**The Ultimate Windows Checklist**

**Table of Contents**

Page 3: Notes and important things

Page 4: Forensic questions

Page 5: Users

Page 6: Security Policies

Page 7: Windows Defender

Page 7: Windows Updates

Page 7:Program Updates

Page 7: Web Browser

Page 8: File Shares

Page 8: Remote Desktop

Page 8: Unexisting Prohibited and Suspicious files

Page 9: Disabling Bad Services

Page 10: Group Policy

Page 14: Things to check if things aren’t working correctly

Page 15: Remote Desktop

Page 16: Windows Logs Event IDs (Forensics)

**Notes and Important things**

During the competitions, it is important that everyone is ready to open the images at the same time. Otherwise, you might lose valuable minutes because some dumbo opened the image ten minutes before everyone else.

After opening the image and you put in your UID, read the README thoroughly. That is where many hints are for points and it will tell you things that you might usually delete shouldn't be deleted and vice versa. Make sure you know the README very well before moving on to other stuff. If you ever get stuck and have nothing else to do but there are still points out there, go back to the README and see if there may have been anything you missed the first time. Also, if anything in the checklist goes against the README, then DON’T DO IT. You will get points taken away if you do something that the README explicitly says not to do.

Do not only do things that are on this checklist. There may be other things to fix that are not on this checklist. So look out for those things. They also might be hinted at in the README.

The rounds get exponentially harder as you advance, so don’t get frustrated with yourself. Realize that most people don’t know how to do even half of the stuff you know and then move on and do your best.

Sometimes when you get stuck and you can’t think of anything else you can do, grab a buddy and go on a short walk. It will help you get the blood moving and then when you get back to work you might have new ideas of what to do.

And finally, this checklist is in no certain order, except for forensics questions, so do whatever you want first, just make sure you do it all. For forensic questions, do these FIRST, before anything else. Something you do could mess up something for a question and you won’t be able to answer it. For example, once we had to find out the number of bits or something. And if anything was edited, a text document or a user deleted, it would've messed up the whole answer. So make sure you do those first. But if you are spending too much time on them and it's a problem you can’t come back to, let others look at it and if they can't get it, give up. Wasting all your time on one problem isn't worth it.

**USE THIS FOR WHATEVER IMAGE YOU ARE DOING:** https://downloads.cisecurity.org/#/

**For scripts go to Summers’ email and download script and policies (my team only)**

To run script run these commands in an Administrator PS “Set-ExecutionPolicy Unrestricted”

Then do & “C:\Users\<youruser>\Downloads\MediaFileSearch.ps1”

**Forensic Questions**

The forensics questions can be any number of things from cryptography to finding a backdoor. Google will be your best friend when trying to solve these problems. If you don’t know how to do something google it. If you don’t find what you need in one article, look at another one and keep going until you find a good one. One good website for cryptography problems is boxentriq. If you don’t know what type of cipher something is, put it into boxentriqs cipher identifier and then you are good to go. (<https://www.boxentriq.com/code-breaking/cipher-identifier>)

**Users and passwords**

To know what users are supposed to be on the system and which ones aren’t, go back to the README and it will have a list of approved users, which ones should be administrators and their passwords. Control Panel > User Accounts > Manage another account (This is where you can do most of the user stuff)

Deleting Users:

If a user on the system isn’t on the README, you need to delete them. Click on their user in the control panel. Click on delete account, then delete files.

Adding Users:

If you are told to add a user in the README, click on add user, give them the name from the README, give them a strong password, and give them the correct user perms.

Users without passwords or Admin has weak password:

Click on add or change password and give them a strong password with a minimum length of 12 with signs, lowercase, uppercase, and numbers.

Users with wrong account permissions:

In the README there is a list of Admins and a group of normal people. If a user is in the wrong group, then click on their account and click change account type and put them in their place.

Change User Access Control to always notify

**Security Policies**

Windows + R will open run. Type secpol.msc and press enter. Right-click on Security Settings, select import, and import a secpol file you can get from Summers. Before you import the file, export a copy of the current policies so that if you lose a lot of points you can easily get them back by importing the copy of the old policies. If you lose just a few points try to go in there manually and find what is wrong and fix it.

If you can’t get the file from me you can manually change it to these.

Account Policies

Enforce password history: 24

Maximum password age: 90 days

Minimum password age: 15 days

Minimum password length: 12

Password must meet complexity requirements: Enabled

Account lockout threshold: mess with it from 5-10

Local Policies

Audit: Set everything to Success, Failure

Also go to advanced audits and do the same

User Rights Assignments: Look through them and make sure nothing is messed up

Security Options:

■ Accounts: Administrator account status - Disable

■ Accounts: Guest account status - Disable

■ Accounts: Limit local account use of blank passwords… - Enable

■ Devices: Restrict CD-Rom access to locally logged-on user... - Enable

■ Devices: Restrict Floppy access to locally logged-on user… - Enable

■ Domain Member: LDAP server signing requirements - Enable

■ Domain Member: Digitally encrypt or sign secure channel data (always) - Enable

■ Interactive Logon: Do not display last user name - Enable

■ Interactive Logon: Do not require CTRL + ALT + DEL - Disable

■ Microsoft Network Client: Digitally sign communications (always) - Enable

■ Microsoft Network Client: Send unencrypted password to third-party SMB Server - Disable

