Windows Server 2012 Hardening Checklist

1. Preparation and Installation
   1. If machine is a new install, protect it from hostile network traffic, until the operating system is installed and hardened.
      1. 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.
   2. Consider using the Security Configuration Wizard to assist in hardening the host.
2. Update Windows
   1. Install the latest service packs and hotfixes from Microsoft.
      1. 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. More information is available at: [Security Configuration Wizard](https://technet.microsoft.com/en-us/library/cc754997.aspx).
   2. Enable automatic notification of patch availability.
      1. There are several methods available to assist you in applying patches in a timely fashion:
         1. Microsoft Update Service  
            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. Microsoft Update includes updates for many more Microsoft products, such as Office and Forefront Client Security. This service is compatible with Internet Explorer only.
         2. Microsoft Baseline Security Analyzer  
            This is a free host-based application that is [available to download from Microsoft](http://technet.microsoft.com/en-us/security/cc184923.aspx). In addition to detailing missing patches, this tool also performs checks on basic security settings and provides information on remediating any issues found.
3. User Policies
   1. Set Min Password Policies
      1. Click Start > Run, type gpedit.msc > click OK  
         Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies > Password Policy
      2. The option for disable "Password must meet complexity requirement" is dim and cannot be changed from enabled,
   2. Enable password complexity requirements.
   3. Do not store passwords using reversible encryption. (Default)
      1. If this option is enabled, the system will store passwords using a weak form of encryption that is susceptible to compromise. This configuration is disabled by default.
   4. Configure account lockout policy
      1. the account lockout policy should be configured as follows:
         1. Account lockout duration — 5 minutes
         2. Account lockout threshold — 5 failed attempts
         3. Reset account lockout counter — 5 minutes
4. User Rights Assignment
   1. Restrict the ability to access this computer from the network to Administrators and Authenticated Users.
   2. Do not grant any users the 'act as part of the operating system' right. (Default)
   3. Restrict local logon access to Administrators.
      1. Any account with this role is permitted to log in to the console. By default, this includes users in the Administrators, Users, and Backup Operators groups. It's unlikely that non-administrative users require this level of access and, in cases where the server is not physically secured, granting this right may facilitate a compromise of the device.
