CyberPatriot Windows Checklist

Here are some things you should look out for when you're doing Windows images for Cyberpatriot.

- Always read the Read Me first! It tells you what to do and what not to do, and it can help guide you to objectives as well.
- Do your forensics questions (or at least check them out) next. If you go through other steps before doing these, like removing suspicious files, you might not be able to do the forensics questions later on.
- By the end of the time frame, you should have updated your windows operating system to the newest version. Although you don't have to do this right away, it takes a while to update (these versions are typically pretty old), so you should do this at minimum before the three hours left benchmark.
- A good starting point for fixing up the security holes in your image is the users page in the control panel. Deleting unauthorized users, updating passwords, revoking admin status from users who shouldn't have it, etc.
- Another key thing to do is turn on windows firewall. This might give you points, but more importantly it can notify you of other security holes to patch up.
- Downloading an antivirus, such as malwarebytes, is also a good idea. It can notify you of a large array of security holes, and it can comb through all the files on your computer and notify you of suspicious ones. Be careful to not just do everything it says though: it might tell you to delete important files that will end up losing you points.
- You should make sure that the passwords you enter meet the minimum requirements. What are the minimum requirements? That's for you to set up! Head to control panel\System and Security\Administrative tools and change the settings to:
    - Password History 5 Days
    - Maximum Password age 30-90 days
    - Minimum Password age 5 days
    - Minimum Password Length 8 char.
    - Password Complexity Enabled
    - Reverse Encryptions Disabled
- Next, look at all the programs installed on your system. If there are any sketchy programs, like adware or hacking tools, delete them. If you're not sure if they should be there or not, you can usually google the software to figure out whether it should be deleted or not.
- Repeat this step for files as well. Good places to find sketchy files include downloads, documents, and in each user's personal files.
- Another good place to rack up some points is auditing. Go to Local Policies (you can search this up in the taskbar), go to account policies, and change the settings to:

    - Account Lockout Duration - 30 minutes
    - Account Lockout Threshold - 3
    - Reset account lockout counter - 30 minutes
- Next, go to windows audit policies (this can be found right under account policies), and change the settings too:
    - Audit Logon Events - Failure
    - Audit Account Management - Success
    - Audit Directory Service - ND
    - Audit logon Events - Failure
    - Audit Objects Access - ND
    - Audit Policy Change - Success
    - Audit Privilege use success - Failure
    - Audit Process tracking Success - Failure
    - Audit System Events - Failure