Cyberpatriot Windows 10 Checklist (With Scripts)

- **Read through the readme**
  - Take a picture of all passwords including your own for future reference
  - Take a mental note of special rules set by the readme

- **Complete forensics questions**

- Ensure Proper Services are Enabled and Disabled **(*scripted*)**
  - Run the “Configure Services” script as an administrator

- Clear Group Policy **(*scripted*)**
  - Run the “Clear Group Policy” script as an administrator
  - Run the “Configure Group Policy” script as an administrator

- Begin Checking for Windows Updates **(control update)**

- Scan for Malware **(windowsdefender:)**
  - → Virus & threat protection
    - → Manage settings → Add or remove exclusions
      - Remove any exclusions not related to CCS (the scoring engine)
    - Start a full scan

- Begin System Integrity Scan **(cmd *run as admin by using ctrl+shift+enter*)**
  - Run the command “sfc -scannow”

- Configure Windows Firewall **(*scripted*)**
  - Run the “Configure Firewall” script as an administrator

- Configure Security Policy and Passwords **(*scripted*)**
  - Run the “Configure Security Policy and Passwords” script as an administrator

- Manage Users **(lusrmgr.msc)**
  - → Users
    - Delete unauthorized accounts
  - → Groups
    - Make sure that the Administrators group contains the correct users
    - Check other groups for unauthorized users

- Manage Features and Programs **(appwiz.cpl)**
  - Uninstall any suspicious programs (make sure they are not required on readme)
  - → Turn Windows features on or off
    - Disable Simple TCPIP Services

        - Disable SMB 1.0
        - Disable Telnet Client
        - Disable TFTP Client
        - Enable Internet Explorer here if required by the readme

- Manage Files and Folders **(explorer)**
    - → View tab → Options → View
        - Select “Show hidden files, folders, and drives”
        - Uncheck “Hide extensions for known file types”
        - Uncheck “Hide protected operating system files”
    - Search the whole computer for a folder called FTP
        - If it exists, edit its properties and turn off write permissions for the “Everyone” group

- Remove any unauthorized media files or programs **(*scripted assisted*)**
    - Run the “Scan for Files” script as an administrator
    - Delete any media files, games, etc. that pop up (but make sure to check the readme for a list of things that you shouldn’t delete)
    - Check your own desktop for any odd programs
    - Check your own user folders for any odd files

- Ensure that all software required in the readme is installed on the latest version (ex: Firefox)
    - Update within the program if possible
    - Otherwise, download the latest version from the internet and run installer
        - Download the 32 bit version of the program if it is installed to Program Files (x86), and get the 64 bit version if it is installed to Program Files

- Secure Internet Connections **(inetcpl.cpl)**
    - → Security Tab
        - Security Level: High
    - → Privacy Tab
        - All options should be enabled/checked
        - → Advanced
            - Block all first and third party cookies
            - Allow session cookies

- Manage Network Sharing **(cmd *run as admin by using ctrl+shift+enter*)**
    - Type “net share” into a cmd Window to view shared network folders
    - There should be 3 items listed: C$, IPC$, and ADMIN$. If there are others, delete them using “net share /delete [name]”

- **<u>***Complete any tasks remaining in the readme***</u>**

End of Main Checklist. If points are still missing, there are likely malicious processes, tasks, etc. on the machine. A more in depth look at certain management menus may reveal some flags:

- Verify safety of programs using Process Explorer **(Program is located in the Sysinternals folder of the flash drive. Run it as an administrator)**
    - → Options → VirusTotal.com
        - Select “Check VirusTotal.com”
    - Sort the processes by the VirusTotal column to see the most likely threats
        - Investigate further into programs that have a high detection score

- Search task scheduler for malicious tasks **(taskschd.msc)**
    - Click “Enable All Tasks History” in the upper right
    - Click “Refresh” periodically and look in the “Task Status” area for activity
    - If anything appears, find the task in the “Active Tasks” area and double click it
        - View what the task does and disable it if it appears to be malicious

- Search startup programs for malicious programs **(msconfig)**
    - → Startup tab
        - Click to view task manager if requested
        - Find where each program is installed to and examine what it does
        - Disable or delete something if it looks to be malicious

- Check network activity for anything suspicious using TCPView **(Program is located in the Sysinternals folder of the flash drive. Run it as an administrator)**
    - Close everything else on the computer if possible
    - → Options
        - Select “Resolve Addresses”
    - Scan through all processes that have a unique remote address
    - Right clicking on processes and bringing up the properties menu will show the certificate holder of the program

- Look in C:\Program Files\ and C:\Program Files (x86) for suspicious program folders
- Sort files in C:\Windows\System & C:\Windows\System32 by recent and look for files that have been inserted into the system
- Get Malwarebytes antivirus scanner and Malwarebytes rootkit scanner and run a full, advanced scan (make sure that it scans for rootkits)
- Check for out of the ordinary inbound and outbound rules in the firewall **(wf)**