ENTERPROTECT

# The Essential Guide to Hardening Windows Servers

ENTERPROTECT.COM

# Introduction

Microsoft Windows Servers have been the fundamental basis of small and large business networks since the early 2000s, and for many companies, servers are their lifeblood.

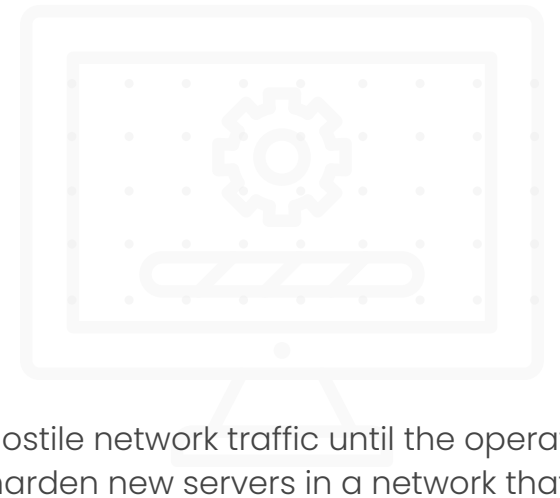
Servers are often the only entry point from the outside world. Workstations seldom require external ports to be open and commonly use local firewalls to block inbound traffic. The nature of a server is to serve, and therefore, the Server Firewall is often disabled or ports opened to allow necessary traffic. Whether you are running an in-house Exchange Server, Remote Desktop Server, File Server, Remote Management and Monitoring Server, or a Custom Application Server, you expose the server itself and your business to the risks of a vulnerability being exploited by attackers.

In 2017, EternalBlue, a computer exploit developed by the US National Security Agency (NSA), was leaked by the hacker group Shadow Brokers. Although Microsoft released a patch for the vulnerability, later that same year, the WannaCry Ransomware used the exploit to infect unpatched machines and using servers to push malware to entire organizations. The EternalBlue vulnerability was in the Windows RPC stack, and while RPC is not likely to be an open port on the public network, it is a port that is open to enable file sharing. This allowed attackers to gain access to the server by infecting one workstation on the local network. The attackers gained access to a workstation through various sources, including poor personal firewall management and a user opening a Microsoft Office document that contained malware.

Unfortunately, over the last five years, the EternalBlue exploit was not the only case where we have seen servers attacked. SolarWinds Orion, the Microsoft Exchange vulnerability, and Log4J are just a few other examples. IT and security professionals need to find ways to harden their servers without shutting down critical services. There is no silver bullet to stop a server from being compromised, but there are some steps you can take that will massively reduce the risk of your server being compromised.

At Enterprotect our aim is to keep your organization safe and secure with our unique approach to cybersecurity. We want to help you work smart and strengthen your cybersecurity from the ground up. In this guide, you'll find top tips and best practices to help you harden your Windows Servers and better protect your organization.

# Setup and Installation Hardening



- [ ] Protect new servers from potentially hostile network traffic until the operating system is fully hardened. Install and harden new servers in a network that is not open to the internet.
- [ ] Set a strong BIOS password to prevent unauthorized changes to the server's settings.
- [ ] Disable automatic administrative logon to the recovery console.
- [ ] Configure the device boot order to prevent unauthorized booting from alternate media.
- [ ] Create a system configuration based on the specific role that is needed. Ensure servers have the minimum features enabled and software installed to perform the required function.
- [ ] When you install Windows Server, immediately update it with the latest patches. Security patches resolve known vulnerabilities that attackers could otherwise exploit to compromise a system.

# User Account Hardening

- [ ] Disable and rename the guest account on each server.
- [ ] Disable and rename the local Administrator account on any machine that is part of a domain where uniquely named domain admin accounts will be used.
- [ ] Minimize access to privileged functions. Pay special attention to rights granted to built-in accounts and groups such as:
  - Local System (NT AUTHORITY\System)
  - Network Service (NT AUTHORITY\NetworkService)
  - Administrators group - Backup Operators group
  - Users group
  - Everyone group
- [ ] Ensure that passwords of system and administrator accounts meet password best practices.
- [ ] Configure account lockout Group Policy according to account lockout best practices.
- [ ] Do not allow “everyone” permissions to apply to anonymous users.
- [ ] Disallow anonymous enumeration of SAM accounts and shares.
- [ ] Disable anonymous SID/Name translation.
- [ ] Promptly disable or delete unused user accounts

