Windows 10 Field Guide 2018-2020 (MKIX)

TKA JROTC Cyber Patriots

C/1LT Perrino

**Intro:**

Windows 10 is an up-to-date, modern operating system from Microsoft, and is used by most people who own a computer. Consequently, people know Windows so well, they hack others and steal private information. As cadets in the cyber patriot program, you will be hardening security inside of a simulator. This document is a how-to-guide on what the United State’s Air Force Cyber Patriot Competition Grading System is looking to see accomplished. The USAF has strict guidelines on what they want from you to gain points, but no fear, this teaches you the basics of Windows 10. First, you need to familiarize yourself with many of these terms in this manual. Any and everything could be used in the tournaments! The whole intent in this is so this becomes muscle memory by the time state comes around.

NOTE: Security is vital! The USAF wants you to do anything to harden the security levels. That ranges from windows updates (only that of permission from a mentor), doing a sweep of every single file (CC Cleaner, Windows Defender).

**Frequently Used Applications:**

There are countless applications on the computer. However, there are a few key ones. They are the Control Panel, Computer Management, MMC, File Explorer, and Local Security Policy. All five of these are vital to navigating the computer. However, the search bar is also useful for looking for these applications. Also, the CMB (Command Prompt) is essential for running specific commands. Keep in mind you may need to hash items. There is a program called WinMD5 which hashes any selected file instantly. The hashes are essential for locating a specific file assigned. Hashing is common in forensic questions.

**Control Panel**

The Control Panel is the hub of the computer. You can change most of the computer’s settings via the control panel. Systems and Security, Network and Internet, Hardware and Sound, Programs, User Accounts, Appearance and Personalization, Clock and Region, and Ease of Access are within the control panel. Then there are different functions under each section. For instance, the firewall settings are under systems and security. Remember, this is an essential space to navigate during a tournament.

**How to use the Control Panel**

Example: Turn on Public Firewall

First, open the Control Panel. Second, locate and open Systems and Security. Next, find the link that says “Windows Defender Firewall.” After you open that link, look on the left for a link that says” turn windows firewall on and off.” Finally, open the link and turn on any the Public Firewall.

**User Auditing and System Auditing**

Auditing is the technical term for monitoring. It is an ability that both you and the computer have. You can audit the computer by checking through the settings, firewalls, etc. However, the computer can also regulate those settings This is where problems begin. You can regulate the computer settings, however, it could accidentally delete an important file, not install an update, or possible leave your computer vulnerable. Auditing can control audit account logons, audit account management, auditing directory service, auditing object access, policy privileges, audit process tracking, and many more. On the bright side, you can fix and manage the auditing programs so you will not have to always monitor that.

**How to use Auditing**

First, open local security policy. Second double click on local policies, third open audit policy. Finally, enable all of the audit programs that were assigned to be enabled. In addition, make sure they all have: success, failure

**Local Group Edit Policy**

The local group edit policy application is a graphical user interface (GUI) friendly program that allows you to disable and enable many policies. As an administrator, this is an ESSENTIAL place to go if you need to disable and enable certain things. This also allows you to manage other’s computers. You can manage: servers, the amount of actions a non-admin can perform, a standard account’s web permissions, and so much more.

*Source: https://www.digitalcitizen.life/simple-questions-what-local-group-policy-editor-how-use-it*

**Third Party Access**

Third party access is the term for when you let certain applications and programs manage and view portions of your account. These applications include apps you use on an everyday basis. For instance, workout apps, mobile transaction apps, certain browsers, and many other apps. These are ways malicious people can rob you of data, private information, or files on your devices. However, this we can decrease these numbers by considering precautions like deleting data or what it will access.

**How to lockdown third party access**

First, go to settings. Second go to the privacy section. Next scroll down on the menu on the left and you will find a section that shows multiple apps. Finally, look under each app and control the amount of access it has on your computer.

**Updates (08/20/2019) [9234 Julian Calendar]**

In the virtual machines, the computer is constantly taking inputs from the user (you. Some inputs may be commands that require it to either update itself. In addition, there are tiny updates that do not require the computer to restart. However, it is annoying to always get a pop-up from an app or from system 32 telling you to update the computer. Instead, take an approach that enables the computer to automatically update itself. Doing this saves time, patience, and can even earn you points

**Manual Updates (07/22/20)**

Despite automatic updates, most downloaded apps that are not a part of the Windows OS will not automatically update. Consequently, you will have to update them yourself. Most apps on the images will not update through an app store, and you will have to manually search for the updates via the internet. When you search for updates, ensure they are RECENT AND STABLE.

