



Team Number _____
Round # ____ Date: ____ / ____ / ____
Operating System: Windows

CyberPatriot Categorized Checklist

First Steps:

- Discuss README together
 - Mark important information about what you specifically need to do to the machine
- Get the flash drive.
 - If Service Packs are available Install them while discussing the README or after (WSUS offline Updater)
 - Download the Programs: MalwareBytes, BitDefender, CCleaner, IOBitUninstaller, MSBA, ProcessExplorer, and Wireshark.
 - Get your script for the machine you are working on.
 - Get the Internet Browsers that you are supposed to be running on your machine.
 - Get the Microsoft Common Console. (Shows services, shares, firewall, users + groups, event viewer, etc.)

NOW FOR THE GOOD STUFF: Before Running script!!!

- **ANSWER YOUR FORENSIC QUESTIONS!**
 - After, Open your Internet browser and make sure your Adobe Flash/Reader and Java Plugins are up-to-date. Also remove any toolbars that are not supposed to be there.

Now for the script

- If you have any question about the script ask the person who made it to make sure everything works correctly.
- After the script has ran take note of the things you have gotten points for if your script didn't get point in a section it should have then you HAVE to check it manually.

After script

- Password Policy
 - Enforce password history: *24*
 - Maximum password age: *60*
 - Minimum password age: *1*
 - Minimum password length: *10*
 - Password must meet complexity requirements: *Enabled*
 - Store password using reversible encryption: *Disabled*
- Lockout Policy
 - Account lockout duration: *30 Minutes*
 - Account lockout threshold: *10*
 - Reset account lockout counter after: *30*
- Check user settings
 - All users should have 'User must change password at next logon' checked
 - All unauthorized users should have 'Account is disabled'
- Check ALL the groups
 - 'Administrators' group should ONLY have AUTHORIZED admins.
 - 'Guests' group should ONLY have 'Guest' in it
 - If the README wants only certain users to use RDP then add ONLY those users to the 'Remote Desktop Users' group
- Use SmartScreen online services(Security and Maintenance)=ON
- Wi-Fi Sense (Network & Internet)
 - Automatically connect to suggested open hotspots=OFF
 - Automatically connect to hotspots temporarily to see if paid network services are available=OFF
- Turn UAC to max(Change User Account Control Settings)
- Change Adapter settings(Disabling IPv6 and other services)=Uncheck these
 - Client for MS Networks
 - File and Printer Sharing for Microsoft Networks
 - QoS



Team Number _____
Round # ____ Date: ____ / ____ / ____
Operating System: Windows

CyberPatriot Categorized Checklist

- Microsoft Network Adapter Multiplexor Protocol
 - Microsoft LLDP Protocol Driver
 - Link Layer Topology Discovery Mapper IO Driver
 - Link Layer Topology Discovery Responder
 - Internet protocol version 6
 - 'Internet Protocol version 4 (TCP IPv4), click Properties, click Advanced,
 - 'DNS' tab, uncheck mark 'register this connections address in DNS'
 - 'WINS' tab, select 'Disable NETBIOS over TCP/IP'
- Disable port 1900 UPnP
 - Regedit path: HKLM\Software\Microsoft\DirectplayNATHelp\DPNHUPnP
 - Right click on right pane, new dword:32 bit, named UPnPMode
 - Double click on that and set it to 2
- Windows Services
 - UPnP Device Host: Stopped – Disabled
 - RDP: Depends on README
 - Telnet: Stopped – Disabled
 - SNMP Trap: Stopped – Disabled
 - Windows Event Collector: Running – Automatic
 - Remote Registry: Stopped - Disabled
 - ##ADD OTHER SERVICES
- Check windows features
 - Control Panel>Programs> Turn Windows features on or off
 - Things to never have on
 - Telnet client\server
 - SNMP
 - RIP Listener
 - Client for NFS
 - Internet Information Services (IIS)
 - World Wide Web Services
 - If FTP sever then turn on TFTP otherwise make sure that it is not checked
 - Disable SMB v1
 - Turn Windows features on or off=Uncheck SMB 1.0/CIFS File Sharing Support
- Shares
 - Only 3 shares should be shared unless README says otherwise
 - ADMIN\$
 - C\$
 - IPC\$
- Firewall rules:
 - Inbound=disable MS Edge



Team Number _____
Round # ____ Date: ____ / ____ / ____
Operating System: Windows

CyberPatriot Categorized Checklist

- Inbound=disable Search
- Inbound=disable MSN Money
- Inbound=disable MSN Sports
- Inbound=disable MSN News
- Inbound=disable MSN Weather
- Inbound=disable Microsoft Photos
- Inbound=disable Xbox
- Turning off Tiles:
 - Right click on the Tile and choose turn off
- Turn off AutoPlay
 - Settings..Devices....AutoPlay=off
- Run the command “netplwiz”
- Disable OneDrive on Startup
 - Use Task Manager or msconfig.exe
- Screen Saver
 - Settings...Personalize....Lock Screen...Screen Saver settings=wait 10 min and checkmark “On resume display Logon screen”
- Auditing
 - Change all to Success/Failure
- Windows defender
 - Turn on Windows defender
 - If disabled go into gpedit.msc and find the ‘windows defender’ option and change to enable
- User Rights Assignment

