

# System Hardening Outline – Windows 10, Server 2016

Last Updated on 11-12-2020

## Readme

- THE README IS YOUR ABSOLUTE AUTHORITY! IT SAYS ANYTHING AND EVERYTHING. IF SOMETHING ON THIS CHECKLIST GOES AGAINST THE README, DON'T DO IT!

## General notes:

- NOTE: Microsoft changes where different tools are in the GUI from time to time. It can therefore be useful to memorize or have a list of shortcut names, accessible from the run menu (Win + R):
  - a. E.g. `mmc.exe` snap-ins, `secpol.msc`, `lusrmgr.msc`, `control update`, and `control firewall.cpl` among others. Don't forget to check out mmc snap-ins! See the following URL for other examples: <https://sid-500.com/2019/06/18/top-10-built-in-mmc-consoles-msc-and-control-panel-files-cpl-in-windows-10-and-windows-server/>
- NOTE: For Windows 10 and Server may have different GUIs, which is yet another reason to know how to navigate via MMC snap-ins and Run menu shortcuts
- Write down:
  - a. Any changes that you make that AWARD you points in case you need to restart from scratch, and/or to refer to these papers in future rounds.
  - b. Any changes that you make that DEDUCT points, so you know what not to do in future rounds.
- Make note of any files associated with questions and answer them as soon as you find the answer.
- Do not irreversibly modify accounts, files, or folders until you've answered as many Readme questions as possible. You could be removing something that's an answer to a question!
- NEVER REMOVE the CyberPatriot Scoring Engine.
- Don't lock yourself out of your administrative account by forgetting your password, or misconfiguring security policies
- Windows Defender is generally good enough so you don't have to worry about using third party AVs, but you can scan your system with an active-antivirus such as Avast or Malwarebytes if desired, or otherwise uncertain what to do next

## Forensics Questions:

- ACTION:
  1. Find a file or directory without clear guidance (think word-problem)
  2. Determine the permissions of a file or directory (which accounts have what level(s) of access?)
  3. Determine the hash (unique identifier) of a file
- 1. METHOD: Win + R > powershell or Win + R > cmd
  - o Use a command to iterate recursively through the Users directory to list all contents, removing the necessity to search each directory individually, place the output of that command into a text file for easy searching
  - o E.g. `tree /f /a C:\Users\ >> C:\Users\users_folder_contents.txt`
- 2. METHOD: See File/Folder Permissions section
- 3. METHOD: Win + R > powershell
  - o `Get-FileHash <FILEPATH AND NAME HERE> -Algorithm <MD5, SHA1, or others>`
  - o E.g. `Get-FileHash C:\Users\batman\Desktop\batcave_location.txt -Algorithm MD5`

## User Accounts:

- ACTION: Bring all accounts into compliance with 1) Readme and 2) Security best-practices
  - o SEE: Local Security Policy section
  - o Make sure that all given passwords are secure/meet the requirements
  - o Make sure all user accounts are in their respective groups/permissions
  - o Disable all unauthorized accounts
  - o Disable guest account unless otherwise specified in readme
- METHOD: Control Panel > User Accounts and Family Safety > User Accounts

# System Hardening Outline – Windows 10, Server 2016

- METHOD: Control Panel > System and Security > Administrative Tools > Computer Management
- METHOD: Open Run dialogue (⌘ + r):
  - Run command: `lusrmgr.msc`
  - Run command: `gpedit`

## File/Folder Permissions:

- ACTION: Ensure that file permissions for all accounts comply with 1) any Readme direction and 2) Security best-practices. E.g. a user should not typically have access to other users' files within `C:\Users\`
- METHOD: Go to a file or directory (⌘ + E) and open a context menu (`right click`) > Properties > Security > Edit
  - NOTE: Specific permissions override group permissions, such as giving all standard users read only but then specifically one user can edit

## Background Tasks:



- ACTION: Apply all system updates, except for FEATURE updates.
  - For update types, see: <https://www.windowscentral.com/whats-difference-between-quality-updates-and-feature-updates-windows-10>
- METHOD: Control Panel > System and Security > Windows Update
  - Download updates in background
  - Will update the service pack, but might have to update more than once to get the points Control Panel > System and Security > Action Center