■ Microsoft network server: Digitally sign communications (always) - Enable

■ Network Access: Allow anonymous SID/Name translation - Disable

■ Network Access: Do not allow anonymous enumeration of SAM accounts and shares - Enable ■ Network Access: Let Everyone permissions apply to anonymous user - Disable

(These are only a few, go to this website to see all of them <https://github.com/Wes-Bl/TKA-Cyberpatriot-Wiki/blob/main/Windows%2010%20Checklist.pdf>)

**USE CIS BENCHMARKS:** https://downloads.cisecurity.org/#/

**Windows Defender**

Windows defender is the windows version of a firewall. Run the virus detection thing.

Make sure no updates are needed. Also, download a free antivirus near the end of the competition (since it slows the computer down).

Here is a free one: <https://www.totalav.com/free-antivirus-software-2>

**Windows Updates**

Sometimes updating the computer will give you points. If you don’t get points the first time, try updating it again. Don’t update more than 3 times. These updates can take up a lot of time so make sure you set aside time for it. Also, tell your team that you are updating so that multiple computers aren’t updating at once. Doing this will make the update go very slowly. Start preparing for the updates near the start of the competition, do this by typing “Windows Update Settings” in the search bar

**Program Updates**

In the README you will be told to keep a web browser and some other things up to date. This means you will have to get the latest update on those programs. To update firefox click on the three lines in the upper right-hand corner, then click about firefox and it should give you an option to update it. The three lines thing might be different for other programs, for example, notepad++ has a ? instead.

**Web Browser**

Most of the time the README will tell you to use firefox as the default browser. In whatever web browser they tell you to use, you have to modify the security settings. Since firefox is usually the web browser used I will tell you how to configure its settings. You can do this by going to privacy and security in firefox.

* Turn on strict
* Always for do not track
* Clear cookies
* Delete cookies
* Turn off autofill logins and passwords
* Enable block pop-up windows and warn when you…
* Turn on block dangerous and deceptive content and warn about unwanted and uncommon software

Do the following in Control Panel > network and internet > internet options to make browsing more secure.

Security tab

* Security level: high
* Privacy tab
* Block all cookies
* Never allow websites to request your information
* Turn on the popup blocker
* Disable toolbars and extensions when in private browsing

**File Shares**

Type computer management in the search bar then go to shared files. Stop sharing all files that it will allow, UNLESS specifically told not to in README. You will lose many points if you stop sharing a file that is supposed to be shared.

**Remote Desktop**

In settings type remote desktop, if it is on, disable it unless told otherwise in the README.

**Unexisting Prohibited and Suspicious files**

Before searching for files, you should turn on “show hidden files.” To do this type “show hidden files” in search, click show settings for “change settings to show hidden and system files”, then click show hidden files, folders, and drives (Any transparent looking files in file explorer are the hidden files).

Prohibited Media files:

In the README it will tell you that non-work-related media files should be removed. To do this go to the C drive in file explorer. Individually search for .mp3 .mp4 .avi .mov .png .jpeg, if any of these look like they shouldn’t be on a work computer, ie. cutecatvideos.mp4, delete it. To filter these files to just ones that end in a certain extension put a \* before the extension (\*.mp3).

Prohibited Games:

Yes, I know it's tempting to try to play these games, and if you are doing pretty well on time and if Sergeant and Mr. Acklen arent in the room, then maybe you could try it out real quick. But, after you try out these games it is a really easy way to get some points. To get those points go to Control Panel > Programs > Programs and Features. Check the box of the unwanted software and click uninstall. If you are not sure whether a program is a game or not, google it. Also, make sure the program files are deleted by going to Program Files and Program Files (x86) in the C drive of file explorer and look for them.

Hacking Software:

To remove these you go to the same place where you deleted the games and uninstall them. And do the same for the files too. Some examples of hacking tools are hashcat, Nmap, Wireshark, Metasploit, putty, and team viewer. And if you see one that you don't know google it and see if it’s needed or not. Do not delete these if you are told otherwise in the README. Also, delete iTunes and CCleaner unless told otherwise.

