Cyberpatriot

# Attack Plans

Mira Costa High School Cyber Securit y Club

# How to use this guide.

This guide is designed to be a comprehensive breakdown of common ways to earn points during the Cyber Patriot competition in the fall and winter season. It was written by the founders of the club as a means to quickly access one central location for help during the competition.

**Please note:** It is easy to get stuck into the cycle of simply following the instructions without internalizing what is going on. **The goal is to get this process ingrained into your head** so you don’t have to reference this guide. *Please* try to understand **how** and **why** we ask you to do the following steps. You’ll find it more rewarding and will be able to pick up advanced concepts much more quickly.

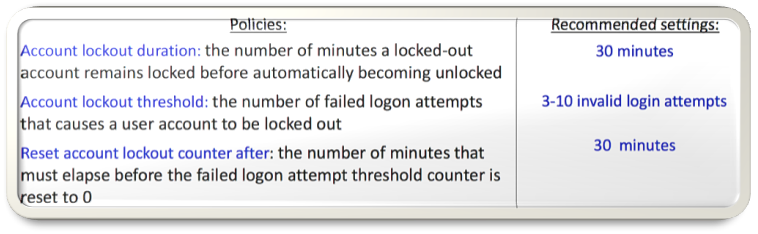
Good luck!

Dave Jha

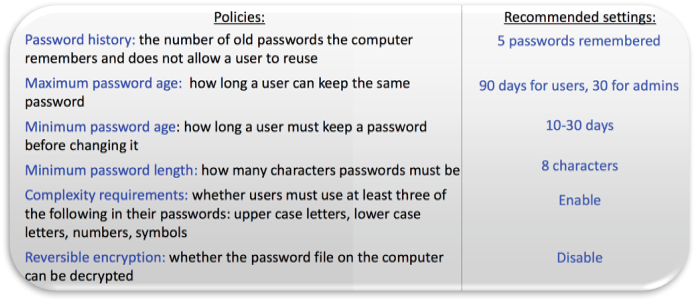
Co-Founder and President, Cyber Security Program (2016-2018)

# Part 1: Windows

1. **Read the README.** It’s pretty obvious, but it’ll tell you all the information you need to know for the following steps. It also might give you hints on what is suppose to STAY on the computer, and what you’re supposed to remove.
2. **Fix the Users**. In the *README*, you’ll find the list of users that are supposed to be on the image. Inevitably, there will be users that don’t belong.
   1. **Go to Control Panel at the bottom left of your screen.**
   2. **Click on User Accounts** (or something like that)
   3. **Cross reference the README users to the User Accounts page.** It might be useful to ask someone to help you with this.
      1. **Delete users in the User Accounts that are not on the README.** Delete their files and directories while you’re at it. Note: It’ll ask you to confirm both of the above actions. Make sure you double check!
      2. **Add missing users in the User Accounts** (based on the README)
      3. **Ensure each user has a password.** For the users that do not, **set their password to “CyberPatriot!”.** DO NOT CHANGE ANY EXISTING PASSWORDS!
      4. **Ensure that each user has the appropriate permissions.** Basically, check to make sure that no users are Admins that aren’t supposed to be and vice versa.
   4. **Turn off the Guest Account**
3. **The Action Center** - where you’re going to get ALL the action (not really). It’s in your Control Panel.
   1. **Uninstall Spyware and unwanted software protection**
   2. **Install an Antivirus software** (WE recommend Avast or Norton Security)
      1. **Run the Antivirus software** in the background and see if it can find any sneaky lurking tasks.
         1. **If it does, delete the program** it originated from and end the process
   3. **Change the settings for Windows Update to daily** (or something like that)
   4. **Turn on the Firewall.** Don’t know what that is? It’s like your front door. You want to make sure it’s closed to strangers.
4. **Local Security Policy** - Search for it
   1. **Go to Account Policies and adjust them to what is below:**



* 1. **Go to Password Policies and adjust them to what is below:**

****

1. **Customize Firewall Settings.** I don’t remember where this is to be honest. It’s somewhere in the advanced Firewall?? Search it up.
   1. **Uncheck all the connections to bad services.** Don’t know if something is bad? Google it. Common bad one: Telnet.
2. **Customize the Audit settings.** You’ll find it under Control Panel → System and Security → Administrative Tools → Event Viewer. Basically, you want to keep logs of everything that happens on your computer so you know what your computer is doing.
   1. **Log Success’ and Failure for each item.**
3. **Go into Task Manager and see what’s up.** You do this by searching Task Manager. Task Manager keeps track of everything running on your computer.
   1. **Go to the file location of sketchy processes.** Right click, file location. Delete it. Don’t know what’s sketchy? Consult your best friend who will get you through anything, Google.
   2. **If applicable, stop the process.** Usually, when you delete the file, it should stop the process. You should double check, though.
4. **Get rid of Media Files.** Media Files are generally prohibited in every competition. These are photos, videos, songs, whatever.
   1. **In File Explorer** (or equivalent where you see all the files) **search “.jpg”, “.png”, ”.mp3”, “.mp4”.** Not all at once, but you will see across the entire system the media files.
5. **Answer the Forensics Questions.** This will always give you a ton of points. There are usually 3 questions, and they’ll give you 5-8 points each.
6. **Go into C:/Program Files/**. You can get here through the file directory. Search for any suspicious programs like web servers and move them to trash.

# Additional Information - Windows

**The following should DEFINITELY not be running:**

* 1. IIS – web server capabilities
  2. NetMeeting Remote Desktop Sharing - VoIP
  3. Remote Desktop Help Session Manager
  4. Remote Registry – allows remote users to edit registry
  5. Routing and Remote Access - allows the system to be used as a router, Simple File Sharing
  6. SSDP Discovery Service – plug and play
  7. Telnet – allows remote users to log on
  8. Universal Plug and Play Device Host – installation of plug and play devices,
  9. Windows Messenger Service – not necessary to use windows instant messenger; allows ‘netsend’ command to be used
  10. **Ftp, Telnet, SSH, VNC, SNMP, LDAP, RDP are evil unless otherwise stated**
  11. **When no centralized maintenance or polling tools are needed, this includes programs with “Maintenance” in the name, EX Mozilla Maintenance Tools**

**Common Policies you may want to change:**

Password History Password Age Minimum Password Length System Events

Password Complexity Requirements Account Lockout Duration Security Settings

Storing Password using Reversible Encryption for all Users in the Domain Policy Change  
  
Account Lockout Threshold Reset Account Lockout Counter Logon Events

Audit Account Logon Events Audit Object Access Audit Process Tracking  
  
Account Management Directory Service Access Privilege Use Security Settings

## USEFUL LINKS:

1. Windows 8 Commands in Terminal: <https://www.lifewire.com/windows-8-command-prompt-commands-2618115>
2. Windows Vista Commands in Terminal:

[http://pcsupport.about.com/od/commandlinereference/tp/windows-vista-commands-p1.html](http://pcsupport.about.com/od/commandlinereference/tp/windows-vista-commands-p1.htm)

1. Windows XP Commands in Terminal:

[http://pcsupport.about.com/od/commandlinereference/tp/windows-vista-commands-p1.html](http://pcsupport.about.com/od/commandlinereference/tp/windows-vista-commands-p1.htm)

1. Windows 7 Commands in Terminal:

<http://pcsupport.about.com/od/commandlinereference/tp/windows-7-commands-p1.htm>

# 