Policy	Default	Secure Setting
Access Credential Manager as a trusted caller	No one	No one
Access the computer from the network	Everyone, Administrators, Users, Backup Operators	Administrators



Team Number _____

Round # ____ Date: ____ / ____ / ____

Operating System: Windows

CyberPatriot Categorized Checklist

<i>Act as park of the operating system</i>	No one	No one
<i>Adjust memory quotas for a process</i>	Administrators, LOCAL SERVICE, NETWORK SERVICE	Administrators, LOCAL SERVICE, NETWORK SERVICE
<i>Allow log on locally</i>	Guest, Administrators, Users, Backup Operators	Administrators, Users
<i>Allow log on through Remote Desktop Services</i>	Administrators, Remote Desktop Users	Administrators, Remote Desktop Users
<i>Back up files and directories</i>	Administrators, Backup Operators	Administrators
<i>Change system time</i>	Administrators, LOCAL SERVICE	Administrators, LOCAL SERVICE
<i>Change the time zone</i>	Administrators, LOCAL SERVICE, Users	Administrators, LOCAL SERVICE, Users
<i>Create a pagefile</i>	Administrators	Administrators
<i>Create a token object</i>	No one	No one
<i>Create global objects</i>	Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE	Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE
<i>Create permanent shared objects</i>	No one	No one
<i>Create symbolic links</i>	Administrators	Administrators
<i>Debug programs</i>	Administrators	Administrators
<i>Deny access to this computer from the network</i>	Guest	Guest, Local account
<i>Deny log on as a batch job</i>	No one	Guest
<i>Deny log on as a service</i>	No one	Guest
<i>Deny log on locally</i>	Guest	Guest
<i>Deny log on through Remote Desktop Services</i>	No one	Guest, Local account
<i>Enable computer and user accounts to be trusted for delegation</i>	No one	No one
<i>Force shutdown from a remote system</i>	Administrators	Administrators
<i>Generate security audits</i>	LOCAL SERVICE, NETWORK SERVICE	LOCAL SERVICE, NETWORK SERVICE
<i>Impersonate a client after authentication</i>	Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE	Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE



Team Number _____
Round # ____ Date: ____ / ____ / ____
Operating System: Windows

CyberPatriot Categorized Checklist

<i>Increase scheduling priority</i>	Administrators	Administrators
<i>Load and unload device drivers</i>	Administrators	Administrators
<i>Lock pages in memory</i>	No one	No one
<i>Log on as a batch job</i>	Administrators, Backup Operators, Performance Log Users	Administrators
<i>Log on as a service</i>	NT SERVICE\ALL SERVICES	No one
<i>Manage auditing and security log</i>	Administrators	Administrators
<i>Modify an object label</i>	No one	No one
<i>Modify firmware environment values</i>	Administrators	Administrators
<i>Perform volume maintenance tasks</i>	Administrators	Administrators
<i>Profile single process</i>	Administrators	Administrators
<i>Profile system performance</i>	Administrators, NT SERVICE\WdiServiceHost	Administrators, NT SERVICE\WdiServiceHost
<i>Replace a process level token</i>	LOCAL SERVICE, NETWORK SERVICE	LOCAL SERVICE, NETWORK SERVICE
<i>Restore files and directories</i>	Administrators, Backup Operators	Administrators
<i>Shutdown the system</i>	Administrators, Backup Operators, Users	Administrators, Users
<i>Take ownership of file or other objects</i>	Administrators	Administrators

○

- Local Security policies
 - **THESE ARE FOR MOST SECURE SETTINGS MAKE SURE TO CHECK THESE AS A TEAM!!!!**
 - Accounts: Administrator account status: *disabled*
 - Accounts: Block Microsoft accounts: *Users can't add or log on with Microsoft accounts*
 - Accounts: Guest account status: *disabled ***
 - Accounts: Limit local account use of blank passwords to console logon only: *enabled*
 - Audit: Audit access of global system objects: *disabled*
 - Audit: Audit the use of Backup and Restore privilege: *disabled*
 - Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings: *enabled*



Team Number _____
Round # ____ Date: ____ / ____ / ____
Operating System: Windows

