Cyberpatriot Windows Checklist

* Login and User Accounts:
  + Log in using the provided credentials.
  + Check if the account is part of the Administrators group:
    - Right-click on the Start menu and select "Computer Management."
    - Navigate to "Local Users and Groups" > "Groups."
    - Double-click on the "Administrators" group and ensure your account is listed.
* Firewall Configuration:
  + Enable the Windows Firewall if it's not already enabled:
    - Open "Control Panel" from the Start menu.
    - Go to "System and Security" > "Windows Defender Firewall."
    - Ensure that "Windows Defender Firewall" is set to "On."
* Windows Updates:
  + Check for and install Windows updates:
    - Open "Settings" from the Start menu.
    - Go to "Update & Security" > "Windows Update."
    - Click on "Check for updates" and install any available updates.
* User Account Control (UAC):
  + Verify that UAC is enabled:
    - Open the "Control Panel."
    - Go to "User Accounts" > "User Accounts."
    - Click on "Change User Account Control settings" and ensure it's set to a level other than "Never notify."
  + Open Command Prompt as an administrator.
    - Adjust UAC settings using the command: reg add "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v ConsentPromptBehaviorAdmin /t REG\_DWORD /d 2 /f
* Network Configuration:
  + Check network connection and disable unused network adapters:
    - Right-click on the network icon in the taskbar and select "Open Network & Internet settings."
    - Click on "Change adapter options" and disable any unnecessary network adapters.
  + Open Command Prompt as an administrator.
  + Disable unused network adapters with: ‘netsh interface set interface "Name of Adapter" admin=disable’
* Password Policies:
  + Check the complexity requirements for passwords:
    - Open "Local Security Policy" by searching in the Start menu.
    - Navigate to "Account Policies" > "Password Policy."
    - Ensure password complexity requirements are enabled.
  + Open Command Prompt as an administrator.
    - Set password complexity with: net accounts /minpwlen:8 /maxpwage:30 /minpwage:1 /uniquepw:5
* Guest Account:
  + Disable the guest account if enabled:
    - Open "Control Panel" and go to "Administrative Tools."
    - Open "Computer Management" and navigate to "Local Users and Groups" > "Users."
    - Right-click on the "Guest" account and select "Properties." Uncheck "Account is disabled."
* Remote Desktop:
  + Disable Remote Desktop if not needed:
    - Open "Control Panel" and go to "System."
    - Click on "Remote settings" on the left sidebar.
    - Select "Don't allow remote connections to this computer."
  + Open Command Prompt as an administrator.
    - Disable Remote Desktop with: reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG\_DWORD /d 1 /f
* AutoRun and AutoPlay:
  + Configure AutoRun and AutoPlay settings:
    - Open "Control Panel" and go to "Hardware and Sound."
    - Under "AutoPlay," configure settings for different media types.
* File Sharing:
  + Disable unnecessary file and printer sharing:
    - Open "Control Panel" and go to "Network and Sharing Center."
    - Click on "Change advanced sharing settings" on the left.
    - Turn off network discovery, file and printer sharing, and public folder sharing if not needed.
* Patch Management:
  + Update all software and applications:
    - Open "Control Panel" and go to "Programs and Features."
    - Review the list of installed software and ensure they're up to date. Update or uninstall any unnecessary applications.
  + Check for updates by typing: wuauclt /detectnow
* Antivirus and Antimalware:
  + Install and configure an antivirus program:
    - Download a reputable antivirus software from the vendor's official website.
    - Install the software and enable real-time scanning.
    - Perform a full system scan to ensure there are no malware threats.
* User Account Control (UAC) Settings:
  + Adjust UAC settings to a higher level:
    - Open "Control Panel" and go to "User Accounts" > "User Accounts."
    - Click on "Change User Account Control settings" and increase the notification level.
* Group Policy Settings:
  + Configure security-related Group Policy settings:
    - Open "Local Group Policy Editor" by searching in the Start menu.
    - Explore different categories under "Computer Configuration" and "User Configuration" to adjust security policies.
* Network Security:
  + Implement stronger network security measures:
    - Configure a separate network profile for public Wi-Fi connections:
      * Open "Settings" > "Network & Internet" > "Wi-Fi" > "Manage known networks."
      * Set public network settings to block file and printer sharing.
    - Enable MAC address filtering on your router if available.
* Data Encryption:
