

# Cyberpatriot Categorized Checklist

## USER ACCOUNT PERMISSIONS

- Go to Control Panel and click on User Accounts (or User Accounts and Family Safety)
- Turn the User Account Control on
- Select the Use User Account Control (UAC) check box to turn on UAC (all submitted by Heinkel)
- Make sure only users listed on the README file are present on the computer. If not delete other users. (Beau Curnow)
- Make sure only users listed on the README file as administrators actually have administrator setting. Set all other users to standard. (Beau Curnow)
- Disable Guest account. (Beau Curnow)
- Make sure only files are on (word processing, web browsing, etc.) are present. Remove any programs that are not stated on README. Setup Software policies. (Beau Curnow)
- Use Applocker. <http://www.howtogeek.com/howto/6317/block-users-from-using-certain-applications-with-applocker/>

## USER ACCOUNT AND PASSWORD

- Determine authorized user accounts from Readme file.
- Go to User Account.
- Delete any unauthorized accounts.
- Determine if all user accounts are password-protected. Determine if there is a password strength requirement.
- Create strong passwords for the accounts that aren't password-protected
- Check the user profiles for hacking tools such as Netcat, Metasploit, and any password cracking tools.
- (<http://www.techrepublic.com/blog/five-apps/five-trustworthy-password-recovery-tools/1411>) (All submitted by Chloe) (LCP, Ophcrack, Windows Key, Windows Password Unlocker, and Hash Suite are the 5 most common). (Added by Charlie Walker)
- Delete Guest Accounts. (Thomas Polk)

## UNNECESSARY SERVICES / APPLICATIONS

Start > Search box > pe services.msc > Click on Services

- Disable: (If something doesn't work right, re-enable the service)

- Media Center Extender service
- adobeLM service
- alerter
- Application management
- Automatic updates
- Clip book
- Cryptographic Services
- Distributed transaction services
- DNS Client
- Error Reporting service
- Net.Tcp Port Sharing Service
- Remote Desktop Configuration
- Remote Desktop Services
- Remote Desktop Services UserMode Port Redirector
- Remote Procedure Call (RPC) Locator
- SeaPort
- SSDP Discovery
- TCP/IP Net BIOS Helper
- UPnP Device History (all submitted by Heinkel)
- Telnet (Beau Curnow)
- ISS (Beau Curnow)
- Universal Plug and Play Device Host (Beau Curnow)
- DNS (Beau Curnow)
- Uninstall any server software present on the computer. (VNC, APACHE, ETC.)(Start -> Control Panel -> Programs -> Uninstall programs -> Click Programs needed to uninstall) (Beau Curnow)
- Uninstall any freeware such as CCleaner, etc. (Submitted by Chloe)

## **MALWARE**


- Install MSE, AVG, McAfee and r\virus / malware is discovered make sure the program stops the malware and deletes it. MSE: <http://windows.microsoft.com/en-US/windows/security-essentials-download> (Submitted by Chloe)
  - AVG: <http://free.avg.com/us-en/free-antivirus-download> (Submitted by Chloe)
  - McAfee: <http://home.mcafee.com/downloads/free-virus-scan?ctst=1> (Submitted by Chloe)
- Here's another free antivirus scanner using Cloud service:
  - Panda Cloud Antivirus <http://www.cloudantivirus.com/en/#!/free-antivirus-download>
- Search for backdoor software using system search bar and delete backdoor. Double check to make sure it isn't located in any other parts of the system. (Beau Curnow)
- Make sure no keylogger software is located in services.
  - Find keylogger file and determine location in services.
  - Right click on service stop, disable, and look at location of file.

- Go to location of file and check for extensions, outsourcing, and folders.
- Delete completely from system. (Delete from recycle bin.) (All by Beau Curnow)
- Make Sure Windows Defender is enabled and scan. (Beau Curnow)
  - Windows Defender (set scan settings)
  - Click the Start Button.
  - Select Control Panel.
  - Click on the Search Bar in the upper right hand corner and type in "Windows Defender". Press enter.
  - Click on Windows Defender.
  - Click on the "Check for Updates" button.
  - After it checks, click on "Tools".
  - Click on Options.
  - Here, you can set the Frequency of the automatic scan.
  - If a scan picks up on spyware or unwanted software, use the hot fixes it gives you, or do manual actions to solve the problem.(All by Thomas Polk)
- Install spyware. (Thomas Polk)
- Setup Windows Firewall settings to secure against public networks, and to secure your private and domain networks. Use recommended settings. (Thomas Polk)

#### OS UPDATES

- Install the latest service pack (from thumb drive).
  - Remember to do this at the beginning. (Beau Curnow)
- Enable Automatic Updates (Beau Curnow)
- Install All Updates (Beau Curnow)
- Make sure no other updates are listed after a MBSA scan. (Beau Curnow)
- Keep firewall updated. (Thomas Polk)
- Update web browser. (Thomas Polk)

#### OVERALL SECURITY POSTURE OF SYSTEM

- Run a MBSA Scan and correct any problems found. (Beau Curnow)
  - MBSA Link: <http://www.microsoft.com/en-us/download/details.aspx?id=7558> 0
- Enable hidden file and folder viewing. (Beau Curnow)
  - Here's how to display hidden files and folders.
    1. Open Folder Options by clicking the Start button , clicking Control Panel, clicking Appearance and Personalization, and then clicking Folder Options.
    2. Click the View tab.
    3. Under Advanced settings, click Show hidden files, folders, and drives, and then click OK.
      - <http://windows.microsoft.com/en-US/windows7/Show-hidden-files>  
(Submitted by Chloe)
- Disable Remote Desktop connection. (Beau Curnow)

- From Readme file, determine if Windows 7 needs to be automatically locked-if so, configure this setting. (Submitted by Chloe)
  - Download Link: <http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx>  
(Submitted by Chloe)
- Delete Shares
  - Use command prompt net share.(Beau Curnow)
- Set audit policies for all areas of system in Local Security Policies. (Beau Curnow)
- View Action Center and correct any problems listed. (Beau Curnow)
- Make sure file sharing is disabled. (unless otherwise specified on README) (Beau Curnow)
- Setup internet security policies
  - Set security level under internet to highest settings. (Beau Curnow)
  - Under Privacy Tab set slider to highest. (Beau Curnow)
- Turn on web browser security features. (Thomas Polk)
- Get rid of spam and use safe e-mail techniques.(Thomas Polk)

○ Re-read Readme file for things missed or not looked at

—highlight key points and re-check all