   4. Deny guest accounts the ability to logon as a service, a batch job, locally, or via RDP.
5. Security Settings
   1. Place warning banner in the Message Text for users attempting to log on.
   2. Disallow users from creating and logging in with Microsoft accounts.
      1. The use of Microsoft accounts can be blocked by configuring the group policy object at:  
         Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Block Microsoft accounts
      2. This setting can be verified by auditing the registry key:  
         HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\NoConnectedUser
   3. Disable the guest account. (Default)
   4. Require Ctrl+Alt+Del for interactive logins. (Default)
   5. Configure machine inactivity limit to protect idle interactive sessions.
   6. Configure Microsoft Network Client to always digitally sign communications.
   7. Configure Microsoft Network Client to digitally sign communications if server agrees. (Default)
   8. Disable the sending of unencrypted passwords to third party SMB servers.
   9. Configure Microsoft Network Server to always digitally sign communications.
   10. Configure Microsoft Network Server to always digitally sign communications.
6. Network Access Controls
   1. Disable anonymous SID/Name translation. (Default)
   2. Do not allow anonymous enumeration of SAM accounts. (Default)
   3. Do not allow anonymous enumeration of SAM accounts and shares.
   4. Do not allow Everyone permissions to apply to anonymous users. (Default)
   5. Do not allow any named pipes to be accessed anonymously.
   6. Restrict anonymous access to named pipes and shares. (Default)
   7. Do not allow any shares to be accessed anonymously.
   8. Require the "Classic" sharing and security model for local accounts. (Default)
7. Network Security Settings
   1. Allow Local System to use computer identity for NTLM.
   2. Disable Local System NULL session fallback. Configure allowable encryption types for Kerberos.
   3. Do not store LAN Manager hash values.
   4. Set LAN Manager authentication level to only allow NTLMv2 and refuse LM and NTLM.
   5. Enable the Windows Firewall in all profiles (domain, private, public). (Default)
   6. Configure the Windows Firewall in all profiles to block inbound traffic by default. (Default)
8. Active Directory Domain Member Security Settings
   1. Digitally encrypt or sign secure channel data (always). (Default)
   2. Digitally encrypt secure channel data (when possible). (Default)
   3. Digitally sign secure channel data (when possible). (Default)
   4. Require strong (Windows 2000 or later) session keys.
   5. Configure the number of previous logons to cache.
      1. Logon information for domain accounts can be cached locally to allow users who have previously authenticated to do so again even if a domain controller cannot be contacted. By default 10 accounts will be cached locally, but there is a risk that in the event of a compromise an attacker could locate the cached credentials and use a brute force attack to discover the passwords. Therefore, it is recommended that this value be reduced so that fewer credentials will be placed at risk, and credentials will be cached for shorter periods of time in the case of devices that are logged into frequently by multiple users.  
         The group policy object below should be set to 4 or fewer logons:  
         Computer Configuration\Windows Settings\Security Settings\Local Policies\ Security Options\Interactive logon: Number of previous logons to cache (in case domain controller is not available)
   6. Run Microsoft’s Domain Controller Diagnostics
      1. If the commands are unrecognized, install Windows Support Tools.
   7. Check your backups
      1. AD backup includes capturing system state, information related to AD database, logs, registry, boot files, SYSVOL and other system files.
   8. Check to make sure that AD replication is working correctly.
      1. To check, you can run the following command: repadmin /showrepl
   9. Allow only secure dynamic updates for all DNS zones.
      1. This ensures that only authenticated users can submit DNS updates using a secure method, which helps prevent the IP addresses of trusted hosts from being hijacked by an attacker.
      2. If the server running the DNS Server service is a domain controller, use AD ACLs to secure access control of the DNS Server service.
9. Audit Policy Settings
   1. Configure Account Logon audit policy.
      1. The Account Logon audit policy logs the results of validation tests of credentials submitted for user account logon requests. The server that is authoritative for the credentials must have this audit policy enabled. For domain member machines, this policy will only log events for local user accounts.   
         Configure the group policy object below to match the listed audit settings:  
         Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Logon\Credential Validation — Success and Failure
   2. Configure Account Management audit policy.
      1. Configure the group policy object below to match the listed audit settings:  
         Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Computer Account Management — Success and Failure  
         Other Account Management Events — Success and Failures  
         Security Group Management — Success and Failure  
         User Account Management — Success and Failure
   3. Configure Logon/Logoff audit policy.
      1. Configure the group policy object below to match the listed audit settings:  
         Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\  
         Account Lockout — Success  
         Logoff — Success  
         Logon — Success and Failure  
         Other Logon/Logoff Events — Success and Failure  
         Special Logon — Success
   4. Configure Policy Change audit policy.
      1. Configure the group policy object below to match the listed audit settings:  
         Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Policy Change\  
         Audit Policy Change — Success and Failure  
         Authentication Policy Change — Success
   5. Configure Privilege Use audit policy.
      1. Configure the group policy object below to match the listed audit settings:  
         Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Privilege Use\  
         Sensitive Privilege Use — Success and Failure
10. Event Log Settings
    1. Configure Event Log retention method and size.
       1. Application: Maximum log size — 32,768 KB  
          Security: Maximum log size — 196,608 KB  
          Setup: Maximum log size — 32,768 KB  
          System: Maximum log size — 32,768 KB
       2. The recommended retention method for all logs is: Overwrite events older than 14 days
       3. 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.
       4. 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 you should use syslog or a similar service to ship logs to another device.
       5. 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.
    2. Configure log shipping
       1. It is highly recommended that logs are shipped from any devices to a service, which provides log aggregation, processing, and real-time monitoring of events among many other things. This helps to ensure that logs are preserved and unaltered in the event of a compromise, in addition to allowing proactive log analysis of multiple devices.
11. Additional Security Protection
    1. Disable or uninstall unused services.
    2. Disable or delete unused users.
    3. Configure User Rights to be as secure as possible.
       1. 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.