**How to enable automatic updates (08/20/2019) [9234]**

First, find the settings app. Second, search “windows update” in the search bar. Next, you will find a link that says, “Advanced options” and click on it. Then, you will turn on “Give me updates for other Microsoft products…” and “Automatically download updates”. Finally, ensure your changes are saved and then close the tab.

**Backup and Restore**

A backup is used as a separate space to store data in case of a sudden data loss in the primary storage. In addition, it is always beneficial to create a backup source just in case of a breach and someone steals your information/personal info.

**How to create a backup storage**

First, open the control panel. Second, you will need select “System and Security”. Next, click on “Backup and Restore”. Then, look on the left side of the screen for “Create a system image”. After clicking on it, select the option, “On a hard disk”. Then, you will need to select a place where the data will go. Finally, press “start backup” and the computer will back your information into the designated space.

**Windows Logs**

Windows Logs is used to “log” what the user changed in the computer’s settings. It is very useful to retrace your steps or to find an error in the computer.

**How to access Windows Logs**

First, type “Windows logs” into the search bar. Second, open the app. Next, you should see four folders. Once, you see the four folders, choose “Windows logs”. Finally, there should be several different child files that will reveal what the computer has done.

**Computer Management:**

Next up is the Computer Management. Computer Management is a program where you will “manage” the “computer.” Remember that phase! In this app, you engage in decisions that could give either points or penalties. The folders in it are Systems Tools, Storage, and Services and Application. These folders are composed of specific applications to harden the security. The folder you use the most is the Systems Tools. This folder is composed of Task Scheduler, Event Viewer, Shared Folders, Local Users and Groups, Performance, and Device Manager. Most of these are not used; however, the most important is the FIRST FOUR. The Task Scheduler allows you to access, view or manually set a task for the computer to carry out. The Event Viewer is responsible for sending notifications when the computer faces a glitch, malfunction, etc. In this app, you can view what is going on behind the scenes while you are using the computer. Next, the Shared Folders. This app allows you to view which files were shared inside the computer. Besides, you can manage who views, opens, or even shares the folder. This is essential for hardening security. Finally, the Local Users and Groups. Any user is displayed here. You can manage the who is on your computer/system, manage their account type, and set passwords for them. The Groups section lists what types of accounts and programs are in your program.

**How to use Computer Management**

Example: Delete the Account “Bobby Broski”

First, type in the search bar, “Computer Management.” Second, open up the computer management application. Next, you look on the left for Local Users and Groups. Then, open that folder up. After you open that folder, there are two folders entitled, Users and Groups. You click in Users to look for Bob’s account. Eventually, you will locate Bob’s account. After you locate Bob’s account, you right-click the account. Finally, you should see a delete button. Press that button, and make sure you SAVE his files in case there are any for future questions.

**Remote Desktop (08/20/19)**

**Firewall Settings**

The Firewall is another vital component inside your computer. The firewall controls what goes in and out of your computer. Two types of firewalls are the Public Network Firewall and the Private Network Firewall. The public network firewall is to protect your computer while you are connected and hides your device to prevent users from getting into your device. Private, on the other hand, does not hide your device because you are on a more secure server. None the less, the USAF Cyber Patriot scoring system always wants these on to harden security.

**Example:**

Turn on Public and Private Firewall

First, type “firewall settings” into the search bar. Second, look on the left and look for a link that says, “Turn Windows Defender Firewall on or off” Next, click the link. Then, there are settings to turn on the firewalls. Finally, enable the firewalls and exit out of the program.

**Firewall Settings Preferences (10/5/19) [9278]**

Inbound:

<Secure Socket Tunneling Protocol>

**MMC**

The MMC is a Graphic User Interface (GUI) that allows the user to run, open, store, and view consols (admin tools). However, not all programs are from Microsoft. The programs can be used to manage the software/programs running. Also, it is ideal for those who want to program their own computer or to create a simple management user-interface. The Cyber Patriot’s simulators rarely need you to go through the program, but it is necessary for altering or deleting programs.

