Cyberpatriot Windows 10 Checklist (With Scripts)

- Complete All Forensics Questions

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

- Configure Group Policy **(*scripted*)**
    - 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 all exclusions
        - 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

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

- Update Programs
    - 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

- 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 Files and Folders **(explorer)**
    - → View tab
        - Enable view of file name extensions and hidden items
    - Remove any unauthorized media files or programs
        - Remove any disallowed media from C:\Users including user desktops
        - Remove any disallowed programs from C:\Users including user desktops
    - If there is a folder called FTP anywhere, edit its properties and turn off write permissions for the “Everyone” group

- 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]”

- Complete any tasks remaining in the readme

End of Main Checklist. If points are still missing, there are likely malicious processes on the machine or breached connections

- Search the central panel of task scheduler for malicious tasks **(taskschd.msc)**
- Search startup programs for malicious programs **(msconfig)** → Startup tab
- Look in C:\Program Files\ and C:\Program Files (x86) for suspicious programs
- 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 scan
- Check for out of the ordinary inbound and outbound rules in the firewall **(wf)**