Windows Ten CyberPatriot Comprehensive Checklist

Some things to do before doing the checklist:

First things first: download the images onto your pc. From there, unzip them using 7zip (or you can find a forked version called p7zip if your on linux) (it's fun to race and see who's computer gets done unzipping them first). Then, once everyone is ready, open them up in VMWare.

After this: enter the UID and began. But before you do anything, READ THE README UNTIL YOU HAVE IT MEMORIZED. If anything in this checklist goes against the readme, DO NOT DO IT. So once you have the readme memorized, do the forensics questions (do them first, because if you don't, you might break them. Ex. What backdoor is listening on a certain port? If you've already closed this port, then you can't answer the question. So do the forensics first so you can answer them and not be sad).

And lastly: the images can have small things that are not in the checklist that only they have (example: in one round, the security policy was really screwed up, unlike normal times), so make sure to get these done too, as they can have a lot of points in them.

And a quick note: the rounds get much harder as they go along, and it will show. The image will be more and more screwed up and the points and forensics will be harder and harder.

Another quick note: make sure that you make the user use Control+Alt+Delete to open the pc up.

P.S. This checklist is in no particular order (except for updates; do those last), so go at your own pace.

Things That Are Covered:

Users And Passwords For The Users

The first thing to do is take another look at the users in the readme. Kill the ones that aren't allowed and make sure that the ones who are are activated and have a password.

After this, put the users in their proper place (the readme will tell you who goes where; put the admins in the admins group, put the commoners in their place in the common pleb group).

Then, give the users all Str0ng_P4ssw0rds! In general, to make sure a user has a Str0ng_P4sw0rd!, make sure that you use r@nd0m_$1gns and that it is at least 8 characters long, wItH PleNtY oF CapiTal LettErS iN It. $0, 4_3x@mp1e, a Str0ng_P4ssw0rd! W0u1ld L00k lIk3 Th1s.

Now it's time to make a nice password policy. Go to Control Panel -> Administrative Tools -> Local Security Policy, -> Account Policies -> Password Policies.

Make sure the Password Policy says these things:

- Enforce password history - 5
- Maximum password age - 90 user 30 admin
- Minimum password age - 10-30 days
- Minimum password length - 8
- Password must meet complexity requirement - Enable
- Store password using reversible encryption - Disable
- Account Lockout Duration - 30
- Account lockout threshold - 3-10
- Reset account lockout counter after - 30

Good job, now you passwords are Str0ng_P4ssw0rds! and secure policies around them.

Event Logging

This is the event logging section. One of these is Event Viewer, which views events (duh) and records them. This helps for finding things that you normally wouldn't find. Here is how to set this up:
Account logon events: Attempts to log into system accounts

Account management: Account creation or deletion, password changes, user group changes

Directory service access: Changes to shared resources on a network

Logon events: Attempts to log into a specific shared computer

Object access: Access to sensitive, restricted files

Policy change: Attempts to change local security policies, user rights, and auditing policies

Privilege use: Attempts to execute restricted system changes

Process tracking: Attempts to modify program files, which have rewritten or disrupted program processes (helps to detect virus outbreaks, since viruses do this)

System events: Computer shutdowns or restarts

This is under user rights assignments: Access this computer from the network: make sure that "Everyone" is removed.

Go to action center, then control panel -> system security -> action center, windows updates, and enable "install updates automatically

Wall Of Fire (firewall)

The windows firewall, called Windows Defender, is a necessary part of keeping a pc secure. Make sure it's enabled and that it has secure settings (block all incoming traffic and make sure that you can have outgoing connections). Make sure that you also have a good antivirus installed (AS LONG AS IT'S FREE), cause holy moly these find some weird things that you never would've thought of. These tend to slow down the VM a good bit so maybe hold off till the end to do this step if your not already there.

(Edit by Matthew Perrino): Windows Defender is super customizable and modular to suit a user's needs. There are "rules" that can be added to allow for a certain program to pass through or be blocked by the firewall. You can block or allow many things like ports, programs, user configurations, and other stuff.

How to set-up Windows Defender:

1. Click on the search bar next to the Windows Icon
2. Type: Windows Defender
3. Hit "Enter"
4. If the firewall says it's off, then turn it on. Skip this step if the firewall appears "on" with a green square.

How to configure rules:

1. Open Windows Defender with advanced security by typing it in the search box
2. Create firewall rules based the rules required to earn points [Needs more editing for steps]

Securing The Internet

NOTE: Do this in firefox as well as in Windows.

Go to control panel -> internet options, then to the security tab. From there go to the security tab and enable the following:

- Security level: high

Then go to the privacy tab and enable the following:

- Block all cookies
- Never allow websites to request your information
- Turn on popup blocker
- Disable toolbars and extensions when in private browsing

DO THESE STEPS IN THE BROWSER SPECIFIED IN THE README AS WELL

Finding And Killing Bad Services

Sometimes the VM's have some naughty services in them that are stealing your points. To get these points, you must find and kill the bad services and programs. Here is a list of things that help you do that:
And before we go over how to kill processes, here are the two types that you'll wanna kill and remove:
Number one are the kind that are unnecessary and decrease efficiency (spotify, music/video players, etc.), and the second type are the kind that are dangerous (unspecified in the readme remote desktop services or things of the sort), so be on the lookout for both of these types. Now for how to find these wayward processes:

1. View your recourse monitor. See what is taking up the most RAM and the most CPU power (although keep in mind that this is just a single

core and a single gig of ram). If a program or programs are absolutely killing you memory and cpu usage, investigate them.

2. Look at every single thing on your pc. This takes a while, but you will find some interesting things (if the process or program has no description, this is a RED FLAG. If your not sure if it's good or bad, check it on this site: www.processlibrary.com).
3. Sometimes there is just an obvious one lying around that is free points (something like wireshark or angry ip scanner that has a desktop icon)
4. Lastly, check the startup applications area. A lot of bad things will be set to start automatically, so make sure that you look there and kill the bad things.

Finding And Killing Bad Ports

Sometimes, you'll have an open port that shouldn't be open and is exposed. Just as a quick security check, run a system diagnostics and see if it finds anything, then fix what it may or may not find. To check your ports, open cmd and type netstat -aon. When you run this, check the ports and see if any are exposed that shouldn't be. Close the ones that aren't supposed to be open and kill the processes that go with them if you can.

WIndows Updates (AT END)

Now you can update Windows, but make sure that you have enough time for it to update. It takes a while, so be prepared and allocate a long while to this. But don’t update/restart the machine more than three times.

FOR EMERGENCIES WHEN YOU REALLY NEED POINTS BUT CAN'T FIND ANY

THIS IS ONLY FOR WHEN YOU ARE GETTING REALLY DESPERATE AND NEED POINTS BUT CAN'T GET ANY; DON'T USE IF YOU DON'T HAVE TOO.

Here is a list of things to do to get more points if you really need them:

- 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