## Quick and Easy Tasks:

- ACTION: Enable Automatic Updates
  - METHOD: Control Panel > System and Security > Windows Update
- ACTION: Turn on Windows Firewall/use recommended settings
  - METHOD: Control Panel > System and Security > Windows Firewall
- ACTION: Bring advanced firewall settings into compliance with Readme
  - METHOD: ⌘ + r > `wf.msc` > block and/or allow any ports associated with prohibited/allowed programs in Readme
  - E.g. If FTP is disallowed, you could block all incoming and outgoing traffic on ports 20 and 21
  - Reference a [Common Ports](https://packetlife.net/library/cheat-sheets/) cheat sheet such as the one located at <https://packetlife.net/library/cheat-sheets/>

# System Hardening Outline – Windows 10, Server 2016

- ACTION: Unless otherwise stated in the Readme, disable these commonly found services and any others found that may be malicious

- METHOD:  + r > services.msc
- METHOD:  + r > msconfig > Services tab
- METHOD: Ctrl + Shift + Esc > Services tab

Microsoft FTP Service

Print Spooler

Remote Desktop Configuration

Remote Desktop Services

Remote Desktop Services UserMode

Remote Registry

RIP Listener Server

SNMP Trap

SSDP Discovery


Telephony

Telnet

UPnP Device Host

TCP/IP NetBIOS Helper

## Local Security Policy

- Control Panel > System and Security > Administrative Tools > Local Security Policy
-  + r > gpedit.msc > Computer Configuration > Windows Settings > Security Settings > Local Policies
- Account Policies

- Password Policy

3 passwords remembered	30 mins account lockout duration
30-90 days maximum password age	5 invalid logon attempts threshold
10 days minimum password age	30 mins reset account lockout counter

- 8-12 minimum password length
- Enable complexity requirements
- Disable reversible encryption
- Account Lockout Policy
- Local Policies
  - Audit Policy
    - ❖ Enable all audit policies (success, failure)
- Security Options – Note: Some Security Options will give points, others may not. Enable/Disable them, write down which award or detract points. The following are the most critical out of the security options. However, be sure to read all of them (click on Explain), not just the following and see what setting would be the most secure setting. - do if you still need points at the end
  - Accounts: Administrator account status - **Disable**
  - Accounts: Guest account status - **Disable**
  - Accounts: Limit local account use of blank passwords... - **Enable**
  - Devices: Restrict CD-Rom access to locally logged-on user... - **Enable**
  - Devices: Restrict Floppy access to locally logged-on user... - **Enable**
  - Domain Member: LDAP server signing requirements - **Enable**
  - Domain Member: Digitally encrypt or sign secure channel data (always) - **Enable**
  - Interactive Logon: Do not display last user name - **Enable**
  - Interactive Logon: Do not require CTRL + ALT + DEL - **Disable**
  - Microsoft Network Client: Digitally sign communications (always) - **Enable**
  - Microsoft Network Client: Send unencrypted password to third-party SMB Server - **Disable**
  - Microsoft network server: Digitally sign communications (always) - **Enable**
  - Network Access: Allow anonymous SID/Name translation - **Disable**
  - Network Access: Do not allow anonymous enumeration of SAM accounts and shares - **Enable**
  - Network Access: Let Everyone permissions apply to anonymous user - **Disable**

# System Hardening Outline – Windows 10, Server 2016



## Windows Features:

- ACTION::
- METHOD: Navigate to Control Panel > Programs > Turn Windows features on or off > and disable the following features:
  - Active Directory Services (Be careful with this one, especially Windows Server versions)
  - Internet Information Services
  - Media Features
  - Print and Document Services
  - RIP Listener
  - Simple TCP/IP
  - SMB
  - Telnet
  - Work Folders

## Remove Malicious/Unwanted Software

- Navigate to Control Panel > Programs > Programs and Features
- Check all programs and remove any that may seem fishy
- Remove programs that are not listed on the Readme file, other than
  - Files to keep(for sure):
    - CyberPatriot Scoring Engine
    - Microsoft .Net Framework
    - Microsoft Visual C++
    - Vmware tools
    - Note: not all programs will be listed here, also check C:\ProgramFiles\ and C:\ProgramFiles(x86)
    - CHECK APPDATA as well for hidden malware/files

## Miscellaneous Items:

- Update web-browsers
- Using previously generated text file, search User directories for “non-work related” media files
- Check if there are any folders/files being shared on the network
- Update any programs that should be on the OS
- Check Event Viewer ( + r > eventvwr.msc) and Task Scheduler ( + r > taskschd.msc) in Administrative Tools