# UNT CCDC WinServer2008/R2 Hardening Checklist

# Quick Checklist First Things ToDo

## Security

### Accounts

Rename administrator account - Rename to something unique (but remember it)

### Use Security Configuration Wizard

The Security Configuration Wizard can greatly simplify the hardening of the server. Once the role for the host is defined, the Security Configuration Wizard 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.

<https://technet.microsoft.com/en-us/library/cc754997.aspx>

GUI: Start->Administrative Tools->Security Configuration Wizard  
CMD: scwcmd

### Network security

LAN Manager authentication level - Send NTLMv2 response only\refuse NTLM & LM

Do not store LAN Manager hash value on next password change – Enabled

### Network access

Do not allow anonymous enumeration of SAM accounts and shares - Enabled

Do not allow anonymous enumeration of SAM accounts - Enabled

Allow anonymous SID/name translation – Disabled

### Interactive logon

Message text for users attempting to log on - sometimes an inject

## Audit

Audit process tracking - Successes

Audit account management - Successes, Failures

Audit logon events - Successes, Failures

Audit account logon events - Successes, Failures

### User Rights Assignment

Debug programs - Remove all groups/users

Allow log on through Terminal Services - Leave blank to disallow login via TS even if it has been started.

### Local GOPs

Export a config from a VM or other default install for reference:

secedit /export /cfg checkme.inf

Edit to to have more secure settings then import onto your target system:

secedit /configure /db secedit.sdb /cfg securecheckme.inf

# Complete Checklist

### Use Security Configuration Wizard

GUI: Start>Administrative Tools>Security Configuration Wizard  
CMD: scwcmd

### Updates

MS09-050

MS08-069

Download here

GUI: Start>Control Panel>System and Security>Check for updates

CMD: wusa [location of .msu] /quiet /norestart

https://support.microsoft.com/en-us/help/934307/description-of-the-windows-update-standalone-installer-in-windows

## Account Policies

Start->Run, gpedit.msc, click OK

Computer Configuration->Policies->Windows Settings->Security Settings->Account Policies->Password Policy

### Set minimum password length

Configuring the minimum password length settings is important only if another method of ensuring compliance with the Standard for Password s and Passphrases is not in place.

### Enable Password Complexity

Configuring the password complexity setting is important only if another method of ensuring compliance with Standard for Passwords and Passphrases is not in place

## Auditing

### Configure Audit policy

### Configure Event Log Settings

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 than 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 the logs are kept, 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 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 AutoBackupLogFiles registry entry.

## Security Settings

### Disable anonymous SID/Name translation (default)

### Do not allow Anonymous Enumeration of SAM accounts (Default)

### Do not allow Anonymous Enumeration of SAM accounts and shares

### Disable the guest account (Default)

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

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

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

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

### Disable the sending of unencrypted password to connect to Third-Party SMB Servers (Default)

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

### Do not allow any named pipes to be accessed anonymously

### Restrict anonymous access to Named Pipes and Shares

### Ensure that no shares can be accessed anonymously

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

### Do not store LAN Manager hash values

### Set LAN Manager Authentication level to NTLMv2 only

## Additional Security Protection

### Disable or uninstall unused services

### Disable or delete unused users

### Configure User Rights to be as secure as possible

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.

### Ensure all volumes are using the NTFS file system

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.

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

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.

### Configure file system permissions

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

### Configure registry permissions

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

unusable.

## Additional Steps

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

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. OIT operates <insert service here> for network time synchronization services for university network administrators.

### Install and enable antivirus software

Download and install Microsoft Forefront Client Security. Microsoft Forefront can be configured directly or through the use of Group Policy Objects (GPOs). GPOs can simplify the management of multiple servers.

### Install and enable anti-spyware software

Anti-spyware software is only required to be installed if the server is used to browse websites not specifically related to the administration of the server. 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.

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

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.

"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.

### Configure antivirus software to update daily

### Configure anti-spyware software to update daily

### Configure a screensaver to lock the console screen automatically if the host is left unattended

Open the Display Properties control panel.

Select the Screen Saver tab.

Select a screensaver from the list. Although there are several available, consider using a simple one such as "Blank."

The value for Wait should be no more than 30 minutes.

Select the On resume, password protect option.

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

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

### 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, file system audits, physically securing the storage media or any combination thereof as deemed appropriate

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 Standard for Data Encryption be implemented.

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

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 much more in depth using Tripwire. Modern versions of Tripwire require the purchase of a license. The Tripwire management console can be very helpful for managing more complex installations.

### If Remote Desktop Protocol (RDP) is utilized, set RDP connection encryption level to high

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.

### Ensure server has been added to the domain

### Ensure server resides in the correct Organizational Unit (OU)

## Resources

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