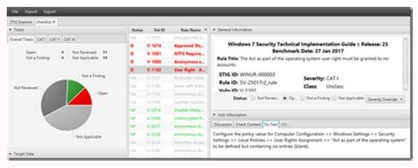
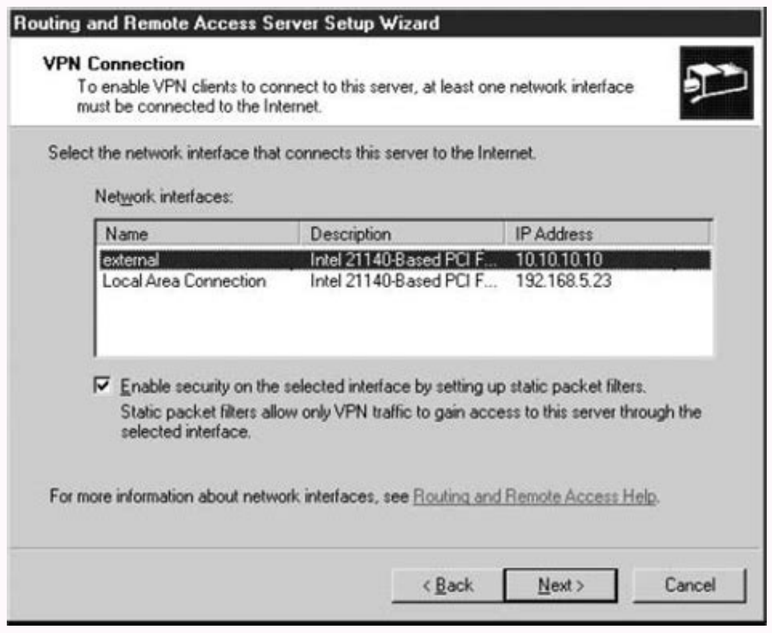
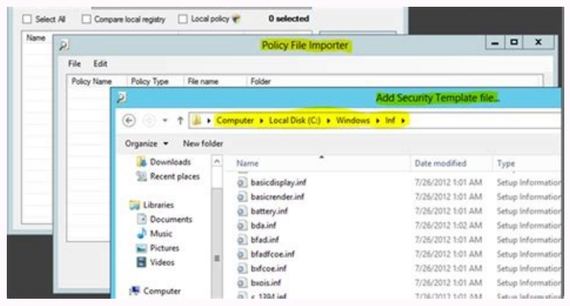
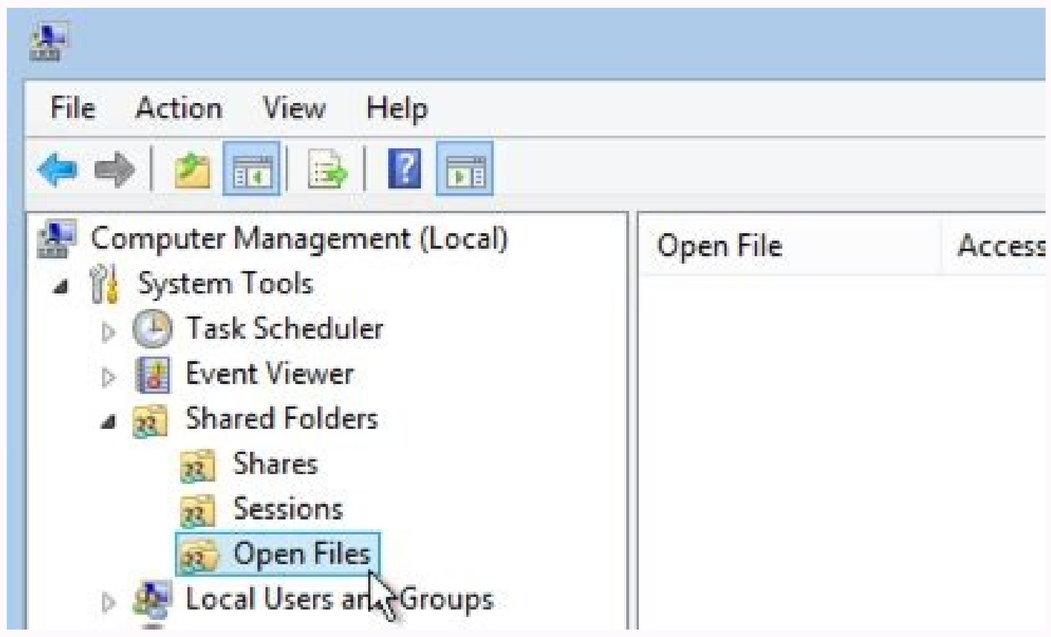
Hardening guide windows server 2012 r2









Windows server 2012 r2 hardening guide. Windows server 2012 r2 hardening guide pdf.

