

Web Server Security Hardening Windows 2000

This document is intended as a starting checklist to harden Windows 2000 Server and IIS for security vulnerabilities. This checklist is designed for those that are extremely familiar with Windows and IIS, as explanations for the checklist actions are not included. It is strongly recommend that you visit the Microsoft Security and Privacy page, at <http://www.microsoft.com/security/default.asp>, for specific information about each step and the reason behind each action.

- Install 2000 Server operating system
 - Install only options required
 - Specify machine is part of a Workgroup and not a domain
- Install latest OS service patches as recommended at <http://v4.windowsupdate.microsoft.com/en/default.asp>
 - Install all needed "critical updates"
 - Install all needed "Windows 2000 updates"
- Install latest Office updates as recommended at <http://office.microsoft.com/productupdates/>
- Run Microsoft Baseline Security Analyzer (MBSA) that can be found at <http://www.microsoft.com/technet/treeview/?url=/technet/security/tools/Tools/MBSAhome.asp>. Select the applicable type of server configuration. Note: This product will automatically set some of the setting below.
- Rename the "Everyone" Group to a different name
- Rename the "Administrator" account to a different name (do not use "admin")
- Run syskey.exe, select Encryption Enabled, then select Ok

Registry Changes

- HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\LegalNoticeCaption change value to include your company name or site owner
- HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\LegalNoticeText change value to "Unauthorized Use Prohibited by 18, U.S.C."
- Run drwtsn32 uncheck all options except Append to "Existing Log File"
- Delete HKLM\System\CurrentControlSet\Control\Session Managaer\SubSystems\OS2
- Delete HKLM\System\CurrentControlSet\Control\Session Managaer\SubSystems\Posix
- Delete HKLM\System\CurrentControlSet\Control\Session Managaer\SubSystems\Optional
- Delete HKLM\Software\Microsoft\RPC\ClientProtocols\ncacn_ip_tcp
- Delete HKLM\Software\Microsoft\RPC\ClientProtocols\ncagd_ip_upd

Control Panel Changes

Control Panel\System\Advanced\Startup and Recovery

- Set display list to 10 seconds.
- Check "Automatic Reboot"
- Set Write Debugging Information to "none"

Control Panel\ Administrative Tools\Local Security Policy\Account Policies\Password Policy\

- Enforce password history to 8
- Minimum password length to 8
- Maximum password age to 30

Control Panel\ Administrative Tools\Local Security Policy\Account Policies\Account Lockout Policy

- Account lockout duration to 10 minutes
- Account lockout threshold to 5
- Reset account lockout counter to 10 minutes

Control Panel\ Administrative Tools\Local Security Policy\Local Policies\Audit Policy

- Audit account logon events to Success, Failure
- Audit account management to Success, Failure
- Audit directory service access to Success, Failure
- Audit login events to Success, Failure
- Audit policy change to Success, Failure
- Audit privilege use to Success, Failure
- Audit process tracking to Success, Failure
- Audit system events to Success, Failure

Control Panel\ Administrative Tools\Local Security Policy\Local Policies\Security Options

- Allow System to Be Shut Down Without Having to Login On to Disabled
- Audit Use of Backup and Restore Privilege to Enabled
- Clear Virtual Memory Pagefile When System Shuts Down to Enabled
- Disable CTRL-ALT-DEL Requirements for Login to Disabled
- Do Not Display Last User Name in Login Screen to Enabled
- Message Text for Users Attempting to Log On to "Unauthorized use prohibited by 18, U.S.C"
- Message Title for Users Attempting to Log On to company or site owners name
- Prevent Users from Installing Printer Drivers to Enabled
- Recovery Console: Allow Automatic Administrative Login to Disabled
- Restrict CD-ROM Access to Locally Logged-On User to Enabled
- Restrict Floppy Access to Locally Logged-On user to Enabled
- Set Unsigned Driver Installation Behavior to Do not allow (NOTE: May prevent software installs)
- Unsigned Non-Driver Installation Behavior to Do no allow (NOTE: May prevent software installs)
- Additional restrictions for anonymous connections to No access without explicit anonymous permissions

Control Panel\Network and Dial-up Connections\<applicable connections>\Properties\General

- Deselect all components except "Internet Protocol (TCP/IP)"

Control Panel\Network and Dial-up Connections\<applicable connections>\Properties\General\, select Internet Protocol (TCP/IP), select Properties, select Advanced\Wins

- Disable NetBIOS over TCP/IP
- Disable LMHOSTS lookup

Control Panel\Network and Dial-up Connections\<applicable connections>\Properties\General\, select Internet Protocol (TCP/IP), select Properties, select Advanced\Options\TCP/IP filtering

- Use SiteRecon's Free Port Scanning page (<http://www.siterecon.com/PortScanning.aspx>) to scan for open ports
- Disable or filter all TCP, UDP, and IP ports as needed
- Use SiteRecon's Port Scanning again to verify that all unused ports are closed.