Example:

Delete the program entitled, M@x3d Pr0f1l3

First, key in “MMC” into the search bar. Second, open it. If the computer prompts you to run it, press “yes.” After you select yes, it opens up a window with a folder that called “console root.” Next, browse through the folder until you find a program called “M@x3d Pr0f1l3” Finally, right click it and delete it.

**File Explorer**

Finally, the File Explorer. The File Explorer is for locating any files within the computer. The USAF Cyber Patriot Practice rounds Heavily rely on you to be able to navigate, locate, and edit the files that the ReadMe lists. Also, the Forensic Questions usually have you explore this application. Most of the time, you will be using the file explorer to check for unauthorized files or for documents to trace back to its original owner.

**Example:**

Locate and delete C/LTC Kirschner’s anime files.

First, open the File Explorer application. If it is not on the desktop, then open it through the search bar. Second, find the local disk file. Next, you will open it up and look for a user’s file. Keep in mind, the simulator will hide the file in a place you will least expect, so look through any files you have a suspicion of. Eventually, you will end up locating the C/SSG Kirschner’s file. Next, you will open it and there will be multiple folders. You should open the document folder, but keep in mind it may be in another folder. After a long time of searching, you find the anime folder. Finally, right click it and delete it.

**Local Security Policy**

The best and most straightforward solution to prevent a malicious person from getting into your computer is a complex password. In this file, you will change the security of your computer. All the password settings are under Account Policy. There are two folders listed that are essential to tighten up security. The Password Policy folder contains how the password can be set. This includes many variables like the Maximum Password Age, Minimum Password Age, Minimum Password Length, and Meets Password Complexity Requirements. There are numbers that the USAF Cyber Patriot scoring system looks for. First, for **Maximum Password Age, put 90 days**. Second, **put 30 days for the Minimum Password Age**, Next, type **10 for Minimum Password Length**. Also, enable **meets password complexity requirements**. Then there is the Account Lockout Policy where you can determine how many times someone can type in a password before getting locked out. Three variables are essential for points: Account Lockout Duration and Account Lockout Threshold. For Account Lockout Duration enter 30 for the blank and Account Lockout Threshold put 5.

Maximum Password Age: The maximum amount of days the password is the account’s password

Minimum Password Age: The minimum amount of days the password is the account’s password

Minimum Password Length: The least amount of characters the password can be

Meets Password Complexity Requirements: Makes the password more complex by using forcing the user to add certain characters to their password ex: Password or P@55w0rD

**Example:**

Change the password setting to meet complexity requirements and set the lock-out policy.

First, key in “Local Security Policy” into the search bar. Second, look on the left for Account Policy. Next, open up the folder and select the Password Policy folder. Then, set edit the password settings to the requirements the Cyber Patriot’s requirements. After you set those requirements, go to the Account Lockout Policy. There you set the lockout policies to the standards of the Cyber Patriot’s. Finally, make sure the information is saved and then you gain points.

**File Sharing (last revision 08/20/19) [9234]**

File sharing is a risky program that can come back to harm you if you are not careful. Why is it dangerous? File sharing could reveal your personal info to another server, or you could download malicious software that can potentially harm your computer. You always need to disable File Sharing. **Usually, you will stop sharing for “C:\Users”**

**Example**

Disable File Sharing on the File, “D@nK M3M3S”

First, open Computer Management. Second, look on the left for Shared Files. Then, open “Shares.”. Next look for the “D@nK M3M3S”. Finally, right-click, choose properties, locate the sharing tab, and disable file sharing.

**Windows SmartScreen (11/1/19 [9305])**

Windows SmartScreen is a built-in web filtering system designed to monitor all websites

**Unauthorized Servers**

There are many servers that hackers can use to get into your computer. FTP, Telnet, and TFTP serves are among the most common that hackers use. An FTP server is a backdoor into the computer via file sharing. The way FTP servers work is they use the internet to share the file. However, the file is usually from anonymous people, and they could have malicious intents. For instance, the documents could say they are linked to Red Cross, but you don’t know if they could be linked to a Russian spy. Telnet is another server that is an unknown backdoor in the computer that a hacker uses to their advantage. The reason telnet is insecure is that there is limited security on this server, which allows users to go in and out of it with ease. Consequently, the limited security allows for unauthorized users to view your IP address. Another unsecure server is the IIS server. The Internet Information Services (IIS) servers are the web host systems that send messages through your computer’s ports. Subsequently, this insecure because they take a code that malicious hackers exploit in order to get into your system.

