Windows 2008R2 Server Hardening Checklist - ISO - Information Security Office - UT Austin Wikis ISO - Information Security Office / Information Security Office / Operating System Hardening Checklists Windows 2008R2 Server Hardening Checklist Added by twm, last edited by Jason M Ragland on Sep 22, 2011

The hardening checklists are based on the comprehensive checklists produced by CIS. The Information Security Office has distilled the CIS lists down to the most critical steps for your systems, with a particular focus on configuration issues that are unique to the computing environment at The University of Texas at Austin.

How to use the checklist

Print the checklist and check off each item you complete to ensure that you cover the critical steps for securing your server. The Information Security Office uses this checklist during risk assessments as part of the process to verify that servers are secure.

How to read the checklist

Step - The step number in the procedure. If there is a UT Note for this step, the note number corresponds to the step number. Check (V) - This is for administrators to check off when she/he completes this portion. To Do - Basic instructions on what to do to harden the respective system CIS - Reference number in the Center for Internet Security Windows Server 2008 Benchmark. The CIS document outlines in much greater detail how to complete each step. UT Note - The UT Note at the bottom of the page provides additional detail about the step for the university computing environment. Cat I - For systems that include Category-I data , required steps are denoted with the ! symbol. All steps are recommended. Cat II/III - For systems that include Category-II or - III data , all steps are recommended, and some are required (denoted by the

Min Std - This column links to the specific requirement for the university in the Minimum Security Standards for Systems document.

Server Information

MAC Address

IP Address

Machine Name

Asset Tag

Administrator Name

Date

Step

✓

To Do

CIS

Cat

Min Std

UT Note

Cat II Cat III

Preparation and Installation

5.1

a

If machine is a new install, protect it from hostile network traffic, until the operating system is installed and hardened.

https://wikis.utexas.edu/displayiSowindows+2008R2+Server+Hardening+Checklist

Consider using the Security Configuration Wizard to assist in hardening the host.

Service Packs and Hotfixes

Install the latest service packs and hotfixes from Microsoft.

5.2

Enable automatic notification of patch availability.

1.6.1

§

!

!

5.3

Auditing and Account Policies

Configure Audit policy as described.

1.2

6.1

Set minimum password length.

1.1.4

Enable Password Complexity.

1.1.5

Configure event Log Settings.

1.4

6.1

Security Settings

Disable anonymous SID/Name translation. (default)

1.9.6

10

1.9.37

5.5

Do not allow Anonymous Enumeration of SAM accounts (Default)

Do not allow Anonymous Enumeration of SAM accounts and shares.

1.9.38

5.5

12

Disable the guest account. (Default)

1.9.5

5.12

1.9.12

5.6

Digitally Encrypt or Sign Secure Channel Data (Always). (Default)

14

| 1.9.13

5.6

Digitally Encrypt Secure Channel Data (When Possible). (Default)

15

1.9.14

5.6

Digitally Sign Secure Channel Data (When Possible). (Default)

§

!

5.10

Place the University warning banner in the Message Text for Users Attempting to log on.

1.9.27- 28

1.9.32

5.6

Disable the sending of unencrypted password to connect to Third-Party

SMB Servers. (Default)

1.9.40

5.12

Do not allow Everyone permissions to apply to anonymous users. (Default)

19

Do not allow any named pipes to be accessed anonymously.

1.9.41

5.12

20

Restrict anonymous access to Named Pipes and Shares.

1.9.43

5.12

21

Ensure that no shares can be accessed anonymously.

1.9.44

5.12

22

1.9.45

5.12

Choose "Classic" as the sharing and security model for local accounts. (Default)

1.9.46

5.13

23

Do not store LAN Manager hash values

https://wikis.utexas.edu/displayISO/Windows+2008R2+Server+Hardening+Checklist

J-

.

24

Set LAN Manager Authentication level to NTLMv2 only

1.9.47

5.13

Additional Security Protection

25

Disable or uninstall unused services.

—

5.4

26

Disable or delete unused users.

5.4

— —

27

Configure User Rights to be as secure as possible.

1.81

28

Ensure all volumes are using the NTFS file system.

cos

—

29

1.5

—

5.5

Use the Internet Connection Firewall or other methods to limit connections to the server.