  + Encrypt sensitive data on the system drive:
    - Open "Control Panel" and go to "BitLocker Drive Encryption."
    - Enable BitLocker encryption for the system drive (C:), following the setup wizard.
* Application Whitelisting:
  + Configure AppLocker to allow only approved applications:
    - Open "Local Security Policy" by searching in the Start menu.
    - Navigate to "Application Control Policies" > "AppLocker."
    - Create rules to only allow approved applications to run.
* Disable Unnecessary Services:
  + Review and disable unnecessary services:
    - Open "Services" by searching in the Start menu.
    - Identify and disable services that are not essential for the system's operation.
* Secure Browser Configuration:
  + Configure browser settings for enhanced security:
    - Install browser extensions for ad-blocking and anti-malware.
    - Disable unnecessary plugins and extensions.
* Remote Desktop Lockdown:
  + Further secure Remote Desktop settings:
    - Open "Local Group Policy Editor" and navigate to "Computer Configuration" > "Administrative Templates" > "Windows Components" > "Remote Desktop Services."
    - Configure settings like "Limit Maximum Color Depth," "Require Use of Specific Security Layer," and "Set Client Encryption Level."
* Password Management:
  + Enforce password expiration and complexity policies:
    - Open "Local Security Policy" and navigate to "Account Policies" > "Password Policy."
    - Configure policies for maximum password age, minimum password length, and password history.
* Audit and Logging:
  + Enable audit policies and review logs:
    - Open "Local Security Policy" and navigate to "Advanced Audit Policy Configuration" under "Advanced Security Settings."
    - Configure audit policies for logon events, account management, and more.
    - Regularly review the Event Viewer for security-related events.
* PowerShell Security Policies:
  + Set execution policy to restrict PowerShell scripts:
    - Open PowerShell as an administrator.
    - Run the command: Set-ExecutionPolicy RemoteSigned
    - Confirm the policy change.
* Software Restriction Policies:
  + Configure software restriction policies to prevent unauthorized software:
    - Open "Local Group Policy Editor" and navigate to "Computer Configuration" > "Windows Settings" > "Security Settings" > "Software Restriction Policies."
    - Create a new software restriction policy and disallow running executables from specific locations.
* Advanced Firewall Rules:
  + Create custom inbound and outbound firewall rules:
    - Open "Windows Defender Firewall with Advanced Security."
    - Define custom rules to allow or block specific applications or ports.
* Command Line Scanning:
  + Use Windows Defender to scan files and folders from Command Prompt:
    - Open Command Prompt as an administrator.
    - Run the command: MpCmdRun.exe -Scan -ScanType 3 -File <path\_to\_file\_or\_folder>
* Group Policy Scripts:
  + Deploy scripts using Group Policy:
    - Open "Group Policy Management Console" by searching in the Start menu.
    - Create a new GPO and configure a startup or shutdown script to perform specific actions.
* Network Monitoring:
  + Use Command Prompt to monitor network connections:
    - Open Command Prompt as an administrator.
    - Run the command: netstat -ano to view active network connections.
* Remote Management Lockdown:
  + Disable unnecessary remote management protocols:
    - iisOpen "Local Group Policy Editor" and navigate to "Computer Configuration" > "Administrative Templates" > "System" > "Remote Assistance" or "Remote Desktop Services."
    - Configure policies to restrict remote access.
* Security Auditing and PowerShell:
  + Use PowerShell to enable security auditing:
    - Open PowerShell as an administrator.
    - Run the command: auditpol /set /subcategory:"Detailed Tracking" /success:enable
    - This will enable auditing of detailed tracking events.
* Custom Scripts and Automation:
  + Create and execute custom scripts for system auditing:
    - Utilize PowerShell to collect system information, such as running processes, installed applications, and system configurations.
* Sysinternals Suite:
  + Download and utilize Sysinternals Suite tools:
    - Download the Sysinternals Suite from the official Microsoft website.
    - Explore and use various tools for advanced system analysis and troubleshooting.
* Hardening Registry Settings:
  + Configure registry settings for added security:
    - Use the Registry Editor (regedit) to adjust permIions, disable autorun, and strengthen security settings.
* Service Hardening:
  + Configure service startup types and permissions:
    - Use the "Services" application or PowerShell to modify service configurations, startup types, and associated user permissions.

