FINCSIRT

# Windows Server Hardening Guide

*v. 1.0*

# *Contents*

# *Introduction*

*This manual is based on the CIS Benchmark and it is a derived version which address the must have security controls which the servers need to be implemented with and hardened. This guide covers the Windows Server 2012 R2 which is the latest version of Windows. FINCSIRT recommends that you always use the latest OS and the security patches to stay current on security.*

# *Server Hardening Policy*

*FINCSIRT highly recommend that the organization have a minimum security standard hardening policy and to that, this guide can be attached as an annexure. Purpose of the policy will be to make sure any server that is deployed and going to be deployed to be properly hardened and maintain a baseline security standard while uplifting the internal information security resiliency against rapidly advancing threats.*

# 1. Installation

## 1.1. Protect the installation until system is hardened

*The operating system should be protected from hostile network traffic until such time the system is installed and hardened.*

*Microsoft Windows Server 2012 R2*

- *Installation of the server should be separated from the network or in an isolated network.*
- *Only Verified media should be used during the installation. (Windows Installation KIT, Drivers)*
- *Additional needed drivers should only be downloaded via official download locations.*
- *Downloaded files should be verify for the integrity via given file hashes.*
- *Downloaded drivers should be scanned via an updated virus guard prior to installations.*
- *Drivers should only be copied to the installation via a clean media dedicated for the installation.*
- *All file systems should be either NTFS or any other security supported file system.*
- *Minimum number of required services should only be installed at the installation.*
- *Anti-malware systems/Firewalls should be installed/configured at the earliest.*

## 1.2. Harden the server

*The operating system should be hardened at the earliest prior connecting it to the cooperate network.*

*Microsoft Windows Server 2012 R2*

- *Security Configuration Wizard developed by Microsoft can be used for the initial security configurations. (https://technet.microsoft.com/en-us/library/cc754997.aspx)*

## 1.3. Installation of latest sevice packs and hotfixes

*After completing the security hardening, the server can be connected to the internet in order to get the latest service packs and hotfixes from the Microsoft Update servers.*

*Microsoft Windows Server 2012 R2*

- *The server can be connected to internet and allowed Microsoft URLs to get the latest updates.*
- *The server should be placed behind a firewall that blocks all incoming sessions during the update period.*

## 1.4. Enable automatic notification of patch availibility.

*Configure Automatic Updates from the Automatic Updates control panel*

*Microsoft Windows Server 2012 R2*

- *According the organizational policy, you can 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."*
- *Having a local Windows Server Update Services server is recommended as it will reduce the burden of the network and the client servers won't be needed to connect directly to get the windows updates.*

## 1.5. Server should be properly placed within the cooperate network

*The server should be properly placed within the cooperate network according to the service requirements.*

*Microsoft Windows Server 2012 R2*

- *A server used for testing or under deployment is not a production server. Hence should not be directly accessible via general network segments (Public or internal).*
- *These servers should always be placed within a physically/logically separated network until such time the server is moved to production level.*
- *Development servers should not contain applications with legitimate data. Only dummy data should be used while the system moves to production level.*

## 1.6. Set proper filesystem permissions

*File systems permissions should be reviewed and enabled on required basis. Each data folder should only be allowed to personals who has required clearance levels to access that information.*

*Microsoft Windows Server 2012 R2*

- *This can be easily achieved using proper user groups.*
- *Read, Write permission should be separately considered and should be given accordingly.*

## 1.7. Set network time protocol

*Using a single time and date source is extremely important to co-relate events and*

*Microsoft Windows Server 2012 R2*

- *All servers should be properly synchronized with a Network Time Protocol ( NTP) Server.*
- *This is recommended to be a local server*

## 1.8. Malware Protection

*Maintenance of proper malware protection is in utmost important task for a secure windows environment.*

*Microsoft Windows Server 2012 R2*

- *Malware protections should include anti-virus, anti-spyware applications.*
- *As a cooperate environment, centrally managed malware protection is recommended as it will allow proper maintenance of policy and have much granular control over the endpoints*

## 1.9. File Intergrity monitoring

*Integrity of critical operating system files and application configuration files should be monitored and verified against the change management requests of the organization.*

*Microsoft Windows Server 2012 R2*

- *A third party application stack should be used for this purpose as windows natively does not support for non-system file integrity monitoring.*
- *For available options, you should contact your security consultant/FINCSIRT.*

## 2. User Account Policies

### 2.1. Set Minimum password length

*Types of password attacks include dictionary attacks (which attempt to use common words and phrases) and brute force attacks (which try every possible combination of characters). Also, attackers sometimes try to obtain the account database so they can use tools to discover the accounts and passwords. The recommended state for this setting is: 14 or more character(s). But this value varies according to your organizational policy.*