30

Configure file system permissions.

—

31

Configure registry permissions.

Additional Steps

Set the system date/time and configure it to synchronize against campus time servers.

33

Install and enable anti-virus software.

3.1

34

Install and enable anti-spyware software.

3.2

35

Configure anti-virus software to update daily.

3.3

36

Configure anti-spyware software to update daily.

3.3

37

Configure a screen-saver to lock the console's screen automatically if the host is left unattended.

38

4.1

If the machine is not physically secured against unauthorized tampering, set a BIOS/firmware password to prevent alterations in system startup

settings.

39

Configure the device boot order to prevent unauthorized booting from alternate media.

40

5.7

Systems will provide secure storage for Category-I data as required by confidentiality, integrity, and availability needs. Security can be provided by means such as, but not limited to, encryption, access controls, filesystem audits, physically securing the storage media, or any combination thereof as deemed appropriate.

5.8

Install software to check the integrity of critical operating system files.

42

If RDP is utilized, set RDP connection encryption level to high.

UT Note: Addendum

https://wikis.utexas.edu/displayISOWindows+2008R2+Server+Hardening+Checklist

11/14/13

Windows 2008R2 Server Hardening Checklist - ISO - Information Security Office - UT Austin Wikis This list provides specific tasks related to the computing environment at the University of Texas at Austin.

If other alternatives are unavailable, this can be accomplished by installing a SOHO router/firewall in between the network and the host to be protected.

The Security Configuration Wizard can greatly simplify the hardening of the server. Once the role for the host is defined, the SCW can help create a system configuration based specifically on that role. It does not completely get rid of the need to make other configuration changes, though. For more information, please see Security Configuration Wizard for Windows Server 2008

3

There are several methods available to assist you in applying patches in a timely fashion: Microsoft Update Service

• Microsoft Update checks your machine to identify missing patches and allows you to download and install them.

• This is different than the "Windows Update" that is the default on Windows 2008. Microsoft Update includes

updates for many more Microsoft products, such as Office and Forefront Client Security.

• This service is compatible with Internet Explorer only.

Windows AutoUpdate ITS offers a Windows Server Update Services Server for campus use using Microsoft's own update servers. It includes updates for additional Microsoft products, just like Microsoft Update, and provides additional administrative control for software deployment. Microsoft Baseline Security AnalyzerThis is a free host-based application that is available to download from Microsoft. In addition to detailing missing patches, this tool also performs checks on basic security settings and provides information on remediating any issues found.

Configure Automatic Updates from the Automatic Updates control panel

. On most servers, you should choose either "Download updates for me, but let me choose when to install them," or

"Notify me but don't automatically download or install them."

• The campus Windows Server Update Services server can be used as the source of automatic updates.

Configuring the minimum password length settings is important only if another method of ensuring compliance with university password standards is not in place.

7

Configuring the password complexity setting is important only if another method of ensuring compliance with university password standards is not in place.

The university requires the following event log settings instead of those recommended by the CIS Benchmark:

• Maximum application log size---50000 KB

• Maximum security log size--- 100000 KB

• Maximum system log size---50000 KB

• Prevent local guests group from accessing application log---enabled

• Prevent local guests group from accessing security log---enabled

• Prevent local guests group from accessing system log---enabled

• Retention method for application log---Overwrite events older than 14 days

• Retention method for security log---Overwrite events older that 14 days

• Retention method for system log---Overwrite events older than 14 days

These are minimum requirements. The most important log here is the security log. 100 MB is a suggested minimum, but if you have a high-volume service, make the file as large as necessary to make sure at least 14 days of security logs are available. You may increase the number of days that you keep, or you may set the log files to not overwrite events. Note that if the event log reaches its maximum size and no events older than the number of days you specified

 exist to be deleted or if you have disabled overwriting of events, no new events will be logged. This may happen deliberately as an attempt by an attacker to cover his tracks. For critical services working with Cat 1 or other sensitive data, you may wish to consider log shipping using syslog, Splunk, Intrust, or a similar service. Another option is to configure Windows to rotate event log files automatically when an event log reaches its maximum size as described in the article http://support.microsoft.com/kb/312571 using the the Auto BackupLogFiles registry entry.

