netwrix

Windows Server Hardening Checklist

Table of Contents

Windows Server hardening involves identifying and remediating security vulnerabilities. Here are the top Windows Server hardening best practices you can implement immediately to reduce the risk of attackers compromising your critical systems and data.

Organizational Security

- ✓ Maintain an inventory record for each server that clearly documents its baseline configuration and records each change to the server.
- ✓ Thoroughly test and validate every proposed change to server hardware or software before making the change in the production environment.
- ✓ Regularly perform a risk assessment. Use the results to update your risk management plan and maintain a prioritized list of all servers to ensure that security vulnerabilities are fixed in a timely manner.
- ✓ Keep all servers at the same revision level.

Windows Server Preparation

- ✓ Protect newly installed machines from hostile network traffic until the operating system is installed and hardened. Harden each new server in a DMZ network that is not open to the internet.
- ✓ Set a BIOS/firmware password to prevent unauthorized changes to the server startup settings.
- ✓ Disable automatic administrative logon to the recovery console.
- ✓ Configure the device boot order to prevent unauthorized booting from alternate media.

Windows Server Installation

- Ensure the system does not shut down during installation.
- Use the Security Configuration Wizard to create a system configuration based on the specific role that is needed.
- Ensure that all appropriate patches, hotfixes and service packs are applied promptly. Security patches resolve known vulnerabilities that attackers could otherwise exploit to compromise a system. After you install Windows Server, immediately update it with the latest patches via WSUS or SCCM.
- Enable automatic notification of patch availability. Whenever a patch is released, it should be analyzed, tested and applied in a timely manner using WSUS or SCCM.

User Account Security Hardening

- Ensure your administrative and system passwords meet password best practices. In particular, verify that privileged account passwords are not be based on a dictionary word and are at least 15 characters long, with letters, numbers, special characters and invisible (CTRL ˆ) characters interspersed throughout. Ensure that all passwords are changed every 90 days.
- Configure account lockout Group Policy according to account lockout best practices.
- Disallow users from creating and logging in with Microsoft accounts.
- Disable the guest account.
- Do not allow “everyone” permissions to apply to anonymous users.
- Do not allow anonymous enumeration of SAM accounts and shares.
- Disable anonymous SID/Name translation.
- Promptly disable or delete unused user accounts.

Network Security Configuration

- ✓ Enable the Windows firewall in all profiles (domain, private, public) and configure it to block inbound traffic by default.
- ✓ Perform port blocking at the network setting level. Perform an analysis to determine which ports need to be open and restrict access to all other ports.
- ✓ Restrict the ability to access each computer from the network to Authenticated Users only.
- ✓ Do not grant any users the 'act as part of the operating system' right.
- ✓ Deny guest accounts the ability to log on as a service, a batch job, locally or via RDP.
- ✓ If RDP is utilized, set the RDP connection encryption level to high.
- ✓ Remove Enable LMhosts lookup.
- ✓ Disable NetBIOS over TCP/IP.
- ✓ Remove ncacn_ip_tcp.
- ✓ Configure both the Microsoft Network Client and the Microsoft Network Server to always digitally sign communications.
- ✓ Disable the sending of unencrypted passwords to third-party SMB servers.
- ✓ Do not allow any shares to be accessed anonymously.
- ✓ Allow Local System to use computer identity for NTLM.
- ✓ Disable Local System NULL session fallback.
- ✓ Configure allowable encryption types for Kerberos.
- ✓ Do not store LAN Manager hash values.
- ✓ Set the LAN Manager authentication level to allow only NTLMv2 and refuse LM and NTLM.
- ✓ Remove file and print sharing from network settings. File and print sharing could allow anyone to connect to a server and access critical data without requiring a user ID or password.

Registry Security Configuration

- ✓ Ensure that all administrators take the time to thoroughly understand how the registry functions and the purpose of each of its various keys. Many of the vulnerabilities in the Windows operating system can be fixed by changing specific keys, as detailed below.
- ✓ Configure registry permissions. Protect the registry from anonymous access. Disallow remote registry access if not required.
- ✓ Set MaxCachedSockets (REG_DWORD) to 0.
- ✓ Set SmbDeviceEnabled (REG_DWORD) to 0.
- ✓ Set AutoShareServer to 0.
- ✓ Set AutoShareWks to 0.
- ✓ Delete all value data INSIDE the NullSessionPipes key.
- ✓ Delete all value data INSIDE the NullSessionShares key.

General Security Settings

- ✓ Disable unneeded services. Most servers have the default install of the operating system, which often contains extraneous services that are not needed for the system to function and that represent a security vulnerability. Therefore, it is critical to remove all unnecessary services from the system.
- ✓ Remove unneeded Windows components. Any unnecessary Windows components should be removed from critical systems to keep the servers in a secure state.
- ✓ Enable the built-in Encrypting File System (EFS) with NTFS or BitLocker on Windows Server.
- ✓ If the workstation has significant random access memory (RAM), disable the Windows swapfile. This will increase performance and security because no sensitive data can be written to the hard drive.
- ✓ Do not use AUTORUN. Otherwise, untrusted code can be run without the direct knowledge of the user; for example, attackers might put a CD into the machine and cause their own script to run.
- ✓ Display a legal notice like the following before the user logs in: “Unauthorized use of this computer and networking resources is prohibited…”
- ✓ Require Ctrl+Alt+Del for interactive logins.
- ✓ Configure a machine inactivity limit to protect idle interactive sessions.
- ✓ Ensure all volumes are using the NTFS file system.
- ✓ Configure Local File/folder permissions. Another important but often overlooked security procedure is to lock down the file-level permissions for the server. By default, Windows does not apply specific restrictions on any local files or folders; the Everyone group is given full permissions to most of the machine. Remove this group and instead grant access to files and folders using role-based groups based on the least-privilege principle. Every attempt should be made to remove Guest, Everyone and ANONYMOUS LOGON from the user rights lists. With this configuration Windows will be more secure.
- ✓ Set the system date/time and configure it to synchronize against domain time servers.
- ✓ Configure a screen saver to lock the console's screen automatically if it is left unattended.

Audit Policy Settings

- ✓ Enable Audit policy according to audit policy best practices. Windows audit policy defines what types of events are written in the Security logs of your Windows servers.
- ✓ Configure the Event Log retention method to overwrite as needed and size up to 4GB.
- ✓ Configure log shipping to SIEM for monitoring.

Software Security Guide

- ✓ Install and enable anti-virus software. Configure it to update daily.
- ✓ Install and enable anti-spyware software. Configure it to update daily.
- ✓ Install software to check the integrity of critical operating system files. Windows has a feature called Windows Resource Protection that automatically checks certain key files and replaces them if they become corrupted.

Finalization

- ✓ Make an image of each OS using GHOST or Clonezilla to simplify further Windows Server installation and hardening.
- ✓ Enter your Windows Server 2016/2012/2008/2003 license key.
- ✓ Enter the server into the domain and apply your domain group policies.

About Netwrix

Netwrix Corporation is a software company focused exclusively on providing IT security and operations teams with pervasive visibility into user behavior, system configurations and data sensitivity across hybrid IT infrastructures to protect data regardless of its location. Over 9,000 organizations worldwide rely on Netwrix to detect and proactively mitigate data security threats, pass compliance audits with less effort and expense, and increase the productivity of their IT teams.

Founded in 2006, Netwrix has earned more than 140 industry awards and been named to both the Inc. 5000 and Deloitte Technology Fast 500 lists of the fastest growing companies in the U.S.
For more information about Netwrix, visit www.netwrix.com.