool (secpol.msc) and navigate to **Advanced Audit Policy Configuration**.
    - Expand **Audit Policies** to configure specific categories such as **Logon/Logoff**, **Account Management**, and **Object Access**.
    - Example: Enable "Audit Logon Events" to track every login attempt and "Audit Object Access" to monitor access to sensitive files or folders.
- **Using Group Policy**: Deploy a consistent policy across multiple machines using Group Policy Management. Go to **Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration** and define organization-wide settings.
- **Benefit**: This ensures a robust audit trail for detecting suspicious activity and conducting investigations.

7.2 Use Centralized Log Management

- **Why It's Important**: Storing logs locally on each machine is inefficient and risky. Centralized log management provides a single point to collect, analyze, and archive logs, simplifying monitoring and compliance.
- **How to Implement**:
    - Use **Windows Event Collector (WEC)** to forward logs from multiple systems to a central server.
    - Alternatively, configure a SIEM (Security Information and Event Management) solution like Splunk, ELK Stack, or Microsoft Sentinel. These tools aggregate logs and provide powerful search, analysis, and alerting capabilities.

    - Ensure secure transmission using encryption (e.g., HTTPS or TLS) to prevent log tampering.
- **Benefit**: A centralized approach makes it easier to identify patterns, correlate events across systems, and maintain logs for audits or compliance needs.

7.3 Review Logs Regularly

- **Why It's Important**: Logs are only valuable if reviewed. Regular log analysis helps identify anomalies, such as repeated failed login attempts, unusual privilege escalations, or access to critical files at odd hours.
- **How to Review**:
    - Use built-in tools like **Event Viewer** to manually inspect logs for specific events. For example, filter the "Security" log for Event ID 4625 (failed login attempts).
    - Automate reviews using scripts or third-party tools that flag anomalies. Example: PowerShell scripts can extract specific log entries and highlight patterns.
    - Define a log retention policy to maintain sufficient history for forensic investigations.
- **Focus on High-Priority Events**: Examples include:
    - **4625**: Failed login attempt.
    - **4673**: Privilege use.
    - **5140**: File share access.

8. Software Security

8.1 Restrict Software Installation

- **Why It's Important**: Allowing unrestricted software installation increases the risk of malware infections or unauthorized tools being deployed, which could compromise system integrity.
- **How to Restrict**:
    - Use **AppLocker**: Configure AppLocker rules to specify which applications and scripts are allowed to run. AppLocker can enforce restrictions based on file path, publisher, or file hash.
        - Example: Allow only applications installed in C:\Program Files\ and block all executables from user directories.
    - **Windows Defender Application Control**: For stricter environments, enforce whitelisting using WDAC policies to control application execution.
    - Enable **User Account Control (UAC)**: Configure UAC to prompt for administrative approval before installing software, ensuring only authorized personnel can make changes.

- **Benefit**: Limits the attack surface by preventing unauthorized or malicious software from running.

8.2 Keep Software Updated

- **Why It's Important**: Vulnerabilities in outdated software are a primary attack vector. Regular updates close these security gaps and reduce the risk of exploitation.
- **How to Keep Updated**:
    - Use Windows Update for OS patches and tools like **Secunia PSI** or **Patch My PC** for third-party software updates.
    - Create an update schedule to regularly patch applications, browsers, and plugins like Java or Adobe Acrobat. Automate this process where possible.
    - Maintain an inventory of installed software to track update requirements and remove unsupported applications.
- **Benefit**: Ensures systems remain protected against known vulnerabilities.

8.3 Run Applications with Limited Privileges

- **Why It's Important**: Applications running with administrative rights can perform unrestricted actions, potentially escalating malware attacks or causing accidental damage.
- **How to Limit Privileges**:
    - Avoid logging in as an administrator for routine tasks. Use a standard user account instead.
    - Configure applications to run with the lowest privileges required for functionality. For example, developers can use tools like **RunAs** or the "Run as different user" option.
    - Use **sandboxing**: Tools like **Windows Sandbox** or third-party solutions (e.g., VMware Workstation, Docker) can isolate high-risk applications from the rest of the system.
- **Example**: Running a web browser with admin rights could allow malware to modify system files. Instead, sandbox the browser to restrict its access to critical resources.
- **Benefit**: Mitigates the impact of attacks and accidental errors by restricting application capabilities.

References (Team, 2024)

Parvez, S. (17 September, 2023). *A guide to the hardening of the Windows 11 operating system*. Retrieved from spca.education: https://spca.education/windows-11-hardening/

Sagstetter, H. (14 July, 2022). *Is Windows 10 secure? 12 best practices for small businesses*. Retrieved from adeliarisk.com: https://adeliarisk.com/is-windows-10-secure-12-best-practices/

Team, U. (18 November, 2024). *How to Secure Your Windows Environment: Top 10 Ways*. Retrieved from upguard.com: https://www.upguard.com/blog/top-10-ways-to-secure-your-windows-environment

Zamir, T. (2024). *Windows 10 Hardening: 19 Ways to Secure Your Workstations*. Retrieved from perception-point.io: https://perception-point.io/guides/os-isolation/windows-10-hardening-19-ways-to-secure-your-workstations/