***DO ALL OF THESE THINGS UNLESS THE README SAYS OTHERWISE.***

***Research defensive countermeasures, and go through operating system settings.***

There are about 4 checklists in total here. The first is the ELITE TEAM MADE! All the others are found online and Ian though could be helpful.

|  |
| --- |
| **Passwords:**   1. **Secpol.msc** 2. **Length, Complexity, History, Lockout** 3. Policies    1. Enforce Password History: 5 passwords remembered    2. Maximum Password Age: 30 to 90 days    3. Minimum Password Age: 5 days    4. Minimum Password Length: 8 characters    5. Password must meet complexity requirements?: Yes    6. Store passwords using reversible encryption?: No. 4. Account lockout threshold!  1. “Security Policy"-> "Account Policies"-> "Account Lockout Policy"-> "Account   Lockout Threshold" 2. Change the setting to a value between 3-10 invalid logon attempts. 3. After setting the value for this setting, you will be prompted to change  “Account Lockout Duration” 4. Change the “Reset account lockout counter after" to 30 minutes each.  5. Apply these values and DAB!   1. All users need to have a secure password    1. 8 characters, letters, numbers, etc   CHANGE ALL USERS PASSWORDS TO: Spoopy\_5car3y |
| **Delete / Disable**   1. Delete    1. Deleted Media files (non-work related files) on all users    2. Deleted unwanted software (hacking tools, not required software)    3. Removing the guest account 2. Disable/Enable    1. Disabled telnet    2. Disabled fttps    3. Disabled vpn    4. Disable netcat    5. Disable remote registry    6. Windows firewall is enabled    7. Turn on windows defender    8. Enabled bitlocker    9. Turning on auto update    10. Make sure that ssh is enabled 3. Remove Unauthorized administrators 4. Remove Unauthorized users 5. Remote Registry!  1. Go to "services.msc"  2. Scroll down and double-click on "Remote Registry"  3. Change the "Startup Type" to "disabled"  4. Click apply and DAB! 6. Install useful stuff (download this beforehand)    1. Security Compliance Manager (<http://technet.microsoft.com/library/cc677002.aspx>) automatically sets those tedious security policies 7. Remove unnecessary Windows features (turn Windows features on or off)    1. Remove games, IIS (Internet Information Services), media features, Telnet, etc. (unless allowed in the readme) 8. Extra Programs    1. ○ Start Menu    2. ○ Add/Remove Programs (Programs and Features in Windows Server 2008)    3. ○ Msconfig – startup tab 9. Remote Access    1. ○ Go through Computer -> Properties -> Remote Settings for CyberPatriot |
| **How to answer most Forensics Questions**   1. How to identify users in any group!   1. Go to "mmc" 2. From the "mmc" window, select File drop down menu  and then “Add/Remove Snap-in.” In the “Available  snap-ins” column, select “Local Users and Groups” 3. Then click the "Add" button. At the "Choose Target  Machine" dialog box, select "Finish" 4. Double click on the new "Local Users and Groups"  snap-in you just added. 5. Then double click on the groups folder and double  click [insert group name here] 6. Look at users and DAB!   1. Change folder options    1. Show hidden files, do not hide protected system files, do not hide extensions |
| **How to do extra things**   1. **File Sharing**    1. **○ MMC -> Shared Folder Snap-In (and remove with right-click)** 2. Steps: to how to get bitlocker Open the group policy editor (gpedit.msc) as admin. Go into the "directory" (left sub-window) "Computer Configuration/Administrative Templates/ Windows Components/ BitLocker Drive Encryption/ Operating System Drives" Open the "Require additional authentification at startup" entry (right sub-window) Set the radio box to "enabled" and check "Allow Bitlocker without a compatible TPM" Optional: Change the cipher strength (128 or 256 bit, difference: 128 is secure for ~50 years and 256 for ~200 years) using the "folder" directly above ("BitLocker Drive Encryption") and the "Choose drive encryption method and cipher strength" entry. Check the enabled and choose your cipher in the dropdown menu. Encrypt your drive as you normally would. 3. **How to show file extensions**    1. **Windows Explorer -> Organize -> Folder & Search Options -> View tab** 4. **Computer Properties**    1. **○ Device Manager**    2. **○ Remote Settings**    3. **○ System Protection/Restore – Not in Server 2008!**    4. **○ Advanced System Settings** 5. **Security Templates**    1. **○ Found in Windows/inf**    2. **○ Three of them**       1. **■ defltbase**       2. **■ defltdc**       3. **■ defltsv**    3. **○ Security Configuration & Analysis Snap-In (SCA)**       1. **■ Create own template for competition** 6. **Removing Rootkits – think SAFE MODE!** |

