ULTIMATE CYBERPATRIOT WINDOWS CHECKLIST

Read the read me file (CRITICAL!!!! This will give you your directions for each CyberPatriot Challenge!!!! Follow it with STRICT guidance)

Make sure to empty the recycle bin

Make sure to turn Firewall back on. It sometimes gets turned off.

Make sure to install anti virus and then update it twice before running it.

Make sure to remove all media and pictures and games not explicitly asked to be kept.

|  |  |
| --- | --- |
|  |  |
| secpol.msc  ⊞+r -> type “secpol.msc” | Account Policy  Password Policy  Enforce password history: **24**  Maximum password age: **30**  Minimum password age: **3**  Minimum password length: **14**  Password must meet complexity requirements: **Enabled**  Store passwords using reversible encryption: **Disabled**  Account Lockout Policy  Account lockout duration: **30**  Account lockout threshold: **5**  Reset account lockout counter: **30**  Local Policies  Audit Policy  Set everything to **Success, Failure**  User Rights Assignment  Check for anything that looks out of place (for instance, nothing should “Act as part of the operating system.” Record anything you remove.  Security Options  Accounts:  Administrator account status: **Disabled**  Guest account status: **Disabled**  Limit local account use of blank passwords to console only: **Enabled**  Limit local use of blank passwords to console only: **Enabled**  Devices:  Allow undock without having to log on: **Disabled**  Restrict CD-ROM / Floppy access to locally logged-on user only: **Enabled**  Interactive Login:  Display user information when the session is locked: **Do not display user information**  Do not require CTRL+ALT+DEL: **Disabled**  Don’t display last signed-in: **Enabled**  MS Network Server:  Digitally sign communications (always): **ENABLED**  MS network client:  Digitally sign communications (always): **Disabled**  -Network Access:  Allow anonymous SID/Name translation: **Disabled**  Do not allow anonymous enumeration of SAM accounts: **Enabled**  Do not allow anonymous enumeration of SAM accounts and shares: **Enabled**  Do not allow storage of passwords and credentials for network authentication: **ENABLED**  Let Everyone permissions apply to anonymous users: **Disabled**  Restrict anonymous access to Named Pipes and Shares: **Enabled**  -Network Security:  Do not store LAN Manager hash value on next password change: **Enabled**  -Recovery Console:  Allow automatic admin logon: **Disabled**  Allow floppy copy and access to all drives and all folders: **Disabled**  -Shutdown:  Allow system to be shut down without having to logon: **Disabled**  -User Account Control:  Admin Approval Mode for Built-in Administrator account: **Enabled**  User Account Control: Switch to the secure desktop when prompting for elevation: **ENABLED**  Behavior of the elevation prompt for standard users automatically: **Deny**  Run all administrators in Admin Approval Mode: **Enabled**  **\*\* Refer to** [**this doc**](https://docs.google.com/document/d/1KSACVeVT4qtK7S-LbtBv20HtrO_AiDVlIwdgzWrcA84/edit?usp=sharing) **for a complete list of all configurations**  \*\* It is unlikely any changes will need to be made to **Network List Manager Policies, Public Key Policies, Software Restriction Policies, Application Control Policies, or IP Security Policies on Local Computer** unless stated otherwise  -Advanced Audit Policy Configuration  Set everything to **Success, Failure** (leave Global Object Access Auditing alone)  \*\* Account Logon |
| lusrmgr.msc  ⊞+r -> type “lusrmgr.msc” | -Users  **\*\* Document any changes you make here** **and refer to the readme**  -Disable the guest account   * + Users -> right click “Guest” -> Properties -> check “Account is disabled”   -Remove any unauthorized users   * + Users -> right click [User] -> Delete   -Add new users   * + Users -> More Actions -> New User -> add applicable settings   -Make changes to user properties   * + Users -> right click [User] -> Properties     - Check “User must change password at next logon” (except for the admin account)     - Uncheck “User cannot change password”     - Uncheck “Password never expires”     - Uncheck “Account is disabled” (unless it’s the Guest account or the account needs to be disabled)     - Uncheck “Account is locked out”   Assign passwords to all users   * + Users -> right click [User] -> Set Password     - Make sure password meets complexity requirements       * Example: PP@@ssword12345   -Groups  **\*\* Document any changes you make here and refer to the readme**  Remove unauthorized users from admin group/other groups they shouldn’t be a part of   * + Groups -> right click [Group] -> Properties -> Select [User] -> Remove   Create groups (as specified)   * Groups -> More Actions -> New Group -> add applicable settings   Add users to groups (as specified)   * Groups -> right click [Group] -> Properties -> Add -> enter [User]   Remove any unnecessary groups   * Groups -> right click [Group] -> Delete   **\*\* Do not delete any of the default groups!** |