16

The text of the university's official warning banner can be found on the ITS Web site. You may add localized information to the banner as long as the university banner is included.

27

Configure user rights to be as secure as possible. Every attempt should be made to remove Guest, Everyone, and ANONYMOUS LOGON from the user rights lists.

28

Volumes formatted as FAT or FAT32 can be converted to NTFS, by using the convert.exe utility provided by Microsoft. Microsoft has provided instructions on how to perform the conversion

This conversion cannot be reversed.

29

IPSec is one method that can limit connections to the server, and it is another standard method by which communication between servers can be encrypted. IPSec configuration can be managed using the IP Security Policies Snap-In. More information can be found on the Microsoft site.

30

Be extremely careful, as setting incorrect permissions on system files and folders can render a system unusable.

31

Be extremely careful, as setting incorrect permissions on registry entries can render a system unusable.

30

By default, domain members synchronize their time with domain controllers using Microsoft's Windows Time Service. The domain controller should be configured to synchronize its time with an external time source, such as the university's network time servers. ITS Networking operates two stratum 2 NTPV4 (NTP version 4) servers for network time synchronization services for university network administrators .

31

Download and install Microsoft Forefront Client Security from BevoWare.

32

Anti-spyware software is only required to be installed if the server is used to browse Web sites not specifically related to the administration of the server. ITS provides anti-spyware software for no additional charge. At a minimum, SpyBot Search and Destroy should be installed. We also recommend the installation of a secondary anti-spyware application, such as Spyware Blaster, EMS Free Surfer, or AdAware. Both SpyWare Blaster and EMS Free Surfer are available from BevoWare.

An additional measure that can be taken is to install ?Firefox with the ? NoScript and ?Adblock Plus add-ons

33

Microsoft Forefront can be configured directly or through the use of GPOS . GPOs can simplify the management of multiple servers.

34

Spyware Blaster — Enabling auto-update functionality requires the purchase of an additional subscription. SpyBot Search and Destroy--Automatic update tasks can be created inside the program itself and are scheduled using the Windows Task Scheduler.

1. In the Spybot Application, click on Mode-->Advanced View. 2. Click Settings on the left hand side of the window. 3. You should now see an option labeled "Scheduler." Select that option. 4. Adding the task to update automatically is relatively straightforward.

• Click Add to create a task.

• Click Edit to edit the task schedule.

• In the Scheduled Task window that pops up, enter the following in the Run field:

"C:\Program Files\Spybot - Search & Destroy\SpybotSD.exe" /AUTOUPDATE/TASKBARHIDE /AUTOCLOSE

• Click the Schedule tab and choose a time for it to update. The duration of the update is very brief, but it is

processor intensive, so consider scheduling it to occur during periods of low usage. The task should be scheduled daily.

37

1. Open the Display Properties control panel. 2. Select the Screen Saver tab. 3. Select a screen saver from the list. Although there are several available, consider using a simple one such as

"Blank." 4. The value for Wait should be no more than 30 minutes. 5. Select the On resume, password protect option.

40

Windows provides the Encrypting File System as a built-in mechanism to allow the encryption of individual users' files and folders. Be aware of the caveats involved in the use of EFS before implementing it for general use, though. Other options such as PGP , GNUPG, and TrueCrypt also exist. Another encryption option to consider is whole-disk encryption, which encrypts the entire contents of the drive instead of just specific files and folders. Windows Vista and Windows 2008 come with BitLocker for this. TrueCrypt can also do whole-disk encryption in addition to file-based encryption. ITS provides WinMagic SecureDoc which is recommended for encrypting laptops.

We strongly recommend that, if encryption is being used in conjunction with Category I data, one of the solutions listed in the Approved Encryption Methods (EID required) be implemented.

41

Windows Server 2008 has a feature called Windows Resource Protection which

automatically checks certain key files and replaces them if they become corrupted. It is enabled by default. You can audit in much more in depth using Tripwire. Modern versions of Tripwire require the purchase of licenses in order to use it. The Tripwire management console can be very helpful for managing more complex installations.

42

This setting is configured using the Terminal Services Configuration tool. On the General tab of the properties of the RDP connection, select High from the list next to encryption level.