Action Center

* Any issue it says in action center should be resolved and all of them usually give you points.
* Answer Forensics Questions
* 8. Make sure that needed services are allowed through the Firewall
* Updates (show how to set)
  + ○ Service packs
  + ○ Other OS updates
  + ○ Non-OS updates

1. ==BARF BUTTS ARE NOT ALLOWED!==("definiately not middle school team")
2. Update computer and turn on automatic updates
   1. This may take quite a while. Since you will know your images ahead, it would be wise to download large, important updates such as service packs for Windows ahead of time and bring them in on a flash drive to be installed immediately- these large updates are the ones that will most likely give points. Ubuntu should upgrade to the latest version and update its software. Run updates in the background while you continue on.
3. Turn on User Account Control to the highest security setting. If you don't get points for it within a few minutes, feel free to turn it off because it gets really annoying.
4. Check users (Helpful to do through computer managements -> users and groups in Windows)
   1. Disable Guest account ya
   2. Change all passwords to something secure (8 characters, numbers, caps, symbols, ex. "R!verV13w")
      1. THIS WILL BE “Spoopy\_5car3y”
   3. Make sure only accounts listed as admins in the readme are admins
   4. Disable remote desktop/assistance (unless allowed in readme)
5. Remove unnecessary programs (add or remove programs in Windows)
   1. Remove server software, games, hacking tools, and other forbidden software (unless allowed in the readme)
6. Remove unnecessary services (run -> services.msc)
   1. Anything "remote" except Remote Procedure Call (unless remote desktop/admin is allowed in the readme), Telnet, etc.
   2. If it doesn't have a description, then it's automatically on the chopping block. Search the name, if it's malicious or if nothing comes up then go properties -> general -> path to executable to find where it is running from. If you'll be disabling the service, you would also do well to delete the executable and probably its containing folder(s).
   3. DO NOT TOUCH DNS Client, Server, or anything else that seems essential to run the computer!
   4. Microsoft Security Essentials for basic antivirus
   5. Glary Utilities (<http://www.glarysoft.com/glary-utilities/download/>) has some handy tools in the "advanced tools" menu including startup items, scheduled tasks, a processes list with user ratings (take with a grain of salt), and a software update checker (make sure a specific version of a program isn't required by the readme)
7. Turn on the firewall
   1. Specific ports to block or keep can be found on the [ports](http://riverview-cyberpatriot.wikia.com/wiki/Ports) page.
8. Remove unnecessary shares (computer management- IPC$, C$, and ADMIN$ cannot be removed)
9. Snoop through user files for prohibited files (programs, pictures, videos, music, etc.)
   1. Use wildcard searches to speed up this process- for example, searching for "\*.mp3" will show all mp3 files on the computer. Make sure hidden files are shown in folder options, and make sure "search hidden files and folders" is enabled in the search menu!
   2. One way to find hacking tools such as John the Ripper or netcat is to search for "readme" as these tools usually come packed with one, and it is otherwise an uncommon file name. Searching for .exe's is less viable because of the sheer number included in Windows.
   3. Right click -> open containing folder is your friend!
   4. If all else fails, just manually look through all folders in a user's account folder.
10. Look at the file system in general. The temp folder, program files, and users folders are great places to find unnecessary or malicious files.

*1. '***Document the Readme and all forensics questions:** Ensure that you have created a good record of what the readme is telling you, and what the forensics questions are asking for. **MAKE SURE YOU HOLD ON TO THIS.** Your documentation will not only help you during the competition, but can also help you prepare for future images.

**2. Search for forensics questions answers:** I like to do this first because sometimes the forensics questions deal with malware, incorrect settings, or other items you would change. If you remove malware that the forensics question is asking you about, you're not going to be able to find the answer. This is an easy way to earn points.

