<http://riverview-cyberpatriot.wikia.com/wiki/General_Checklist>

1. Input team ID
2. Reahiw5\td mh za8uyh7hfvnb
   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!
3. Change folder options
   1. Show hidden files, do not hide protected system files, do not hide extensions
4. Install useful stuff (download this beforehand)
   1. Security Compliance Manager (<http://technet.microsoft.com/library/cc677002.aspx>) automatically sets those tedious security policies
   2. Microsoft Security Essentials for basic antivirus
   3. 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)
5. 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.
6. Remove unnecessary shares (computer management- IPC$,  C$, and ADMIN$ cannot be removed)
7. 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.
8. Look at the file system in general. The temp folder, program files, and users folders are great places to find unnecessary or malicious files.

<http://riverview-cyberpatriot.wikia.com/wiki/Ubuntu_12.04>

1. Change passwd on logged in account to secure format 1) passwd argus

2. Authentication section!

a.Install Cracklib 1) sudo apt-get install-cracklib --force-yes -y (DO THIS FIRST)

b. Setup failed login attempts 1) sudo gedit /etc/pam.d/common-auth 2) add line, auth optional pam\_tally.so deny=5 unlock\_time=900 onerr=fail audit even\_deny\_root\_account silent

c. Minimum Password Length & Compositon 1) sudo gedit /etc/pam.d/common-password 2) add line, password requisite pam\_cracklib.so retry=3 minlen=8 difok=3 reject\_username minclass=3 maxrepeat=2 dcredit=1 ucredit=1 lcredit=1 ocredit=1

d. Password History 1) (In same file as above) add line, password requisite pam\_pwhistory.so use\_authtok remember=24 enforce\_for\_root

e. Hashing Algorithm 1) (in same file as above) add line, password [success=1 default=ignore] pam\_unix.so obscure use\_authtok sha512 shadow

3.Setup Password Policy 1) gedit /etc/login.defs 2) change the PASS.. line to reflect the following a. PASS\_MIN\_DAYS 7 b. PASS\_MAX\_DAYS 90 c. PASS\_WARN\_AGE 14

4. Change each user's password type, 1) passwd (username)

5. Lock other accounts execpt your own! 1) passwd -| (username) 2) (optional GUI way) UbuntuDesktop/system/administration/users and groups

6.Remove Argus's password from the GECOS field 1) sudo gedit /etc/passwd

7.Remove Everyone from the admin group 1) sudo gedit /etc/group

8. System Patching 1) sudo apt-get update and sudo apt-get dist-update -y

9. Remove Scheduled message 1) sudo rm/var/spool/cron/crontabs/root

The ports that should be closed will differ from image to image, for example if the image is running a server (that it is supposed to be running!) then the ports the server is listening on must not be blocked.  The simplest thing to do is to make sure port 80 and 443 are not closed as they are needed for scoring, and to close only the ports listed under "Common ports to be CLOSED."

## Ports you absolutely must keep[Edit](http://riverview-cyberpatriot.wikia.com/wiki/Ports?action=edit&section=1)

|  |  |
| --- | --- |
| **Port** | **Purpose** |
| 80 | HTTP |
| 443 | HTTPS |

## Common ports to be KEPT[Edit](http://riverview-cyberpatriot.wikia.com/wiki/Ports?action=edit&section=2)

|  |  |
| --- | --- |
| **Port** | **Purpose** |
| 7 | ECHO (Ping) |
| 25 | SMTP (E-mail) |
| 88 | Kereberos (Authentication system) |
| 137-139 | NETBIOS (Network discovery, printer sharing, etc.) |
| 143 | IMAP (More E-mail) |
| 161-162 | SNMP (Network management) |
| 445 | AD, DS (Group policy) |
| 587 | More SMTP |
| 631 | Internet Printing |

## Common ports to be CLOSED[Edit](http://riverview-cyberpatriot.wikia.com/wiki/Ports?action=edit&section=3)

|  |  |
| --- | --- |
| **Port** | **Purpose** |
| 20-21 | FTP (File transfers) |
| 23 | Telnet (Unless it's a Telnet server) |
| 135 | RPC (Remote stuff) |
| 411-412 | Direct Connect (Peer-to-peer) |