Windows Checklist

Last Updated on 2-05-18

- **START WITH QUESTION**
- **Read Readme File**
- **THE README IS YOUR GOD! IT SAYS ANYTHING AND EVERYTHING. IF SOMETHING ON THIS CHECKLIST GOES AGAINST THE README, *DON'T DO IT!***
- Make note of any question files and answer them as soon as you find the answer.
- Remember not to delete/remove any user, account, file, or script as they can be the answer to your questions. **NEVER REMOVE the CyberPatriot Scoring Engine.**
- Write down any change that you make that gives you points. This is in case you need to restart your image.
- Note: For Windows Server, some navigation may be slightly different
- Make sure to write down everything that you change. Refer to these papers in future rounds.
- **Make sure to not lock yourself out**

User Accounts

Control Panel > User Accounts and Family Safety > **User Accounts**

OR

Control Panel > System and Security > Administrative Tools > **Computer Management**

- Create/Change password for all accounts
- Make sure that all given passwords are secure/meet the requirements
- Make sure all user accounts are in their respective groups/permissions
- Disable all user accounts not authorized
- Disable guest account unless stated in readme file
- Make sure that file permissions are correct for the users
    - Go to a file and right click > Properties > Security > Edit
        - Specific permissions override group permissions, such as giving all standard users read only but then specifically one user can edit

Background Tasks

Control Panel > System and Security > **Windows Update**

- **Download updates in background**
- Will update the service pack, but might have to update more than once to get the points (don't update more than three times)

Control Panel > System and Security > **Action Center**

- Update security protocols
- Backup if necessary
- Antivirus, antimalware
    - Ex. Avast

- Note: this slowed down the VM a lot, so do near the end

Quick and Easy Tasks

Control Panel > System and Security > **Windows Update**

- Enable Automatic Updates (recommended settings)

Control Panel > System and Security > **Windows Firewall**

- Turn on Windows Firewall / use recommended settings
- Check inbound/outbound rules

Control Panel > System and Security > Administrative Tools > **System Configuration**

- Disable startup services/tasks

Local Security Policy

Control Panel > System and Security > Administrative Tools > **Local Security Policy**

- Account Policies
  - Password Policy
    - 3 passwords remembered
    - 30-90 days maximum password age
    - 10 days minimum password age
    - 8-12 minimum password length
    - Enable complexity requirements
    - Disable reversible encryption
  - Account Lockout Policy
    - 30 mins account lockout duration
    - 5 invalid logon attempts threshold
    - 30 mins reset account lockout counter
- Local Policies
  - Audit Policy
    - Enable all audit policies (success, failure)
  - Security Options

    Note: The following are the most critical out of the security options. However, be sure to read all of them(click on Explain), not just the following and see what setting would be the most secure setting. - do if you still need points at the end
    - Accounts: Administrator account status - **Disable**
    - Accounts: Guest account status - **Disable**
    - Accounts: Limit local account use of blank passwords… - **Enable**
    - Devices: Restrict CD-Rom access to locally logged-on user... - **Enable**
    - Devices: Restrict Floppy access to locally logged-on user… - **Enable**
    - Domain Member: LDAP server signing requirements - **Enable**
    - Domain Member: Digitally encrypt or sign secure channel data (always) - **Enable**
    - Interactive Logon: Do not display last user name - **Enable**
    - Interactive Logon: Do not require CTRL + ALT + DEL - **Disable**
    - Microsoft Network Client: Digitally sign communications (always) - **Enable**

    - Microsoft Network Client: Send unencrypted password to third-party SMB Server - **Disable**
    - Microsoft network server: Digitally sign communications (always) - **Enable**
    - Network Access: Allow anonymous SID/Name translation - **Disable**
    - Network Access: Do not allow anonymous enumeration of SAM accounts and shares - **Enable**
    - Network Access: Let Everyone permissions apply to anonymous user - **Disable**

Disable Services

Unless otherwise stated in the Readme, disable these commonly found services. To disable a service: right click on it > properties > select startup type > select disable. Remember to also select stop service in case it is running. Also look for any new harmful services that could have been added.

You can also view services from msconfig (search it)

Control Panel > System and Security > Administrative Tools > **Services**

- Microsoft FTP Service
- Print Spooler
- Remote Desktop Configuration
- Remote Desktop Services
- Remote Desktop Services UserMode
- Remote Registry
- RIP Listener
- Server
- SNMP Trap
- SSDP Discovery
- TCP/IP NetBIOS Helper
- Telephony
- Telnet
- UPnP Device Host

Windows Features

Disable the following features:

Control Panel > Programs > **Turn Windows features on or off**

- Active Directory Services (Be careful with this one, especially Windows Server versions)
- Internet Information Services
- Media Features
- Print and Document Services
- RIP Listener
- Simple TCP/IP
- SMB
- Telnet
- Work Folders

Remove Malicious/Unwanted Software

Control Panel > Programs > **Programs and Features**

- Check all programs and remove any that may seem fishy
- Remove programs that are not listed on the Readme file, other than
    - Files to keep(for sure):
        - CyberPatriot Scoring Engine
        - Microsoft .Net Framework
        - Microsoft Visual C++
        - Vmware tools
- Note: not all programs will be listed here, also check C:\ProgramFiles\ and C:\ProgramFiles(x86)
- CHECK APPDATA as well for hidden malware/files

Miscellaneous Items

- Update browser: Firefox
    - Go online and install the update, google how to if you do not know
- Search User Directories for “non-work related” media files
- Check if there are any folders/files being shared on the network
- Update any programs that should be on the OS
- Check Event Viewer and Task Scheduler in Administrative Tools
- Check Task Manager
    - Can start from Ctrl+Alt+Delete
    - Services tab
        - If it doesn’t have a description, that is a red flag