# Network Configuration Hardening

- [ ] Enable the Windows firewall and make sure the Firewall is enabled for each of the Domain, Private and Public firewall Profiles.
- [ ] Configure the default behaviour of the Firewall for each Profile to block inbound traffic by default.
- [ ] Where inbound access is required to a server, restrict it to necessary protocols, ports and IP addresses.
- [ ] Perform port blocking at the network setting level. Perform an analysis to determine which network ports need to be open and restrict access to all other ports.
- [ ] Allow only Authenticated Users to access any computer from the network.
- [ ] 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, as a batch job, locally or via RDP.
- [ ] If RDP is used, 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.

# Network Configuration Hardening Continued

- [ ] Disable the sending of unencrypted passwords to third-party Server Message Block (SMB) servers.
- [ ] Do not allow any shares to be accessed anonymously.
- [ ] Set up the LAN Manager to refuse LM and NTLMv1 authentication.
- [ ] Allow Local System to use computer identity for NTLMv2 authentication.
- [ ] Disable Local System NULL session fallback.
- [ ] Configure allowable encryption types for Kerberos authentication.
- [ ] Do not store LAN Manager hash values.
- [ ] 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 keys. Many of the vulnerabilities in the Windows operating system can be mitigated by changing the following keys:

- [ ] 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 values in the NullSessionPipes key.
- [ ] Delete all values in the NullSessionShares key.

# General Security Settings

- [ ] Disable any unneeded services included in the default installation to reduce the server's vulnerability.
- [ ] Remove unnecessary Windows Server roles and features.
- [ ] Enable the built-in Encrypting File System (EFS) with NTFS or BitLocker.
- [ ] Disable the AUTORUN and AUTOPLAY Windows features
- [ ] 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, and configure an inactivity limit to terminate idle interactive sessions.
- [ ] Ensure all volumes are using the NTFS file system.
- [ ] Remove  Guest, Everyone and ANONYMOUS LOGON from local file and folder permissions.
- [ ] Set the system date/time and configure it to synchronize against domain time servers.
- [ ] Configure a local timeout policy that locks the server's screen automatically if it is left unattended.

# Audit Policy Configuration

- [ ] Create an audit policy according to audit policy best practices to define which events are written to the security logs to gain visibility into critical activity.
- [ ] Configure the event log retention method to overwrite as needed and make sure up to 4GB of storage is reserved.
- [ ] Leverage a tool like Enterprotect 360 to capture and analyze security events to improve threat detection and response.

# Additional Hardening Recommendations

- [ ] Promptly review, test and install recommended updates and patches for all operating system and applications to promptly patch vulnerabilities and improve application security
- [ ] Perform regularly vulnerability scans and promptly address any detected vulnerabilities.
- [ ] Follow the latest threat intelligence and proactively hunt for threats hiding in your servers.
- [ ] Use DNS & web filtering to block threats that originate online including command and control servers for malware such as ransomware.
- [ ] Install and enable anti-virus & anti-spyware software. Configure it to scan all downloads and attachments and to provide realtime protection. Set to update daily.
- [ ] Consider using application whitelisting technology to ensure that only authorized software executes, and all unauthorized software is blocked.
- [ ] Follow security best practices, as well as database hardening and application hardening guidance, for all your systems.

# Introducing
# ENTERPROTECT 360

## The Cybersecurity Platform for Busy IT Teams

Enterprotect 360 is an an all-in-one cybersecurity solution that provides powerful protection across your endpoints, network, and cloud - monitored 24/7 by security experts and integrated into a single, easy-to-use console.


**Protect Against Ransomware and Zero-day Threats**
Prevent, detect, and quickly respond to ever-changing cyberthreats with behavioral AI threat detection, automated remediation, and rollback.

**Improve Your Security Posture**
Proactively reduce your cyber risk by eliminating known vulnerabilities on your endpoints and network.

**Find and Eliminate Persistent Threats**
Catch hackers who are lurking in your environment while plotting their next attack.

**Add Cyber Experts to Your Arsenal**
24x7 monitoring of your networks, endpoints, and cloud environments to help you detect, respond, and recover from modern cyber attacks.

**Get Visibility Over Your Cybersecurity**
See all of your cybersecurity in one place, ensuring you always know exactly where your cybersecurity stands.

Learn more at: ENTERPROTECT.COM/360