*Microsoft Windows Server 2012 R2*

- *To establish the recommended configuration via Group Policy, set the following UI path to 14 or more character(s):*
- ***"Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\ Password Policy\Minimum password length"***

### 2.2. Enable password complexity requirements.

*Passwords that contain only alphanumeric characters are extremely easy to discover with several publicly available tools.*

*Microsoft Windows Server 2012 R2*

- *To establish the recommended configuration via Group Policy, set the following UI path to Enabled:*
- ***"Computer Configuration\Policies\Windows Settings\Security Settings\AccountPolicies \Password Policy\Password must meet complexity requirements"***

### 2.3. Ensure 'Store passwords using reversible encryption' is set to 'Disabled'.

*Enabling this policy setting allows the operating system to store passwords in a weaker format that is much more susceptible to compromise and weakens your system security*

*Microsoft Windows Server 2012 R2*

- *To establish the recommended configuration via Group Policy, set the following UI path to Disabled:*
- ***"Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\ Password Policy\Store passwords using reversible encryption"***

## 2.4. Deploy a propoer account lockout policy.

*Having a proper account lockout policy is important as it will be helpful to protect against a bruteforce or a password guessing attack*

*Microsoft Windows Server 2012 R2*

- *To establish the recommended configuration via Group Policy, set the following values*
- *Account lockout duration: Value - 15 or more minute.*
    - ***"Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\ Password Policy\Store passwords using reversible encryption"***
- *Account lockout threshold: Value - 10 or fewer invalid logon attempt(s), but not 0.*
    - ***"Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Account lockout threshold "***
- *Reset account lockout counter after: Value - 15 or more minute(s).*
    - ***"Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Reset account lockout counter after "***

## 2.5. Disable or delete unused users.

*Existence of unused or unnecessary user accounts is always a risk to be exploited. Therefore, it is highly recommended to disable to remove any kind of user account that does not have a required purpose.*

*Microsoft Windows Server 2012 R2*

- *The management console and the user account management snap-in can be used to manage local users and groups.*

## 3. User Rights Assignment

### *3.1.* Ensure 'Act as part of the operating system' is set to 'No One'

*The Act as part of the operating system user right is extremely powerful. Anyone with this user right can take complete control of the computer and erase evidence of their activities. The recommended state for this setting is: No One.*

*Microsoft Windows Server 2012 R2*

- *To establish the recommended configuration via Group Policy, set the following UI path to No One:*
  - ***"Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Act as part of the operating system"***

### 3.2. Set who can log on locally to the systems

*This determines who can login to the system via direct consoles (By Pressing CTRL + ALT + DEL, Through Remote Desktop etc…. This user right should generally be restricted to the Administrators groups. Assign this user right to the Backup Operators group if your organization requires that they have this capability*

*Microsoft Windows Server 2012 R2*

- *To establish the recommended configuration via Group Policy, configure the following UI path*
  - ***"Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Allow log on locally"***

### 3.3. Set who can log on using Remote Desktop

*This determines which users or groups have the right to log on as a Terminal Services client. Remote desktop users require this user right. If your organization uses Remote Assistance as part of its help desk strategy, create a group and assign it this user right through Group Policy. If the help desk in your organization does not use Remote Assistance, assign this user right only to the Administrators group or use the restricted groups feature to ensure that no user accounts are part of the Remote Desktop Users group.*

*Microsoft Windows Server 2012 R2*

- *To establish the recommended configuration via Group Policy, configure the following UI path*
  - ***"Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Allow log on through Remote Desktop Services"***

# 4. General Hardening

## 4.1. Security Banners when login in.

*Displaying a warning message before logon may help prevent an attack by warning the attacker about the consequences of their misconduct before it happens. It may also help to reinforce corporate policy by notifying employees of the appropriate policy during the logon process..*

*Microsoft Windows Server 2012 R2*

- *To establish the recommended configuration via Group Policy, configure the following registry path*
  - ***"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System: LegalNoticeCaption"***

## 4.2. Ensure 'Accounts: Guest account status' is set to 'Disabled'

*Set the system flag to force randomized virtual memory region placement. Randomly placing virtual memory regions will make it difficult for to write memory page exploits as the memory placement will be consistently shifting.*

*Microsoft Windows Server 2012 R2*

- *To establish the recommended configuration via GP, set the following UI path to Disabled :*
  - ***"Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Guest account status"***

## 4.3. Ensure 'Microsoft network client: Send unencrypted password to third-party SMB servers is set to 'Disabled'

*It is recommended that you disable this policy setting unless there is a strong business case to enable it. If this policy setting is enabled, unencrypted passwords will be allowed across the network.*

*Microsoft Windows Server 2012 R2*

- *To establish the recommended configuration via GP, set the following UI path to Disabled :*
  - ***"Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network client: Send unencrypted password to third-party SMB servers"***

