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
  - Microsoft Network Adapter Multiplexor Protocol

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

  - o   Inbound=disable MS Edge

  - o   Inbound=disable Search

  - o   Inbound=disable MSN Money

  - o   Inbound=disable MSN Sports

  - o   Inbound=disable MSN News

  - o   Inbound=disable MSN Weather

CyberPatriot Categorized Checklist

_____

- o   Inbound=disable Microsoft Photos

- o   Inbound=disable Xbox

- Turning off Tiles:

    - o   Right click on the Tile and choose turn off

- Turn off AutoPlay

    - o   Settings..Devices….AutoPlay=off

- Run the command "netplwiz"

- Disable OneDrive on Startup

    - o   Use Task Manager or mscofig.exe

- Screen Saver

    - o   Settings…Personalize….Lock Screen...Screen Saver settings=wait 10 min and checkmark "On resume display Logon screen"

- Auditing

    - o   Change all to Success/Failure

- Windows defender

    - o   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 Manger as a trusted caller	No one	No one
Access the computer from the network	Everyone, Administrators, Users, Backup Operators	Administrators
Act as park of the operating system	No one	No one
Adjust memory quotas for a process	Administrators, LOCAL SERVICE, NETWORK SERVICE	Administrators, LOCAL SERVICE, NETWORK SERVICE
Allow log on locally	Guest, Administrators, Users, Backup Operators	Administrators, Users
Allow log on through Remote Desktop Services	Administrators, Remote Desktop Users	Administrators, Remote Desktop Users

CyberPatriot Categorized Checklist

Back up files and directories	Administrators, Backup Operators	Administrators
Change system time	Administrators, LOCAL SERVICE	Administrators, LOCAL SERVICE
Change the time zone	Administrators, LOCAL SERVICE, Users	Administrators, LOCAL SERVICE, Users
Create a pagefile	Administrators	Administrators
Create a token object	No one	No one
Create global objects	Administrators, LOCAL SERIVCE, NETWORK SERVICE, SERVICE	Administrators, LOCAL SERIVCE, NETWORK SERVICE, SERVICE
Create permanent shared objects	No one	No one
Create symbolic links	Administrators	Administrators
Debug programs	Administrators	Administrators
Deny access to this computer from the network	Guest	Guest, Local account
Deny log on as a batch job	No one	Guest
Deny log on as a service	No one	Guest
Deny log on locally	Guest	Guest
Deny log on through Remote Desktop Services	No one	Guest, Local account
Enable computer and user accounts to be trusted for delegation	No one	No one
Force shutdown from a remote system	Administrators	Administrators
Generate security audits	LOCAL SERVICE, NETWORK SERVICE	LOCAL SERVICE, NETWORK SERVICE
Impersonate a client after authentication	Administrators, LOCAL SERIVE, NETWORK SERVICE, SERVICE	Administrators, LOCAL SERIVE, NETWORK SERVICE, SERVICE
Increase scheduling priority	Administrators	Administrators
Load and unload device drivers	Administrators	Administrators
Lock pages in memory	No one	No one
Log on as a batch job	Administrators, Backup Operators, Performance Log Users	Administrators
Log on as a service	NT SERVICE\ALL SERVICES	No one

CyberPatriot Categorized Checklist

Manage auditing and security log	Administrators	Administrators
Modify an object label	No one	No one
Modify firmware environment values	Administrators	Administrators
Perform volume maintenance tasks	Administrators	Administrators
Profile single process	Administrators	Administrators
Profile system performance	Administrators, NT SERVICE\WdiServiceHost	Administrators, NT SERVICE\WdiServiceHost
Replace a process level token	LOCAL SERVICE, NETWORK SERVICE	LOCAL SERVICE, NETWORK SERVICE
Restore files and directories	Administrators, Backup Operators	Administrators
Shutdown the system	Administrators, Backup Operators, Users	Administrators, Users
Take ownership of file or other objects	Administrators	Administrators

- o

- Local Security policies

    - o **THESE ARE FOR MOST SECURE SETTINGS MAKE SURE TO CHECK THESE AS A TEAM!!!!!**

    - o Accounts: Administrator account status*: disabled*

    - o Accounts: Block Microsoft accounts: *Users can't add or log on with Microsoft accounts*

    - o Accounts: Guest account status: disabled **

    - o Accounts: Limit local account use of blank passwords to console logon only: *enabled*

    - o Audit: Audit access of global system objects: *disabled*

    - o Audit: Audit the use of Backup and Restore privilege: *disabled*

    - o Audit: Force audit policy subcategory settings (Windows Vista of later) to override audit policy category settings: *enabled*

    - o Audit: Shutdown system immediately if unable to log security audits: *enable?*

    - o DCOM: Machine access restrictions: *no remote access for all accounts*

    - o DCOM; Machine launch restrictions: *no remote launch and remote activation for all accounts*

    - o Devices: Allow undock without having to log on: *disabled*

    - o Devices: Allowed to format and eject removable media: *administrators and interactive users*

CyberPatriot Categorized Checklist

_____

- o Devices: Prevent users from installing printer drivers: *enabled*

- o Domain member: Digitally encrypt or sign secure channel data (always): *enabled*