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 (√) - 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 systemCIS - Reference number in the Center for Internet Security Windows Server 2012 R2 Benchmark v1.1.0. 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 Server Information MAC Address IP Address Machine Name Asset Tag Administrator Name Date Checklist Checklist Step √ To Do MFD UT Note Cat I Cat II/III Min Std Preparation and Installation 1 If machine is a new install, protect it from hostile network traffic, until the operating system is installed and hardened. § ! ! 4.5.1 2 Consider using the Security Configuration Wizard to assist in hardening the host. § Service Packs and Hotfixes 3 Install the latest service packs and hotfixes from Microsoft. § ! ! 4.5.2 4 Enable automatic notification of patch availability. § ! ! 4.5.5 User Account Policies 5 Set minimum password length. 1.1.4 § ! ! 6 Enable password complexity requirements. 1.1.5 § ! 7 Do not store passwords using reversible encryption. (Default) 1.1.6 § ! ! 8 Configure account lockout policy. 1.2 § ! ! User Rights Assignment 9 Restrict the ability to access this computer from the network to Administrators and Authenticated Users. 2.2.2 10 Do not grant any users the 'act as part of the operating system' right. (Default) 2.2.3 ! ! 11 Restrict local logon access to Administrators. 2.2.6 § 12 Deny guest accounts the ability to logon as a service, a batch job, locally, or via RDP. 2.2.18-21 ! Security Settings 13 Place the University warning banner in the Message Text for users attempting to log on. 2.3.7.4 § ! ! 4.5.10 14 Disallow users from creating and logging in with Microsoft accounts. 2.3.1.1 § ! ! 15 Disable the guest account. (Default) 2.3.1.2 ! ! 16 Require Ctrl+Alt+Del for interactive logins. (Default) 2.3.7.2 ! ! 17 Configure machine inactivity limit to protect idle interactive sessions. 2.3.7.3 ! ! 18 Configure Microsoft Network Client to always digitally sign communications. 2.3.8.1 ! 19 Configure Microsoft Network Client to digitally sign communications if server agrees. (Default) 2.3.8.2 ! ! 20 Disable the sending of unencrypted passwords to third party SMB servers. 2.3.8.3 ! ! 4.5.6 21 Configure Microsoft Network Server to always digitally sign communications. 2.3.9.2 ! 22 Configure Microsoft Network Server to digitally sign communications if client agrees. 2.3.9.3 ! Network Access Controls 23 Disable anonymous SID/Name translation. (Default) 2.3.11.1 ! ! 24 Do not allow anonymous enumeration of SAM accounts. (Default) 2.3.11.2 ! ! 4.5.5 25 Do not allow anonymous enumeration of SAM accounts and shares. 2.3.11.3 ! 4.5.5 26 Do not allow everyone permissions to apply to anonymous users. (Default) 2.3.11.4 ! ! 4.5.12 27 Do not allow any named pipes to be accessed anonymously. 2.3.11.5 ! 4.5.12 28 Restrict anonymous access to named pipes and shares. (Default) 2.3.11.8 ! ! 4.5.12 29 Do not allow any shares to be accessed anonymously. 2.3.11.9 ! 30 Require the "Classic" sharing and security model for local accounts. (Default) 2.3.11.10 ! ! 4.5.12 Network Security Settings 31 Allow Local System to use computer identity for NTLM. 2.3.12.1 32 Disable Local System NULL session fallback. 2.3.12.2 33 Configure allowable encryption types for Kerberos. 2.3.12.4 34 Do not store LAN Manager hash values. 2.3.12.5 ! ! 4.5.13 35 Set LAN Manager authentication level to only allow NTLMv2 and refuse LM and NTLM. 2.3.12.7 ! 4.5.13 36 Enable the Windows Firewall in all profiles (domain, private, public). (Default) 9.{{1-3}}.1 ! ! 4.5.5 37 Configure the Windows Firewall in all profiles to block inbound traffic by default. (Default) 9.{{1-3}}.2 ! ! Active Directory Domain Member Security Settings 38 Digitally encrypt or sign secure channel data (always). (Default) 2.3.6.1 ! 4.5.6 39 Digitally encrypt secure channel data (when possible). (Default) 2.3.6.2 ! ! 4.5.6 40 Digitally sign secure channel data (when possible). (Default) 2.3.6.3 ! ! 4.5.6 41 Require strong (Windows 2000 or later) session keys. 2.3.6.6 ! 42 Configure the number of previous logons to cache. 2.3.7.6 § Audit Policy Settings 43 Configure Account Logon audit policy. 17.1 § ! 44 Configure Account Management audit policy. 17.2 § ! ! 45 Configure Logon/Logoff audit policy. 17.5 § ! ! 46 Configure Policy Change audit policy. 17.7 § ! ! 47 Configure Privilege Use audit policy. 17.8 § ! Event Log Settings 48 Configure Event Log retention method and size. 18.7.19 § ! ! 4.6.1 49 Configure log shipping (e.g. to Splunk). § Additional Security Protection 50 Disable or uninstall unused services. ! 51 Disable or delete unused users. ! 52 Configure user rights to be as secure as possible. § ! 53 Ensure all volumes are using the NTFS file system. § ! 54 Configure file system permissions. § ! 55 Configure registry permissions. § ! 56 Disallow remote registry access if not required. 2.3.11.6 § Additional Steps 57 Set the system date/time and configure it to synchronize against campus time servers. § ! 58 Install and enable anti-virus software. § ! ! 59 Install and enable anti-spyware software. § ! 60 Configure anti-virus software to update daily. § ! ! 61 Configure anti-spyware software to update daily. § ! 62 Provide secure storage for Confidential (category-I) Data as required. 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. § ! 63 Install software to check the integrity of critical operating system files. § ! 64 If RDP is utilized, set RDP connection encryption level to high. Make sure to restrict RDP access to local VPNgroup and local campus management subnets. Do not allow RDP to be available to the Internet at large. § ! Physical Security 65 Set a BIOS/firmware password to prevent alterations in system start up settings. 4.4.1 66 Disable automatic administrative logon to recovery console. 2.3.13.1 ! 67 Do not allow the system to be shut down without having to log on. (Default) 2.3.14.1 ! ! 68 Configure the device boot order to prevent unauthorized booting from alternate media. ! 