**3. Go through the User Accounts section of the Control Panel:** Look through all of the users. Make sure that they are at the level that they need to be at, are adhering to password policies, and are actually supposed to be there. Disable the guest account unless the readme specifically tells you not to.

**4. Set the security policies in secpol.msc:** Go through secpol.msc and set the Password and Audit log settings. They should look something like this:

* Enforce Password History: 5 passwords remembered
* Maximum Password Age: 30 to 90 days
* Minimum Password Age: 5 days
* Minimum Password Length: 8 characters
* Password must meet complexity requirements?: Yes
* Store passwords using reversible encryption?: No.

You should also go through and turn on auditing for failed and successful log-ons while in secpol.msc.

**5. Enable UAC (User Account Control):** Turning UAC up to the highest level is generally a good practice and will earn you points in most cases.

**6. Enable Windows Firewall:** Turning on the Windows Firewall is a requirement in most images. The level of protection for your system may vary, and some exceptions in the firewall may apply. Be sure to check that the firewall is still up periodically after you do it the first time.

**8. Check the Windows Scheduled Tasks:** If you've been experiencing any unexplained settings changing, pop-ups, or any other odd behavior, check the Scheduled Tasks. Look for anything that runs suspicious programs, opens error messages, etc. This is tedious, but is a good way to earn some extra points. Figuring out how often the nuisance occurs is a good way to nail down exactly what scheduled task is causing your problem.

**9. Look at Windows features in Programs and Features:** Look for anything that you know that your computer shouldn't have. Telnet is usually a no-no, but sometimes the Readme tells you to leave it on, or even enable it. Make sure your computer isn't running a web server if it shouldn't be.

**10. Look for junk programs, malware, and hacking tools:** The Programs and Features section of the control panel will display a list of programs that are installed. This is a good place to find programs that you can install for some extra points. Tools like JRT and PC Decrapifier help expedite this process, but there's no alternative to looking for yourself.

**11. Ensure that all required programs are running correct versions:** Note that the latest version is not always the correct version. The readme will usually tell you what version of a program to have.

**12. Enable Antivirus Software:** Free antivirus software like AVG or Avast will do, but it has to be a free trial version for the competition. Scanning the system with MalwareBytes is a good idea, too.

**13. Use Process Explorer to see what's running on your computer:** I could write an article just about this. Look for anything suspicious. Remove. Repeat.

**14. Use Autoruns to see what's running when you first start up your computer:** This will help you locate pop-ups, and speed up start times.

**15. Make sure any important Windows Updates and Patches are installed:** This can be a long and tedious process, so see what you can bring in on removable media to help speed up the process.

**16. Verify that your browser is in good, working, uncluttered order:** Make sure that there are no unauthorized add ons, plug-ins, un-needed toolbars, etc. The process for removing these items varies by browser.

**17. Make sure your image doesn't contain any unauthorized media files:** Things like .mp3, .mov, have to go. Using the Windows search bar (\*.mp3 searches the selected area for .mp3 files) is a good place to quickly find these media files.

**18. Use netstat -a to look for unauthorized ports:** Netstat -a in the command prompt will show you all of the entries and exits going through your computer. Check iana's list of common ports to help decide what you should keep.

**19. Go through everything more than once, and document everything:** Going back through and making sure everything is exactly how you left it and how you want it is a good way to find errors that you might have missed. Documenting everything helps identify errors that you may have caused.

[*http://beastcyberpatriot.wikia.com/wiki/Ed's\_Windows\_7\_Checklist*](http://beastcyberpatriot.wikia.com/wiki/Ed's_Windows_7_Checklist)

CyberPatriot Checklists:

Windows 7:

1. Follow all requirements on the read me file

2. Do all the Forensic Questions

3. Check User Accounts to check proper permissions, password policies are followed, and disable guest account unless told not to