CyberPatriot Categorized Checklist

- Audit: Shutdown system immediately if unable to log security audits: *enable?*
- DCOM: Machine access restrictions: *no remote access for all accounts*
- DCOM; Machine launch restrictions: *no remote launch and remote activation for all accounts*
- Devices: Allow undock without having to log on: *disabled*
- Devices: Allowed to format and eject removable media: *administrators and interactive users*
- Devices: Prevent users from installing printer drivers: *enabled*
- Domain member: Digitally encrypt or sign secure channel data (always): *enabled*
- Domain member: Digitally encrypt secure channel data (when possible): *enabled*
- Domain member: Digitally sign secure channel data (when possible); *enabled*
- Domain member: Disable machine account password changes: *disabled*
- Domain member: Maximum machine account password age: *30 days*
- Domain member: Require strong (Windows 2000 or later) session key: *enabled*
- Domain member: Display user information when session is locked: *do not display user information*
- Interactive logon: Do not display last user name: *enabled*
- Interactive logon: Do not require CTRL+ALT+DEL: *disabled*
- Interactive logon; Machine account lockout threshold: *10 invalid logon attempts*
- Interactive logon: Machine inactivity limit: *900 seconds*
- Interactive logon: Number of previous logons to cache (in case domain controller is not available: *4 logons*
- Interactive logon: Prompt user to change password before expiration: *14 days*
- Interactive logon; Require Domain Controller authentication to unlock workstation; *Disabled*
- Interactive logon: Require smart card: *disabled..*
- Interactive logon: Smart card removal behavior: *Lock workstation*
- MS network client: Digitally sign communications (always): *enabled*
- MS network client: Digitally sign communications (if server agrees): *enabled*
- MS network client: Send unencrypted password to third-party SMB servers: *disabled*
- MS network server; Amount of idle time required before suspending session: *15 minutes*
- MS network server: Digitally sign communications (always): *enabled*



Team Number _____
Round # ____ Date: ____ / ____ / ____
Operating System: Windows

CyberPatriot Categorized Checklist

- MS network server; Digitally sign communications (if client agrees); *enabled*
- MS network server: Disconnect clients when logon hours expire: *enabled*
- MS network server: Server SPN target name validation level: *Accept if provided by client*
- Network access: Allow anonymous SID/Name translation: *disabled*
- Network access: Do not allow anonymous enumeration of SAM accounts: *enabled*
- Network access: Do not allow anonymous enumeration of SAM accounts and shares: *enabled*
- Network access: Do not allow storage of passwords and credentials for network authentication: *enabled*
- Network access: Let Everyone permissions apply to anonymous users: *disabled*
- Network access: Named Pipes that can be accessed anonymously: *blank*
- Network access: Remotely accessible registry paths: *blank*
- Network access; Remotely accessible registry paths and sub-paths: *blank*
- Network access: Restrict anonymous access to Named Pipes and Shares: *enabled*
- Network access: Shares that can be accessed anonymously: *blank*
- Network access: Sharing and security model for local accounts: *Classic - local users authenticate as themselves*
- Network security: Allow Local System to use computer identity for NTLM: *enabled*
- Network security: Allow LocalSystem NULL session fallback: *disabled*
- Network security: Allow PKU2U authentication requests to this computer to use online identifies: *disabled*
- Network security: Configure encryption types allowed for Kerberos: *RC4_HMAC_MD5, AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types*
- Network security: Do not store LAN Manager hash value on next password change: *enabled*
- Network security: Force logoff when logon hours expire: *enabled*
- Network security; LAN Manager authentication level: *Send NTLMv2 response only, Refuse LM & NTLM*
- Network security: LDAP client signing requirements: *Negotiate signing*
- Network security: Minimum session security for NTLM SSP based (including secure RPC) clients: *Require NTLMv2 session security, Require 128 bit encryption*
- Network security: Minimum session security for NTLM SSP based (including secure RPC) server: *Require NTLMv2 session security, Require 128 bit encryption*
- Network security: Restrict NTLM: Incoming NTLM traffic: *Deny all accounts*



Team Number _____
Round # ____ Date: ____ / ____ / ____
Operating System: Windows

CyberPatriot Categorized Checklist

- Network security: Restrict NTLM: NTLM authentication in this domain: *Deny all*
- Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers: *Deny all*
- Recovery console: Allow automatic administrative logon: *disabled*
- Recovery console: Allow floppy copy and access to all drives and all folders: *disabled*
- Shutdown: Allow system to be shut down without having to logon: *disabled*
- Shutdown: Clear virtual memory page-file: *disabled*
- System cryptography: Use FIPS compliant algorithms for encryption, hashing and signing: *disabled*
- System objects: Require case insensitivity for non-Windows subsystems: *enabled*
- System objects: Strengthen default permissions of internal system objects (e.g. Symbolic links) : *enabled*
- System settings: Optional subsystems: *blank*
- System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies: *disabled*
- UAC: Admin Approval Mode for Built-in Administrator account: *enabled*
- UAC: Allow UIAccess applications to prompt for elevation without using the secure desktop: *disabled*
- UAC: Behavior of elevation prompt for administrators in Admin Approval Mode: *Prompt for consent on the secure desktop*
- UAC: Behavior of the elevation prompt for standard users: *Automatically deny elevation requests*
- UAC: Detect application installations and prompt for elevation: *enabled*
- UAC: Only elevate executables that are signed and validated: *disabled*
- UAC; Only elevate UIAccess applications that are installed in secure locations: *enabled*
- UAC: Run all administrators in Admin Approval Mode: *enabled*
- UAC: Switch to the secure desktop when prompting for elevation: *enabled*
- UAC: Virtualize file and registry write failures to per-user locations: *enabled*