Control Panel\ Administrative Tools\Computer Management\Local Users and Groups\Users

- Guest account\General Tab\Cannot change password
- Guest account\General Tab>Password never expires
- Guest account\General Tab\Account disabled
- Guest account\Dial-in Tab\Remote Access Permission\Deny access

Services

Configure the following Windows Services to start automatically:

- DNS Client
- Logical Disk Manager
- Plug and Play
- Remote Registry Service
- Security Accounts Manager
- Event Log
- IPsec Policy Agent
- Protected Storage
- RunAs
- Task Scheduler

Configure the following Windows Services to start manually

- Application Management
- COM+ Event System
- Distributed Link Tracking Server
- File Replication
- Internet Connection Sharing
- Netmeeting Remote Desktop
- Network DDE
- NT LM Security Support Provider
- Qos RSVP
- Remote Access Connection Manager
- Smart Card
- Unit Power Supply
- Windows Installer
- ClipBook
- Logical Disk Manager Administrative Service
- Fax Service
- Indexing Service
- Net Logon
- Network Connections
- Network DDE DSDM
- Performance Logs and Alerts
- Remote Access Auto Connection Manager
- Remote Procedure Call (RPC) Locator
- Smart Card Helper
- Utility Manager
- Windows Management Instrumentation Driver Extensions

Disable the following Windows Services:

- Intersite Messaging
- Routing and Remote Access
- Print Spooler
- DHCP Client
- Telephony
- Windows Time
- Kerberos Key Distribution Center
- Terminal Services
- Simple Mail Transport Protocol (SMTP)
- Messenger
- Telnet

General Changes

For the Everyone Group that was renamed

- C Drive: Document and Settings folder rights: Read & Execute, List Folder Contents, Read
- C Drive: WinNT folder rights: none
- Web folder: Read & Execute, List Folder Contents, Read

Remove all rights for the Everyone group, that was renamed, from following c:\winnt\system32 files

- | | | |
|-------------------------------------|---------------------------------------|---------------------------------------|
| <input type="checkbox"/> arp.exe | <input type="checkbox"/> ipconfig.exe | <input type="checkbox"/> netstat.exe |
| <input type="checkbox"/> at.exe | <input type="checkbox"/> net.exe | <input type="checkbox"/> ping.exe |
| <input type="checkbox"/> cacls.exe | <input type="checkbox"/> nslookup.exe | <input type="checkbox"/> rdisk.exe |
| <input type="checkbox"/> cmd.exe | <input type="checkbox"/> posix.exe | <input type="checkbox"/> regedt32.exe |
| <input type="checkbox"/> debug.exe | <input type="checkbox"/> rcp.exe | <input type="checkbox"/> route.exe |
| <input type="checkbox"/> edit.com | <input type="checkbox"/> regedit.exe | <input type="checkbox"/> runone.exe |
| <input type="checkbox"/> edlin.exe | <input type="checkbox"/> rexec.exe | <input type="checkbox"/> syskey.exe |
| <input type="checkbox"/> finger.exe | <input type="checkbox"/> rsh.exe | <input type="checkbox"/> tracert.exe |
| <input type="checkbox"/> ftp.exe | <input type="checkbox"/> telnet.exe | <input type="checkbox"/> command.exe |
| <input type="checkbox"/> xcopy.exe | <input type="checkbox"/> nbtstat.exe | (And any others not needed) |

IIS

- Stop Administrative Web Site
- Stop Default SMTP Virtual Server
- Stop FTP Site if installed
- Delete the "iisstart.asp" in the WWWRoot directory
- Delete the "iissamples" folder under the "inetpub" directory
- Delete the "iisadmin" folder under the "inetpub" directory
- Delete the "iishelp", "iissadmin" and "iissamples" virtual directory for all current webs. NOTE: These directories should be deleted on any future webs also.

Display Properties

- Set screen saver to "Logon Screen Saver"
- Set screen saver to 5 minutes
- Check password protect

Install remote control program if desired

- Disable Guest account
- Uncheck Internet Locator services if an option

Install Firewall software

- Use SiteRecon's Free Port Scanning page (<http://www.siterecon.com/PortScanning.aspx>) to scan for open ports
- Disable or close all unnecessary ports
- Use SiteRecon's Port Scanning again to verify that all unused ports are closed.
- Be sure to grant access IP access to any machine that will be used to administer the server remotely

Install AntiVirus program

- Enable "start program on Windows startup" option
- Turn on all activity logs (detection, quarantine, etc)
- Disable "audible alert" option
- Check that "how to respond when a virus is found" is set for an automatic solution. (Norton for example uses the a default of "ask me what to do".)
- Enable scan of "master boot records"
- Enable scan of "boot records"
- Scan all inbound file types

Web Content

- Create directory for web content (do not use default web directory)
- Load content
- Set directory, and .NET if applicable, permissions
- Use SiteRecon's URL Comments page (<http://www.siterecon.com/URLComments.aspx>) to verify not inappropriate comments are embedded in your pages.

Vulnerability Scan

- Use a vulnerability scanner or scanning services to verify your site is secure and no vulnerability exist. A web search for the term "vulnerability scanner" will yield numerous companies to select from.

NOTE: Other security steps may be required based on you system, architecture, and specific needs!

Site and server security requires daily procedures to insure a proper defense. Security patched must be applied upon release, and the system and firewall logs need to be reviewed daily to track activity and intrusion attempts.

<http://www.SiteRecon.com>