| fsmgmt.msc  ⊞+r -> type “fsmgmt.msc” | -Shares:   * Unshare any folders besides the mandatory folders:   + **ADMIN$**   + **C$**   + **IPC$**   (Any required folder shares will have a $ sign at the end)  -Sessions:   * Disconnect All Sessions from the top left corner of the Shared Folders Directory. |
| services  ⊞ -> type “services” | -Service  Stop and disable unnecessary services  **\*\* Be sure to check the readme for any critical services. Do not disable or stop DNS Client, Server, or any other vital services.**   * + Services -> Double click a service to edit properties -> Stop service and choose disabled * Common services to disable: * RDP, ICS, RDP UserMode, RD Configuration, UPnP Device Host, Remote Desktop, WWW Publishing Service, Telnet, FTP, RIP Listener, RPC Locator, SNMP Trap, Bitlocker, Remote Registry, UPnP, SSDP Discovery   + Full list of services [here](https://docs.google.com/document/d/1MXdBDpV1CBHZOZZQfJWhzqRaz9wJ_wCJQC0byBDB3mY/edit?usp=sharing) (wip)   Services are running   * Services -> Double click a service to edit properties -> Start service and choose Automatic   + Make sure services specified in the readme are running (ex. Windows Event Log, Windows Update, etc)   -Windows Features  In Windows 10:   * + Control Panel -> Programs -> Turn Windows features on or off -> uncheck to remove or check to install   In Server 2019:   * + Server Manager -> Manage -> Remove Roles and Features -> Next -> Next ->     - uncheck Server Roles -> Remove     - uncheck Features -> Remove * Common Features to remove:   + FTP, Simple TCP/IP Services, Telnet, SMB 1.x |
| remote desktop  ⊞+r -> type “sysdm.cpl” | Remote Desktop  **\*\* Be sure to check the readme if remote desktop is a critical service.**   * System Properties -> Remote -> Remote Assistance ->uncheck "Allow Remote Assistance connections to this computer" AND select "Don't allow connections to this computer" |
| task manager | Task Manager  Disable unwanted startup services   * Task Manager -> Startup -> Disable |
| task scheduler | Task Scheduler  Remove unwanted scheduled tasks   * Find task in Active Tasks -> Double click [task] -> Delete |
| powershell  ⊞ -> search “powershell” and run as administrator | Update Powershell   * Check current version of Powershell (the latest version is 5.1)   + Type “$PSVersionTable.PSVersion”     - Refer [here](http://woshub.com/install-update-powershell-windows/) for further instruction       * You may install PowerShell Core 7, but this is a separate platform entirely. Instructions found in the same link |
| screensaver  ⊞ -> type “screensaver” | Screensaver  Enable screensaver and require password for logging back on (Control Panel -> Hardware and Sound -> Power Options)   * Enable “On resume, display logon screen” |
| UAC  ⊞ -> type “control panel” | User Account Control settings  Control Panel -> User Accounts -> User Accounts -> Change User Account Control Settings   * Set as high as possible (Always notify) |
| AutoPlay  ⊞ + i | AutoPlay has been disabled   * Settings -> Devices -> AutoPlay -> Use AutoPlay for all media and devices **Off** |
| firewall and ports  ⊞ -> type “firewall” | Turn on Firewall   * Control Panel -> System and Security -> Windows Defender Firewall -> Use Suggested Settings   Windows Defender Firewall with Advanced Security   * gpedit.msc -> Computer Configuration -> Windows Settings -> Security Settings -> Windows Defender Firewall with Advanced Security -> Windows Defender Firewall Properties   Domain Profile  Firewall state: **On**  Inbound connections: **Block (default)**  Outbound connections: **Allow (default)**  Settings  Display a notification: **No**  Logging  Size limit (KB): **16384 KB or greater**  Log dropped packets: **Yes**  Log successful connections: **Yes**  Private Profile  Firewall state: **On**  Inbound connections: **Block (default)**  Outbound connections: **Allow (default)**  Settings  Display a notification: **No**  Logging  Size limit (KB): **16384 KB or greater**  Log dropped packets: **Yes**  Log successful connections: **Yes**  Public Profile  Firewall state: **On**  Inbound connections: **Block (default)**  Outbound connections: **Allow (default)**  Settings  Display a notification: **No**  Apply local connection security rules: **No**  Logging  Size limit (KB): **16384 KB or greater**  Log dropped packets: **Yes**  Log successful connections: **Yes**  Close ports through Firewall   * Control Panel -> System and Security -> Windows Firewall -> Advanced Settings   + Specify ports to block     - Inbound Rules -> New Rule -> Port -> List [ports you wish to block](https://docs.google.com/document/u/0/d/1TC7pMeOv6BrXj_kiFRFRZ2qEUGEcaK7bof54bBlwYMA/edit) under “Specific local ports” -> Block the connection -> Apply rule to all sections (should be all by default; if not, check them all) -> Name rule -> Finish     - Block FTP, SSH, TelNet, SNMP, LDAP, RDP, etc. |