4.4.1 69 Configure a screen-saver to lock the console's screen automatically if the host is left unattended. § ! ! UT Note: Addendum This list provides specific tasks related to the computing environment at The University of Texas at Austin. UT Note: Addendum 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 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. 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. 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 via WSUS 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 Analyzer This 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. 4 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. 5 Configuring the minimum password length settings is important only if another method of ensuring compliance with university password standards is not in place. The Information Resources Use and Security Policy requires passwords be a minimum of 8 characters in length. It is strongly recommended that passwords be at least 14 characters in length (which is also the recommendation of CIS). Longer passwords (e.g., more than 20 characters) offer much more protection (entropy) in the event a password hash is obtained and an attacker is attempting to crack it. 6 Configuring the password complexity setting is important only if another method of ensuring compliance with university password standards is not in place. The Information Resources Use and Security Policy requires that passwords contain letters, numbers, and special characters. 7 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. 8 Instead of the CIS recommended values, the account lockout policy should be configured as follows: Account lockout duration — 5 minutes Account lockout threshold — 5 failed attempts Reset account lockout counter — 5 minutes 11 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. 13 The text of the university's official warning banner can be found on the ISO's web site. You may add localized information to the banner as long as the university banner is included. 14 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 This setting can be verified by auditing the registry key: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\NoConnectedUser 42 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 logins: 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) 43 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 44 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 45 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 46 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 47 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 48 The university requires the following event log settings instead of those recommended by the CIS Benchmark: 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 The recommended retention method for all logs is: 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 should use Syslog, Splunk, Intrust, or a similar service to ship logs to another device. 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 using the AutoBackupLogFiles registry entry. 49 It is highly recommended that logs are shipped from any Category I devices to a service like Splunk, 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. The ISO maintains a centrally-managed Splunk service that may be leveraged. Please see the on-boarding form for more details. 52 Configure user rights to be as secure as possible, following the recommendations in section 2.2 of the CIS benchmark. Every attempt should be made to remove Guest, Everyone, and ANONYMOUS LOGON from the user rights lists. 53 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. Windows servers used with Category I data must use the NTFS file system for all partitions where Category I data is to be stored. 54 Be extremely careful, as setting incorrect permissions on system files and folders can render a system unusable. 55 Be extremely careful, as setting incorrect permissions on registry entries can render a system unusable. 56 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. 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 This object should be set to allow access only to: System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server Applications Software\Microsoft\Windows NT\CurrentVersion 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 57 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. 58 ISO provides Cisco AMP, a managed, cloud-based malware protection service, free of charge for all university-owned devices. More information about obtaining and using AMP is at . 59 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. At a minimum, SpyBot Search and Destroy should be installed. Consider installing 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 uBlock add-ons. 60 Cisco AMP is the recommended anti-virus solution. Microsoft Forefront may also be used, and can be configured directly or through the use of GPOs, which can simplify the management of multiple servers. 61 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. In the Spybot Application, click on Mode --> Advanced View. Click Settings on the left hand side of the window. You should now see an option labeled "Scheduler." Select that option. 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. 62 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 and GNUPG 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 comes with BitLocker for this. If encryption is being used in conjunction with Category I data, one of the solutions listed in the Approved Encryption Methods (EID required) must be implemented. 63 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. 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. 64 This setting is configured by group policy object at: \Computer Configuration\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security This policy object should be configured as below: Set client connection encryption level — High Require use of specific security layer for remote (RDP) connections — SSL (TLS 1.0) Require user authentication for remote connections by using Network Level Authentication — Enabled 69 Open the Display Properties control panel. Select the Screen Saver tab. Select a screen saver 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 15 minutes. Select the On resume, password protect option.