Cyberpatriot Checklist: Windows 10 Machines (No Scripts)

- **Read the readme and note everything mentioned**
- **Complete all forensics questions**
- **Plug in the Windows 10 flash drive and copy <u>all</u> files to a folder on the virtual machine**

- Ensure Proper Services are Enabled and Disabled
    - Run ServicesConfig.bat as an administrator (within Scripts folder of flash drive)

- Configure Windows Updates. **(control update)**
    - → Advanced Options
        - Check "Give me updates for other Microsoft products when I update Windows."
        - Turn on automatic updates
        - Make sure that updates are not paused
        - → View configured update policies (if appeared)
            - Fix any significant changes
        - → Delivery optimization (if appeared)
            - Allow downloads from other PCs: Off
    - Manually check for updates and let it run in the background

- Configure Windows Defender Firewall **(wf.msc)**
    - → Windows Defender Firewall Properties
        - Turn the firewall on, block all inbound connections, and allow all outbound connections for each profile
        - Customize protected network connections and ensure that all network adapters are checked for each profile
    - Investigate inbound and outbound rules if some process is not functioning properly
        - Enable any required connections that have been maliciously disabled

- Configure Windows Defender **(windowsdefender:)**
    - → Virus & Threat Protection
        - Turn on every setting
        - Immediately start a full scan (Advanced scan → Full scan)
    - → App & browser control
        - Set every setting to warn

- Begin a System Integrity Scan
    - Open up cmd as an administrator and run "sfc -scannow" (run in background)

- Configure Firefox (typically required)
    - Ensure the machine has the latest version of Firefox
    - In Firefox, Options → Privacy and Security
        - Enable popup blocker
        - Configure any other obvious settings

- Search Task Scheduler for Malicious Tasks **(taskschd.msc)**
    - Check the central area for suspicious tasks and disable anything malicious

- Configure Features and Programs **(appwiz.cpl)**
    - Uninstall any suspicious programs
    - → 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

- Configure Startup Programs **(msconfig)**
    - → Startup tab
        - Disable any suspicious processes

- Manage Accounts **(lusrmgr.msc)**
    - → Users
        - Disable Guest and Administrator accounts
        - Delete unauthorized accounts
        - Change any unsecure or blank passwords (just change every user password to be safe)
    - → Groups
        - Make sure that those in Administrators group are meant to be administrators
        - Make sure that no other groups contain unauthorized users

- Configure Security Settings **(scripted)**
    - Run SecPolConfig.bat as an administrator (within Scripts folder of flash drive)

- Secure Internet Connections **(inetcpl.cpl)**
    - → Security Tab
        - Security Level: High
    - → Privacy Tab

        - Check “Never allow websites to request your physical location”
        - Check “Turn on Pop-up Blocker”
        - Check “Disable toolbars and extensions when InPrivate Browsing starts”
        - → Advanced
            - Block all first and third party cookies
            - Allow session cookies

- Delete Suspicious and Unauthorized Files **(explorer)**
    - → View tab
        - Enable view of file name extensions and hidden items
    - Sort files in C:\Windows\System & C:\Windows\System32 by recent and look for manipulated files
    - Look in C:\Program Files\ and C:\Program Files (x86) for suspicious programs
    - Remove any unauthorized media files
        - Search in C:\Users for various file types (.png, .gif, .mp3, etc.)

- Secure Folder Permissions
    - If there is an FTP folder, turn off write permissions for the “Everyone” group for it
    - Type “net share” into a cmd Window to view shared network folders
        - If anything is shared between users, type “net share [name of folder] /delete” to delete the folder

- Configure Remote Desktop **(sysdm.cpl)**
    - → Remote tab
        - Disable remote assistance
        - Allow or don’t allow remote desktop connections depending on what is said in the readme
        - If allowed, make sure that the requirement for Network Level Authentication is checked

- Configure Group Policy **(gpedit.msc)**
    - → Computer Configuration → Administrative Templates → All Settings
        - Sort by State to view all things that have been enabled/disabled
        - Check each item for possible vulnerabilities
        - Configure well known vulnerable settings
            - Enable “Turn off Autoplay”
            - Enable “Do not allow supported Plug and Play device redirection”

- Configure anything else mentioned in the readme (ex: update notepad++)

- Enable UAC **(useraccountcontrolsettings.exe)**
    - The slider should be set to “Always Notify”

- Finish Previous Processes
    - Restart if Windows updates are installed
    - Restart if required after sfc scan
    - Quarantine anything found by antivirus

- If There Are Still Flags to Be Found
    - Review the checklist to make sure that you ran through everything correctly
    - Read back through the readme and make sure that nothing there was missed
    - Use a program like process explorer to look for hidden malicious processes
    - Install SCC 5.5 from the flash drive files and run a full hardening scan