| updates/  programs  ⊞ -> type “update” | Windows Updates  Update Windows   * Update Settings -> Update & Security -> Check for updates   \*\* Never save this for the last minute—updates can take a long time!  Turn on Automatic Updates  \*\* If Automatic Windows Updates are disabled:   * gpedit.msc -> Administrative Templates -> Windows Components -> Windows Update -> Configure Automatic Updates -> **Enabled**   Uninstall Unnecessary Programs (Control Panel)   * Common programs to remove:   + WireShark, Nmap, uTorrent, Netcat * Any video game or launcher unless listed in the readme * Find in Program Files (check file timestamps) or check Downloads for any zip files   Update Necessary Programs   * Update Firefox and any other programs specified in the readme (such as Notepad++)   + If you’re unable to update a program, instead uninstall it and reinstall the latest version |
| browser settings | Firefox  Update Firefox   * + Menu icon -> Options -> General -> Check for Updates     - Enable Automatic Updates       * check “Automatically install updates (recommended)”   Enable pop-up blocker   * + Menu icon -> Options -> Content -> Make sure "Block pop-up windows" is checked     - Also check “Warn you when websites try to install add-ons”   Block dangerous resources   * + Menu icon -> Options -> Privacy & Security -> Check “Block dangerous and deceptive content”, “Block dangerous downloads”, “Warn you about unwanted and uncommon software”   Remove Add-ons   * Menu icon -> Options -> Extensions & Themes -> Extensions -> Manage Your Extensions   Autoplay   * + Menu icon -> Options -> Privacy & Security -> Autoplay (Settings) -> Block Audio and Video   \*\* Can also block any other requests under Permissions  Internet Explorer  Update Internet Explorer   * Check what version of Internet Explorer is installed (most recent is Internet Explorer 11)   + Internet Explorer updates should be downloaded with system updates. You can install Internet Explorer if needed under “Turn Windows features on or off” in Control Panel   Enable pop-up blocker   * + Tools -> Pop-up Blocker -> Turn On Pop-up Blocker   Disable Flash and Unauthorized toolbars   * + Tools -> Manage Add-ons -> Show: All add-ons -> Right-click Flash -> Disable * Disable anything else that may be suspicious * Refer [here](https://docs.google.com/document/d/1G3cHpc1T6368qsPUOwNTWaLovvYP1We6T51rtqgWKt8/edit?usp=sharing) (Windows Components -> Internet Explorer) |
| media files | Delete any prohibited media files (.png, .jpg, .gif, .mov, .mp4, .mp3, etc.)  \*\* Note that sometimes files used in the forensics questions (not the forensics question files themselves) may need to be removed. **Only remote them after you have gotten the points associated with that file.**   * Search in command line using \*.<file extension>   + (ex. dir /s \*.txt) * Manually search through folders for specific file types (usually found in user folders)   + Turn on see hidden files |
| malware & windows security  ⊞ -> type “windows security” | Malware  Remove detected malware threats   * Install and run one or more of the following:   + WinRar, Malware Bytes, Microsoft Safety Scanner, Malicious Software Removal Tool.     - You can also use Windows Defender by going Settings -> Update & Security -> Windows Security -> Virus & threat protection   Windows Security  Windows Smartscreen configured to warn or block   * Windows Security -> App & browser control -> SmartScreen for Microsoft Edge/Microsoft Store apps -> select “Warn” or “Block” |
| gpedit.msc  ⊞ +r -> type “gpedit.msc”  [additional settings](https://docs.google.com/document/d/1G3cHpc1T6368qsPUOwNTWaLovvYP1We6T51rtqgWKt8/edit?usp=sharing) | Local Group Policy Editor  Check for any pre-configured settings   * gpedit.msc -> Administrative Templates -> All Settings -> Sort by “State”   + Adjust changed settings accordingly   Require secure RPC communication   * gpedit.msc -> Administrative Templates -> Windows Components -> Remote Desktop Services -> Remote Desktop Session Host -> Require secure RPC communication **Enabled**   RDP connection encryption level has been set to high   * gpedit.msc -> Administrative Templates -> Windows Components -> Remote Desktop Services -> Remote Desktop Session Host -> Set client connection * encryption level **Enabled** -> Encryption Level **High Level**   Make sure everyone gets your policy by using: gpupdate /force |
| Registry Editor  ⊞ +r -> “regedit” | Disable IPv6   * Control Panel -> Network and Internet -> Network Connections -> Change adapter settings -> Right click connection -> Properties -> Uncheck “Internet Protocol Version 6 (TCP/IPv6)”   OR   * Registry Editor -> HKEY\_LOCAL\_MACHINE -> System -> CurrentControlSet -> Services -> Tcpip6 -> Parameters -> DisabledComponents   + To establish the recommended configuration, set the following Registry value to 0xff (255) (DWORD) |
| server specific vulns |  |
|  | Run software like: MS Baseline, etc.  Run commands like: Netstat, nmap, etc. |
| Clean the Host File | C:\Windows\System32\drivers\etc\host.txt |
| Configure a message text for users who are logging on. | Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options.  Interactive logon: Message title for users attempting to log on  Add Message Title, Add Message Text |
| Restrict Printer Drivers | Group Policy  Computer Configuration > Administrative Templates > Printers  Devices: Prevent users from installing printer drivers |
| Sharing | CMD > net share  More details > net share <shareName> |
| Check Scheduled Tasks | PowerShell > schtasks /query  Or Windows + R > control schedtasks |