4. Set proper security policies in the Security Audit Tool and secpol.msc:

5. Enable UAC to highest level

6. Enable Windows Firewall

7. Check scheduled tasks for suspicious activity

8. Look for unapproved applications in Programs and Features

9. Look for junk programs, maleware and hacking tools (Search for readme)

19. Remove unnecessary Windows Tools as well

10. Ensure the versions of the software are correct

11. Enable antivirus - Free antivirus like AVG or Avast

12. Use Process Explorer to find suspicious processes

13. Use autoruns when you start up the computer

14. Install important Windows Updates and Patches (Takes a while)

15. Check browser condition (Add ons, plugins, toolbars, etc.)

16. Check for unauthorized media files (search for files like .mp3 and .mp4 and .mov)

17. Use netstat -a in command prompt to find unauthorized ports

18. Make a list of everything fixed and check to make sure

changes are still applied

20. Use the security compliance manager to set policies for you:

EXTRA

6. Read the readme file

7. Update the VM and turn automatic updates on

8. Turn the User Account Control to the highest setting

9. Remove unauthorized programs

10. Disable guest account and make all passwords secure\

11. Only authorized users (Defined in readme) are admins

12. Remove unnecessary services

13. Go through user files to find unauthorized files

14. Disable Ports 21-22 (FTP), 23 (If not a telnet), 135 (Remote connections) and 411-412 (PTP connection)

*(source: cyberpatriot.org)*

* [**Automatic Updates**](http://support.microsoft.com/kb/306525) **-** A feature that allows you to easily and effectively keep your computer up-to-date.
* [**Forensics**](http://www.bleepingcomputer.com/tutorials/tutorial24.html) - A guide on how to determine if your computer has been attacked.
* [**GodMode**](http://www.bleepingcomputer.com/tutorials/enable-godmode-in-windows/) - A special mode in later Windows operating systems that gives you access to a wide range of administrative tasks.
* [**Malware and Services**](http://www.bleepingcomputer.com/tutorials/tutorial83.html)- Information on malware that disguise themselves as legitimate services.
* **Recovery Console** - A boot-up option that can fix startup problems.
  + **[Windows 7](http://www.bleepingcomputer.com/tutorials/windows-7-recovery-environment-command-prompt/)**
  + **[Windows 8](http://www.bleepingcomputer.com/tutorials/windows-8-recovery-environment-command-prompt/)**
* [**Safe Mode**](http://www.bleepingcomputer.com/tutorials/tutorial61.html) - A boot-up option that allows you to run administrative and diagnostic tasks.
* [**SVCHOST**](http://www.bleepingcomputer.com/tutorials/list-services-running-under-svchostexe-process/) **-**  A primer on services and processes in general, and svchost.exe in particular.
* [**Sysinternals**](http://technet.microsoft.com/en-us/sysinternals/bb545021.aspx) **-** A database of system tools developed by Microsoft.
* **System Restore -** A feature that lets you restore your computer to known working conditions.
  + **[Windows 7](http://windows.microsoft.com/en-us/windows7/products/features/system-restore)**
  + **[Windows 8](http://www.bleepingcomputer.com/tutorials/windows-8-system-restore-guide/)**
* [**Windows Firewall**](http://windows.microsoft.com/en-us/windows7/products/features/windows-firewall) - Information on the first line of defense against attacks.
* [**Windows Networking**](http://www.windowsnetworking.com/)  **-** Tutorials on networking in Windows.
* [**Windows Registry**](http://www.bleepingcomputer.com/tutorials/tutorial74.html) - A database that stores the configuration settings for the operating system.

[https://s3.amazonaws.com/cpvii/Training+materials/Unit+Five+-+Microsoft+Windows+Security.pdf](https://s3.amazonaws.com/cpvii/Training+materials/Unit+Five+-+Microsoft+Windows+Security.pdf%5C)

[https://www.princeton.edu/~achaney/tmve/wiki100k/docs/Distributed\_Component\_Object\_Mode](https://www.princeton.edu/~achaney/tmve/wiki100k/docs/Distributed_Component_Object_Model.html)

<http://beastcyberpatriot.wikia.com/wiki/Beast_Cyber_Patriot_Wiki>

<http://technet.microsoft.com/library/cc677002.aspx>

<https://pastebin.com/DKJvxZT6>

<https://technet.microsoft.com/en-us/library/hh987048.aspx>

<https://www.effinghamschools.com/Page/19298>

<https://www.upguard.com/articles/top-20-critical-windows-server-2008-vulnerabilities-and-remediation-tips>