## 5. Network Access Control and Network Security

### 5.1. Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled'

*This policy setting determines what additional permissions are assigned for anonymous connections to the computer.*

*Microsoft Windows Server 2012 R2*

- *To establish the recommended configuration via Group Policy, set the following UI path to Disabled :*
  - ***"Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Let Everyone permissions apply to anonymous users"***

### 5.2. Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None'

*It is very dangerous to allow any values in this setting. Any shares that are listed can be accessed by any network user, which could lead to the exposure or corruption of sensitive data.*

*Microsoft Windows Server 2012 R2*

- *To establish the recommended configuration via GP, set the following UI path to <blank>*
  - ***"Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Shares that can be accessed anonymously"***

### 5.3. Ensure 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled'

*NULL sessions are less secure because by definition they are unauthenticated.*

*Microsoft Windows Server 2012 R2*

- *To establish the recommended configuration via Group Policy, set the following UI path to Disabled :*
  - ***"Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Allow LocalSystem NULL session fallback"***

### *5.4.* Enable the Windows (or Thirdparty) Firewall

*Enable the windows firewall or any relevant firewall to all the profiles of the server (Domain, Private , Public )*

*Microsoft Windows Server 2012 R2*

- *Ensure 'Windows Firewall: Domain Profile: Firewall state' is set to 'On*
    - ***Domain Profile: Inbound – Block***

      ***Outbound – Allow***
- *Ensure 'Windows Firewall: Private Profile: Firewall state' is set to 'On*
    - ***Private Profile: Inbound – Block***

      ***Outbound – Allow***
- *Ensure 'Windows Firewall: Public Profile: Firewall state' is set to 'On*
    - ***Public Profile: Inbound – Block***

      ***Outbound – Allow***

***** Ensure that minimum required services are exposed to outside in every profile.***

# 6. Audit Policy Settings

## 6.1. Enable required Windows Audit policies

*Following Audit policies should be enabled so that they can be used in an incident to further investigate.*

*Microsoft Windows Server 2012 R2*

- *Account Logon audit policy where successful and login failures are audited: To establish the recommended configuration via Group Policy, set the following UI path to Success and Failure:*
  - ***"Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Logon\Audit Credential Validation"***
- *Application Group Management audit policy where group related activities such as group add, remove are audited: To establish the recommended configuration via Group Policy, set the following UI path to Success and Failure:*
  - ***"Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Application Group Management"***
- *Audit Computer Account Management audit policy where account related activities such as Computer account add, remove are audited: To establish the recommended configuration via Group Policy, set the following UI path to Success and Failure:*
  - ***"Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Computer Account Management"***
- *Security Group Management audit policy where group related activities such as group add, remove are audited: To establish the recommended configuration via Group Policy, set the following UI path to Success and Failure:*
  - ***Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Distribution Group Management***
  - ***Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Security Group Management***

- *User account management audit policy where group related activities such as user add, remove are audited: To establish the recommended configuration via Group Policy, set the following UI path to Success and Failure:*
    - ***Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit User Account Management***
- *Audit account lockout policy where a user's account is locked out as a result of too many failed logon attempts: To establish the recommended configuration via Group Policy, set the following UI path to Success*
    - ***Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Account Lockout***
- *Audit audit policy change where it reports changes in audit policy. To establish the recommended configuration via Group Policy, set the following UI path to Success and Failure*
    - ***Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Policy Change\Audit Audit Policy Change***
- *Audit Sensitive Privilege Use policy where reports when a user account or service uses a sensitive privilege. To establish the recommended configuration via Group Policy, set the following UI path to Success and Failure.*
    - ***Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Privilege Use\Audit Sensitive Privilege Use***

# 7. Event Logs Configuration

## *7.1.* Event Log retention size

*This policy setting specifies the maximum size of the log file in kilobytes. The maximum log file size can be configured between 1 megabyte (1,024 kilobytes) and 2 terabytes (2,147,483,647 kilobytes) in kilobyte increments. The recommended state for this setting is: Enabled: 32,768 or greater.*

*Microsoft Windows Server 2012 R2*

- *To establish the recommended configuration via Group Policy, set the following UI path to Enabled: 32,768 or greater :*
    - ***Computer Configuration\Policies\Administrative Templates\Windows Components \Event Log Service\Application\Specify the maximum log file size (KB)***

# 8. Physical Security

## 8.1. Set Physical System Configurations

*System should be protected against alterations of physical system configurations*

*Please refer to the original support document of the system for guides to achieve the following recommendations.*

- *Set a BIOS/Firmware password to prevent alterations in system startup settings*
- *Disable automatic administrative login to recovery console*
- *Do not allow the system to be shut down without having to log on*
- *Configure the device boot order to prevent unauthorized booting from alternate media.*
- *Configure a screen-saver to lock the console's screen automatically if the host is left unattended.*