File Cleanup and Analysis:

* Step 1: Open Command Prompt as an administrator.
* Step 2: To navigate to a specific directory (e.g., Downloads), type: cd C:\Users\<YourUsername>\Downloads
* Step 3: To list all .mp4 files in the directory, type: dir \*.mp4 /s
* Step 4: To delete a specific .mp4 file, type: del <filename.mp4>

Temporary Files Cleanup:

* Step 1: Open the Run dialog by pressing Win + R.
* Step 2: Type %temp% and press Enter to access the temporary files directory.
* Step 3: Select all files and folders (Ctrl + A) and press Delete.
* Browser Privacy Settings:
  + Adjust browser settings for improved privacy:
    - Open your web browser's settings.
    - Review and modify privacy settings, disable cookies, and manage browsing history.
* Securing Documents and Folders:
  + Review and adjust file and folder permissions:
    - Right-click on files or folders and go to "Properties" > "Security."
    - Adjust permissions to limit access to authorized users.
* Unused User Accounts:
  + Disable or remove unused user accounts:
    - Open "Control Panel" and go to "User Accounts" > "User Accounts."
    - Manage user accounts, disable or remove any accounts that are not needed.
* Advanced Registry Cleanup:
  + Scan and clean up unused or invalid registry entries:
    - Use a reliable registry cleaner tool to perform a scan and remove unnecessary entries.
* Application Logs Review:
  + Explore application logs for potential issues:
    - Open "Event Viewer" and navigate to "Windows Logs" > "Application."
    - Review logs for errors, warnings, or events that could indicate misconfigurations.
* Network Analysis:
  + Use network analysis tools to identify vulnerabilities:
    - Utilize tools like Wireshark to capture and analyze network traffic for suspicious activities.
* Third-Party Software Updates:
  + Check for updates in third-party applications:
    - Launch applications like Adobe Reader, Java, and web browsers to check for updates.
* Review Your Work:
  + Double-check your changes and configurations:
    - Carefully review all the changes you've made during the competition to ensure they're correct and secure.
* Documentation and Notes:
  + Document your changes and create notes:
    - Write down the tasks you've completed, changes you've made, and any important notes for future reference.
* Final System Scan:
  + Run a final antivirus and antimalware scan:
    - Open your installed antivirus program and perform a full system scan.

Malware Removed:

* Install Antivirus Software:
  + Download a reputable antivirus software from a trusted source.
  + Install the antivirus software following the installation wizard.
  + Enable real-time scanning and updates.
* Run a Full System Scan:
  + Open the installed antivirus software.
  + Initiate a full system scan from the software's user interface.
  + Follow any prompts to quarantine or remove any detected malware.

Removed VNC Server Software:

* Uninstall VNC Software:
  + Open the Control Panel.
  + Go to "Programs and Features."
  + Locate the VNC server software in the list of installed programs.
  + Right-click on the software and select "Uninstall."
  + Follow the uninstallation wizard to remove the software.

Web Server Is Turned Off:

* Disable IIS (Internet Information Services):
  + Open the Control Panel.
  + Go to "Programs and Features."
  + Click on "Turn Windows features on or off" on the left.
  + Uncheck the "Internet Information Services" option.
  + Click OK to confirm and disable IIS.

TFTP Server Is Turned Off:

* Disable TFTP Server:
  + Open the Control Panel.
  + Go to "Programs and Features."
  + Click on "Turn Windows features on or off" on the left.
  + Uncheck the "Trivial File Transfer Protocol (TFTP) Client" and "Trivial File Transfer Protocol (TFTP) Server" options.
  + Click OK to confirm and disable TFTP.

File Sharing Is Disabled for C Drive:

* Disable File Sharing:
  + Open the Control Panel.
  + Go to "Network and Sharing Center."
  + Click on "Change advanced sharing settings" on the left.
  + Under "File and printer sharing," select the option "Turn off file and printer sharing."

Guest Account Has Been Disabled:

* Disable Guest Account:
  + Open the Control Panel.
  + Go to "Administrative Tools."
  + Open "Computer Management" and navigate to "Local Users and Groups" > "Users."
  + Right-click on the "Guest" account and select "Properties."
  + Check the box "Account is disabled."

Remote Registry Service Is Stopped:

* Stop Remote Registry Service:
  + Press Win + R to open the Run dialog.
  + Type "services.msc" and press Enter.
  + Locate the "Remote Registry" service in the list.
  + Right-click on it and select "Stop."

FAT File System Converted to NTFS:

* Convert Filesystem:
  + Open Command Prompt as an administrator.
  + Type the command: convert C: /fs:ntfs
  + Follow the prompts to schedule the conversion for the next restart.