**Example (last revision 08/20/19) [9234]**

Disable FTP, Telnet, TFTP servers, and IIS Servers

First, type windows features into the search bar. Second, open the application. Then, look for a file called Internet Information Services. Next, you double-click it and turn off FTP and telnet servers. After you make sure, those two are turned off, scroll down until you see a file named Telnet Client. Then, turn off the program off. As you continue, locate the TFTP Client, and shut it off. Then, locate LDAP, RDP, SNMP and RIP listener and shut them off. Next, look for the Web Management Tools File. Then, open it. Finally, disable IIS servers and points will be added to your score. Keep in mind, some of these services will appear and some will not, but be vigilant.

**Ports** (08/24/19)

**Write Protection**

Write-protect is a security system used to prevent unauthorized editing or removing/adding a file to a storage space. Today; USB drives, SD cards, and even some hard drives use this security mechanism so that people can not tamper with their disk drives. Windows 10 has one readily available in its programing and must be manually enables by the user.

**Example**

Turn on Write-Protect

First, open the “Control Panel”. Secondly, locate “System and Security”. Then, look on the left of the screen for “System Protection”. Next, find a button under “protection settings” that says “configure”. Finally, select “turn on” and scroll the max usage all the way to 100%.

**Uninstaller App (6/22/19) [Needs more elaboration]**

If you delete a file it may not delete EVERYTHING that came with it. Revo Uninstaller

**Font Types**

Font types are unique types of “print” that are used when writing a paper. Notice the word “unique”. While most fonts are fairly legible, some are cryptic, illegible, and a headache to comprehend. This is what some people use to get a key phrase or password through. Even after decoding a message, the message has to be decoded by you physically. The final product of a decoding program may be “However, if you simply copy it into a document and switch fonts it is”Fornite sucks”. A very simple, but hidden way to get a message across.

**Example:**

The end product of a decoding program is “ “ and it is an incorrect answer for a forensics question.

First, open a blank Microsoft Word Document or Google Docs document. Second, copy and paste the phrase. Next, select the font on the phrase. Then, you will switch the font if it is in “Symbol” to any legible font. Finally, copy and paste the new message into the Forensics Question.

**Commands (last modified: 11-9-19)**

Commands are THE way to get the computer to do the work for you. It is not laziness, but it is simply a fact that a computer can do something faster than you can. By hand, it can take hours to finish something. However, these commands only take a minute to enter and the computer takes a second to accomplish the task. Whether it is commanding the computer to monitor the things flowing in/out ports, to clearing cache, commands are essential tools to make your life a lot easier. Sure, they may be long, but it is not as exhausting as wheeling the mouse around the screen and clicking things. BE WARNED: This requires the precision of a brain surgeon! One simple typo and the command will not work!

* Clearing DNS cache:
  + C:\> ipconfig /flushdns
* Changing passwords:
  + C:\> net user <INSERT USER> \* /domain
  + C:\> net user <USER ABOVE> <NEW PASSWORD HERE>
* Changing passwords remotely:
  + C:\> pspasswd.exe \\<IP ADDRESS or NAME OF REMOTE COMPUTER> -u <REMOTE USER NAME> -p <NEW PASSWORD>
  + PS C:\> pspasswd.exe \\<IP ADDRESS or NAME OF REMOTE COMPUTER>
* Firewall program script (run cmd as admin):

(turning on): Netsh advfirewall set allprofiles state on

**External Sources:**

<https://blanchard.productions/wp-content/uploads/2018/03/CyberPatriot-Windows-Checklist.pdf>

**Ending Remarks (last modified: 03-18-19)**

This field manual is made so newcomers to Windows 10 in Cyber Patriot will have a basic idea of what they will need to be on the lookout for. It is complicated, but it is easy to overcome. I hope you were able to gain something from this manual and good luck on your next competition!

-C/1LT Perrino

ALL items in this manual are taken from the cyber camp at The University of Central Florida, many resources online, Cisco Netacad, Blue Team Field Manual, Red Team Field Manual, instructors, and experiences with Windows 10.