CPU - Windows Attack Plan

Pre – Competition

- Download and transfer images to all computers.
- Have unique ID and password to extract images ready
- Make sure all computers are up to date
- Make sure there is enough storage space in hard drive
- Download any software needed. (service packs, antivirus, antimalware)

Competition

- Give VM a ram boost (2-4gb)
- Enter Unique ID
- Read Readme File
- Make note of scored/forensics question (answer these 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
Write down every change you make that gives you points. This is just in case you need to restart your image.
DO NOT disable CyberPatriot Scoring Engine

User Accounts

- Create/Change password for all accounts (Admins,Standard)
- Make sure all user accounts are in their respective groups
- Disable all user accounts not authorized
- Disable guest account if not stated in readme file.

******

Tip

Managing user accounts can all be done under computer management.
Use this instead of control panel
To access Computer Management use:
Search bar in start menu and type: Computer Management
Press Windows Key + R and same time and type compmgmt.msc in the run box.

******

Background Tasks

- Start Automatic Updates
- Install and run any software needed (antivirus, antimalware, service packs)

Quick and Easy Tasks

- Bring up Firewall
- Enabling Automatic Updates
- Disabling startup services/tasks

This can be done under msconfig. Can be found by typing msconfig in search bar under start menu.

****

Tip

To bring up firewall, go to control panel > system and security > windows firewall > use use recommended settings

To Enable Automatic Updates, go to control panel > system and security > Windows Update > use recommended settings (download and install automatically)

******

Local Security Policies

Remember: 50% of issues will be within Local Security Policies if not more

Do not spend all your time going over all the settings in one sitting. Go over the ones listed here first then come back later if you have time left or if you don't know what to do

- Account Policies:

  Password Policies
  Password History: 5
  Max Age: 30
  Min age: 1-10
  Pass Length - 8
  Complexity Req. - Enabled
  Reversible Encryp. - Disabled

  Account Lockout Policies
  Lockout Threshold - 5
  Lockout Duration - 30 min
  Lockout counter reset - 30 min

- Local Policies

  Audit Policies - turn on success and failure for all of them

  Security Options

  More than often this is where teams miss issues needed to be fixed
  I will only mention the ones that are critical. It is your job to go through every Setting carefully and enable or disable a feature.

- Account: 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

******

Tip

Local Security policies can be accessed by typing:
Local Security Policies in the start menu search bar
Pressing Windows Key + R and typing secpol.msc in run box
Look for Security Policies that have been disabled. Often times these have been changed. Read carefully what each policy does and think carefully whether or not the setting it is on is secure.
******

Disable Services

Unless otherwise stated in readme file disable these commonly found services:

- Microsoft FTP Service
- Print Spooler
- Remote Desktop Services
- Remote Registry
- Rip Listener
- Server
- SNMP Trap
- TCP/IP NetBIOS Helper
- Telephony
- Telnet

****

Tip

To access services:
Type services in search bar under start menu
Press Windows Key + R and type services.msc in run box

To Disable Services:
Right click a service > select properties > select startup type > select disable
***Remember to also select stop services in case it is running. Disabling the services on its own is not enough**
******

Windows Features

There are certain windows features that can pose security risks. Other are unnecessary and should be disabled unless otherwise told.

- Active Directory Services
- Internet Information Services
- Media Features
- Print and Document Services
- RIP Listener
- Simple TCP/IP
- SMB
- Telnet
- Work Folders

Remove Malicious/Unwanted Software

- Check all your programs installed and remove any programs that may seem fishy
- Remove Programs that are not stated on Readme file other than:

CyberPatriot Scoring Engine
Microsoft .Net Framework
Microsoft Visual C++
Vmware tools
****

Tip

To view list of installed programs:
Type uninstall program in search bar under start menu
Not all programs will be listed in this menu. Some programs you have to search for yourself.
They can be found under C:\ProgramsFIles\, C:\ProgramFIles (x86)\
****

MISC. Items

- Search User Directories for “non-work related” media files
- Check and see if there are any folders/files being shared on the network
- Update any programs that should be on the OS

What to do if you are stuck?

- GOOGLE! Search things such as: Windows hardening checklists, how to secure windows etc
- Take a break! Competition can be stressful.
- Ask your team for help.
- Remember, the team is only as good as how well we have documented our notes and how well we communicate between each other.
- Do not be afraid to ask questions.