- o Domain member: Digitally encrypt secure channel data (when possible): *enabled*

- o Domain member: Digitally sign secure channel data (when possible); *enabled*

- o Domain member: Disable machine account password changes: *disabled*

- o Domain member: Maximum machine account password age: *30 days*

- o Domain member: Require strong (Windows 2000 or later) session key: *enabled*

- o Domain member: Display user information when session is locked: *do not display user information*

- o Interactive logon: Do not display last user name: *enabled*

- o Interactive logon: Do not require CTRL+ALT+DEL: *disabled*

- o Interactive logon; Machine account lockout threshold: *10 invalid logon attempts*

- o Interactive logon: Machine inactivity limit: *900 seconds*

- o Interactive logon: Number of previous logons to cache (in case domain controller is not available: *4 logons*

- o Interactive logon: Prompt user to change password before expiration: *14 days*

- o Interactive logon; Require Domain Controller authentication to unlock workstation; *Disabled*

- o Interactive logon: Require smart card: *disabled*..

- o Interactive logon: Smart card removal behavior: *Lock workstation*

- o MS network client: Digitally sign communications (always): *enabled*

- o MS network client: Digitally sign communications (if server agrees): *enabled*

- o MS network client: Send unencrypted password to third-party SMB servers: *disabled*

- o MS network server; Amount of idle time required before syspending session: *15 minutes*

- o MS network server: Digitally sign communications (always): *enabled*

- o MS network server; Digitally sign communications (if client agrees); *enabled*

- o MS network server: Disconnect clients when logon hours expire: *enabled*

- o MS network server: Server SPN target name validation level: *Accept if provided by client*

- o Network access: Allow anonymous SID/Name translation: *disabled*

- o Network access: Do not allow anonymous enumeration of SAM accounts: *enabled*

CyberPatriot Categorized Checklist

_____

- o Network access: Do not allow anonymous enumeration of SAM accounts and shares: *enabled*

- o Network access: Do not allow storage of passwords and credentials for network authentication: *enabled*

- o Network access: Let Everyone permissions apply to anonymous users: *disabled*

- o Network access: Named Pipes that can be accessed anonymously: *blank*

- o Network access: Remotely accessible registry paths: *blank*

- o Network access; Remotely accessible registry paths and sub-paths: *blank*

- o Network access: Restrict anonymous access to Named Pipes and Shares: *enabled*

- o Network access: Shares that can be accessed anonymously: *blank*

- o Network access: Sharing and security model for local accounts: *Classic - local users authenticate as themselves*

- o Network security: Allow Local System to use computer identity for NTLM: *enabled*

- o Network security: Allow LocalSystem NULL session fallback: *disabled*

- o Network security: Allow PKU2U authentication requests to this computer to use online identifies: *disabled*

- o Network security: Configure encryption types allowed for Kerberos: *RC4_HMAC_MD5, AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types*

- o Network security: Do not store LAN Manager hash value on next password change: *enabled*

- o Network security: Force logoff when logon hours expire: *enabled*

- o Network security; LAN Manager authentication level: *Send NTLMv2 response only, Refuse LM & NTLM*

- o Network security: LDAP client signing requirements: *Negotiate signing*

- o Network security: Minimum session security for NTLM SSP based (including secure RPC) clients: *Require NTLMv2 session security, Require 128 bit encryption*

- o Network security: Minimum session security for NTLM SSP based (including secure RPC) server: *Require NTLMv2 session security, Require 128 bit encryption*

- o Network security: Restrict NTLM: Incoming NTLM traffic: *Deny all accounts*

- o Network security: Restrict NTLM: NTLM authentication in this domain: *Deny all*

- o Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers: *Deny all*

- o Recovery console: Allow automatic administrative logon: *disabled*

- o Recovery console: Allow floppy copy and access to all drives and all folders: *disabled*

- o Shutdown: Allow system to be shut down without having to logon: *disabled*

_____

o   Shutdown: Clear virtual memory page-file: *disabled*

o   System cryptography: Use FIPS compliant algorithms for encryption, hashing and signing: *disabled*

o   System objects: Require case insensitivity for non-Windows subsystems: *enabled*

o   System objects: Strengthen default permissions of internal system objects (e.g. Symbolic links) : *enabled*

o   System settings: Optional subsystems: *blank*

o   System settings: Use Certificate Rules on Windows Executables for Software Restriction Policies: *disabled*

o   UAC: Admin Approval Mode for Built-in Administrator account: *enabled*

o   UAC: Allow UIAccess applications to prompt for elevation without using the secure desktop: *disabled*

o   UAC: Behavior of elevation prompt for administrators in Admin Approval Mode: *Prompt for consent on the secure desktop*

o   UAC: Behavior of the elevation prompt for standard users: *Automatically deny elevation requests*

o   UAC: Detect application installations and prompt for elevation: *enabled*

o   UAC: Only elevate executables that are signed and validated: *disabled*

o   UAC; Only elevate UIAccess applications that are installed in secure locations: *enabled*

o   UAC: Run all administrators in Admin Approval Mode: *enabled*

o   UAC: Switch to the secure desktop when prompting for elevation: *enabled*

o   UAC: Virtualize file and registry write failures to per-user locations: *enabled*