Unnecessary Testing Account Removed:

* Remove User Account:
  + Open the Control Panel.
  + Go to "User Accounts" > "User Accounts."
  + Select "Manage another account."
  + Locate the testing account you want to remove.
  + Select "Delete the account" and follow the prompts.

Secure Browser Configuration:

* Install Browser Extensions:
  + Open your web browser.
  + Visit the extension/add-on store (e.g., Chrome Web Store for Google Chrome).
  + Search for and install reputable ad-blocking and anti-malware browser extensions.
* Disable Unnecessary Plugins and Extensions:
  + Open your browser's settings or extensions/add-ons page.
  + Review the list of installed plugins and extensions.
  + Disable or remove any plugins or extensions that are not necessary.

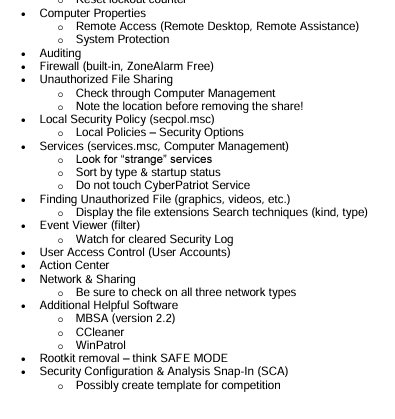
Group Policy Scripts:

* Create a Script:
  + Prepare the script you want to deploy. Save it in a location accessible by the target systems.
* Open Group Policy Management:
  + Press Win + R to open the Run dialog.
  + Type "gpmc.msc" and press Enter to open the Group Policy Management Console.
* Create a New Group Policy Object (GPO):
  + In the left pane, expand your domain and right-click on "Group Policy Objects."
  + Select "New" and give the GPO a name.
* Edit the GPO:
  + Right-click on the newly created GPO and select "Edit."
* Configure Startup or Shutdown Script:
  + Navigate to "Computer Configuration" > "Policies" > "Windows Settings" > "Scripts (Startup/Shutdown)."
  + Double-click on "Startup" or "Shutdown" (depending on when you want the script to run).
  + Click "Add" to add your script file.
* Specify Script Parameters (if needed):
  + Click "Show Files" to open the script directory.
  + Copy your script file into this directory.
  + Go back to the "Add a Script" dialog and click "Browse."
  + Select your script file and add any necessary parameters.
* Close and Link the GPO:
  + Close the Group Policy Management Editor.
  + Link the GPO to an organizational unit (OU) containing the target computers.
  + The script will run during the computer startup or shutdown process based on your configuration.

Network Monitoring:

* Use Command Prompt for Network Monitoring:
  + Open Command Prompt as an administrator.
  + Run the command: netstat -ano
  + This will display a list of active network connections along with the process IDs (PIDs).
* Open Windows Firewall Settings:
  + Press Win + R, type firewall.cpl, and press Enter.
  + Click on “Advanced settings” to open the Windows Firewall with Advanced Security.
* Review Inbound Rules:
  + In the left pane, click on “Inbound Rules”.
  + Look through the list of inbound rules for any that are related to the executable file in question (C:\ProgramData\SoftwareDistribution\rvlkl.exe in your case).
* Find the Rule and IP Address:
  + Once you find the relevant rule, double-click on it to view its properties.
  + Go to the “Scope” tab where you will find the list of allowed IP addresses under “Remote IP address”. This is where you should find the external IP address that is allowed to connect.
* Document the IP Address:
  + Note down the IP address for your report.

This IP address is the external address that the firewall rule allows to connect to the specified executable, potentially indicating the backdoor set up by the contractor.



Checklists:  
[chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://sjbdigital.com/cyber/DOCs/CyberPatriot\_Windows\_CheckList.pdf](https://sjbdigital.com/cyber/DOCs/CyberPatriot_Windows_CheckList.pdf)

<https://github.com/ponkio/CyberPatriot?tab=readme-ov-file#scripts>

<https://www.coursehero.com/file/71990275/Copy-of-Chantilly-Cyber-Patriot-Windows-Checklist/>

SERVICES CHECKING FOR NATS: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/<https://www.cusd80.com/site/handlers/filedownload.ashx?moduleinstanceid=111871&dataid=175133&FileName=Unit%208%20-%20Microsoft%20Windows%20Security%20Configuration.pdf>