A COMPREHENSIVE CHECKLIST FOR

Windows Hardening

In response to the ever-growing attack surface, our Security Operations Analyst Cameron Krivanek has put together a list of top recommended Windows hardening techniques you can use to boost security and reduce risk across your enterprise systems.

What is hardening?

Hardening involves reducing risk through the identification and remediation of vulnerabilities across the attack surface of a system. A system tends to have more vulnerabilities or a larger attack surface as its complexity or functionality increases.

Hardening is necessary in a production environment in order to reduce any risk and loss to critical business assets, but it is also a process that can–and often should–be applied everywhere.

Proactive security techniques can significantly reduce your risk

Below is an unordered list of best practices the viewer should implement and/or perform.

Quick Note: Depending on your environment, there will be use cases where certain settings are appropriate, but others may not be desirable for functionality or usability purposes. Some techniques may only be relevant or specific to certain Windows versions. For example, the DisableAntiSpyware registry key is now considered legacy and the setting is now protected under tamper protection on newer versions of Windows 10.

It is highly recommended that you understand and test these settings before implementation so as to avoid any unexpected breaks that might occur.

MICROSOFT DEFENDER FIREWALL

- [ ] Enable all profiles, disable inbound by default, and enable inbound and outbound rules as needed for services.

  Note: Be wary of remote access protocols (e.g., Telnet, SSH, RDP).

SERVICES

- [ ] Disable any unnecessary services on the system
- [ ] Disable Remote Registry

USER ACCOUNTS

- [ ] Apply the principle of least privilege
- [ ] **Disable Accounts**
  - Default accounts
  - Unused accounts

STARTUP

- [ ] Disable or remove any unnecessary executables or services that run on startup / logon (Sysinternals Autoruns is a great tool for this)

WINDOWS FEATURES

- [ ] Disable unused features (e.g., Telnet / TFTP clients, WSL)

WINDOWS UPDATES

- [ ] Ensure all appropriate patches, hotfixes, and service packs are applied promptly

WINDOWS DEFENDER ANTIVIRUS

- [ ] Ensure this is enabled and up to date with definitions

GROUP POLICY OBJECT (GPO)

- [ ] **Password policy**
  - Minimum password length: 8 characters
  - Maximum password length: 64 characters
  - Minimum password age: 1 day
  - Maximum password age: 90 days
  - Complexity requirements: Enabled
  - Store passwords using reversible encryption: Disabled
- [ ] **Lockout policy**
  - Account lockout duration: 15 minutes
  - Account lockout threshold: 10 failed authentication attempts
  - Reset counter after: 15 minutes
- [ ] **User Account Control**
  - Admin Approval Mode for the built-in Administrator account: Enabled
  - Run all administrators in Admin Approval Mode: Enabled
- [ ] **Interactive logon**
  - Machine inactivity limit: 900 seconds
  - Prompt user to change password before expiration: 14 days
  - Do not require CTRL+ALT+DEL: Disabled

- [ ] **Network Access**
  - Do not allow anonymous enumeration of SAM accounts: Enabled
  - Do not allow anonymous enumeration of SAM accounts and shares: Enabled
- [ ] **Network Security**
  - LAN Manager authentication level: 5 (Send NTLMv2 response only. Refuse LM & NTLM)
- [ ] **Windows Defender Antivirus**
  - Turn off Windows Defender Antivirus: Disabled
- [ ] **Windows Update**
  - Configure Automatic Updates: 3 (automatically download and notify for install)
  - Remove access to use all Windows Update features: Disabled
- [ ] **Additional notes**
  - Applocker: restrict executables for certain users
  - Bitlocker: encrypt drives through File Explorer or GPO
  - Password: protect the screensaver

REGISTRY

The registry is a hierarchical database used to store configuration information for users, applications, and hardware devices. Group policy is used to push values into the registry for settings. There are registry keys associated with these policies. If you want to use Command Prompt, you can edit the registry directly with the reg command. If you edit the registry directly, we recommend that you back it up beforehand in case anything goes wrong.

REGISTRY COMMANDS

- [ ] **Enable User Account Control (UAC):**
  reg add HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t Reg DWORD /d 1 /f
- [ ] **Enable Windows Defender Antivirus:**
  reg delete “HKLM\Software\Policies\Microsoft\Windows Defender” /v DisableAntiSpyware /f
- [ ] **Enable Automatic Updates**
  reg add “HKLM\Software\Microsoft\Windows\CurrentVersion\WindowsUpdate\AU” /v NoAutoUpdate /t Reg_DWORD /d 0 /f
- [ ] **Automatically download and notify of install for updates**
  reg add “HKLM\Software\Microsoft\Windows\CurrentVersion\WindowsUpdate\AU” /v AUOptions /t Reg_DWORD /d 3 /f
- [ ] **Restrict anonymous access:**
  reg add HKLM\System\CurrentControlSet\Control\Lsa\ /v restrictanonymous /t Reg_DWORD /d 1 /f
- [ ] **Block anonymous enumeration of SAM accounts and shares:**
  reg add HKLM\System\CurrentControlSet\Control\Lsa\ /v restrictanonymoussam /t Reg_DWORD /d 1 /f
- [ ] **Send NTLMv2 response only; refuse LM & NTLM:**
  reg add HKLM\System\CurrentControlSet\Control\Lsa\ /v lmcompatibilitylevel /t Reg_DWORD /d 5 /f
- [ ] **Disable admin autologon:**
  reg add “HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon” /v AutoAdminLogon /t Reg_DWORD /d 0 /f

- [ ] **Prevent the inclusion of the Everyone security group SID in the anonymous user's access token:**
reg add HKLM\System\CurrentControlSet\Control\Lsa\ /v everyoneincludesanonymous /t Reg_DWORD /d 0 /f

- [ ] **Disable EnablePlainTextPassword:**
reg add HKLM\System\CurrentControlSet\services\LanmanWorkstation\Parameters /v EnablePlainTextPassword /t Reg_DWORD /d 0 /f

- [ ] **Disable IPv6:**
reg add HKLM\System\CurrentControlSet\services\TCPIP6\Parameters /v DisabledComponents /t Reg DWORD /d 255 /f

- [ ] **Disable Remote Desktop Protocol (RDP):**
reg add "HKLM\System\CurrentControlSet\Control\Terminal Server" /f /v fDenyTSConnections /t Reg DWORD /d 1

Helpful Resources

REFERENCES

- Server Hardening Standard (Windows) via the University of Connecticut
- Windows Security Hardening Configuration Guide via Cisco
- Blue Team Field Manual

SOFTWARE FOR BENCHMARKING / BEST PRACTICES

- CIS tools and best practices collection
- Microsoft Security Compliance Toolkit 1.0

Windows hardening is a fascinating topic. It enhances security by reducing risk and vulnerabilities. Hardening covers many separate aspects of the operating system, and you may better understand Windows by going through the different components and hardening them.

How Hurricane Labs can help

Hurricane Labs' dedicated SOC can help you implement the appropriate strategies for your enterprise environment. Contact us to learn how we can help harden your security and reduce your risk of attack.

P. 216-923-1330 | 888-276-4106
E. sales@hurricanelabs.com