    4. Ensure all volumes are using the NTFS file system.
       1. 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.](http://support.microsoft.com/kb/314097) Windows servers used with Category I data must use the NTFS file system for all partitions where Category I data is to be stored.
    5. Configure file system permissions.
       1. Be extremely careful, as setting incorrect permissions on system files and folders can render a system unusable.
    6. Configure registry permissions.
       1. Be extremely careful, as setting incorrect permissions on registry entries can render a system unusable.
    7. Disallow remote registry access if not required.
       1. Some remote administration tools, such as Microsoft Systems Management Server, require remote registry access to managed devices. Disabling remote registry access may cause such services to fail. If remote registry access is not required, it is recommended that the remote registry service be stopped and disabled.
       2. If remote registry access is required, the remotely accessible registry paths should still be configured to be as restrictive as possible. The group policy object below controls which registry paths are available remotely:  
          Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Remotely accessible registry paths
       3. This object should be set to allow access only to:  
          System\CurrentControlSet\Control\ProductOptions  
          System\CurrentControlSet\Control\Server Applications  
          Software\Microsoft\Windows NT\CurrentVersion
       4. Further restrictions on the registry paths and subpaths that are remotely accessible can be configured with the group policy object:  
          Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Remotely accessible registry paths and sub-paths
12. Additional Steps
    1. Set the system date/time and configure it to synchronize against campus time servers.
       1. By default, domain members synchronize their time with domain controllers using Microsoft's [Windows Time Service](http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03mngd/26_s3wts.mspx). The domain controller should be configured to synchronize its time with an external time source, such as the university's network time servers.
    2. Install and enable anti-virus software.
    3. Install and enable anti-spyware software.
       1. 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, which is not recommended.
       2. 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](http://www.utexas.edu/its/bevoware/download).
       3. An additional measure that can be taken is to install [Firefox](http://www.mozilla.com/en-US/firefox/personal.html) with the [NoScript](https://addons.mozilla.org/en-US/firefox/addon/722/) and [uBlock](https://addons.mozilla.org/en-us/firefox/addon/ublock/) add-ons.
    4. Configure anti-virus software to update daily.
       1. Microsoft Forefront may also be used, and can be [configured directly](http://www.utexas.edu/its/help/anti-virus-software/456)or through the use of GPOs, which can simplify the management of multiple servers.
    5. Configure anti-spyware software to update daily.
       1. SpyBot Search and Destroy - Automatic update tasks can be created inside the program itself and are scheduled using the Windows Task Scheduler.
       2. In the Spybot Application, click on Mode --> Advanced View.
       3. Click Settings on the left hand side of the window.
       4. You should now see an option labeled "Scheduler." Select that option.
       5. Adding the task to update automatically is relatively straightforward.
       6. Click Add to create a task.
       7. Click Edit to edit the task schedule.
       8. In the Scheduled Task window that pops up, enter the following In the Run field:
       9. C:\Program Files\Spybot - Search & Destroy\SpybotSD.exe" /AUTOUPDATE /TASKBARHIDE /AUTOCLOSE
       10. 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.
    6. 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.
       1. 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](http://www.pgp.com/) and [GNUPG](http://www.gnupg.org/) also exist.
       2. 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 comes with BitLocker for this.
    7. Install software to check the integrity of critical operating system files.
       1. Windows 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.
    8. If RDP is utilized, set RDP connection encryption level to high.
       1. This setting is configured by group policy object at:
       2. \Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security
       3. This policy object should be configured as below:
       4. Set client connection encryption level — High
       5. Require use of specific security layer for remote (RDP) connections — SSL (TLS 1.0)
       6. Require user authentication for remote connections by using Network Level Authentication — Enabled
13. Physical Security
    1. Set a BIOS/firmware password to prevent alterations in system start up settings.
    2. Disable automatic administrative logon to recovery console.
    3. Do not allow the system to be shut down without having to log on. (Default)
    4. Configure the device boot order to prevent unauthorized booting from alternate media.
    5. Configure a screen-saver to lock the console's screen automatically if the host is left unattended.
       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 15 minutes.
       5. Select the On resume, password protect option.