RevoUninstaller:

User RevoUninstaller to remove any programs that need to be gotten rid of

Windows Features:

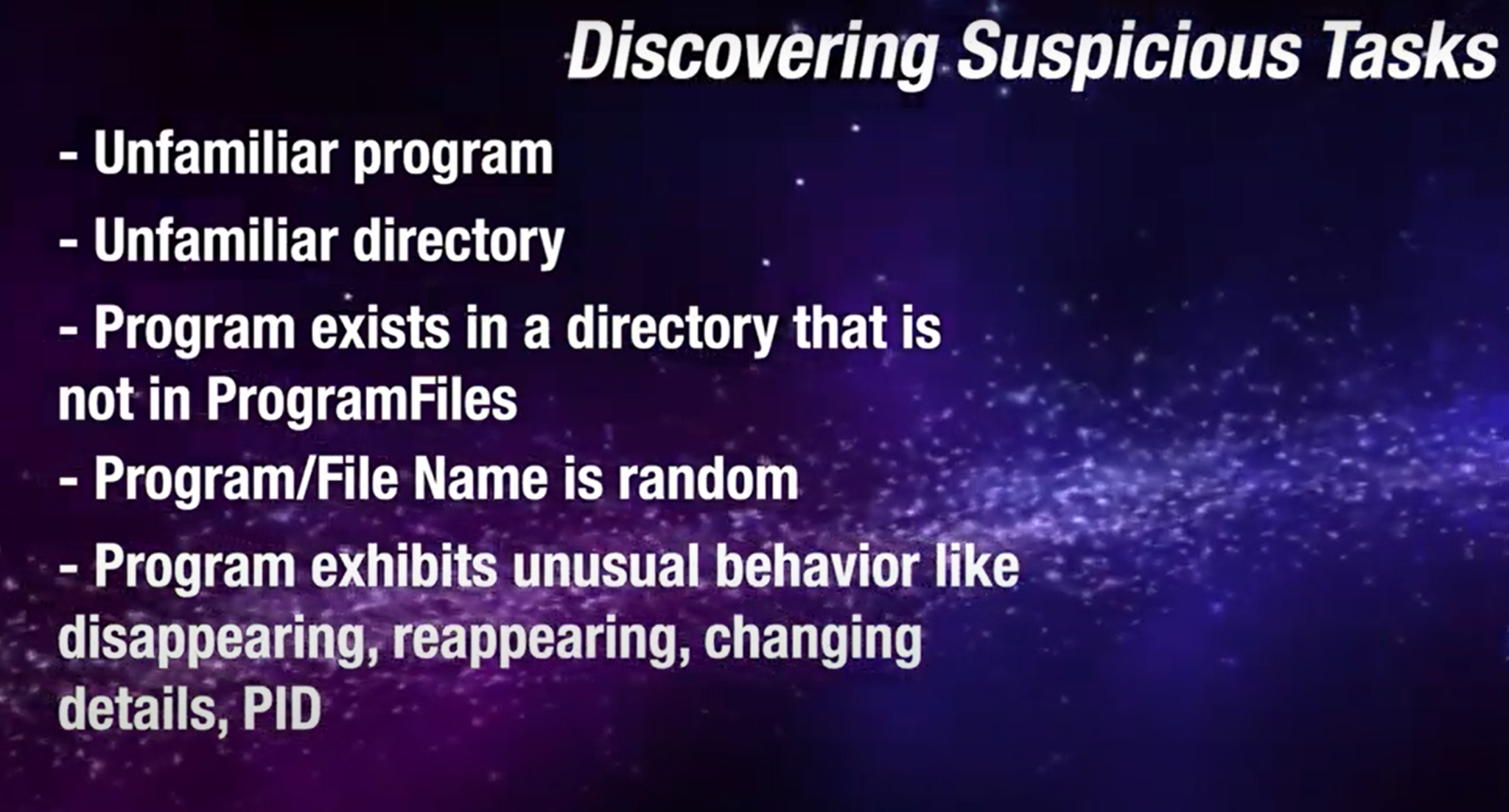
Use Turn on and off Windows Features in Control Panel > Programs > Programs and Features to turn off anything that is not needed

**Disabling Bad/Unnecessary Services**

Sometimes you can get points for disabling bad services. These services can make your computer more vulnerable to hacks. If you want to know more about the services you are disabling google it. Here are a list of some of the services you should disable:

* FTP
* Geolocation service
* IIS
* Microsoft FTP service
* MySQL
* NetMeeting Remote Desktop Sharing – VoIP
* NFS
* Peer Name Resolution Protocol
* Print Spooler
* Remote Assistance Connections
* Remote Desktop Help Session Manager
* Remote Desktop Services
* Remote Registry
* Routing and Remote Access
* RPC
* Simple File Sharing
* Simple TCP/IP Services
* SSD Discovery Service
* Telnet
* TFTP
* Universal Plug and Play Device Host
* Windows Messenger Service
* Any other services that might be specified in the README

**Killing Unknown Processes**

****

**Kill Bad Ports**

Open a command prompt as administrator then type “netstat -aon” this will show all listening ports and their PID's. The port number is the number right after the IP address. Use this website to see if there are any ports you should kill ([https://www.lifars.com/2020/10/are-open](https://www.lifars.com/2020/10/are-open-ports-a-security-risk/)

[-ports-a-security-risk/](https://www.lifars.com/2020/10/are-open-ports-a-security-risk/)). If there are type “taskkill /pid <theportsPID> /f”

**Finding malicious applications**



**Local Group Policy Editor**

To do this go to local group policy editor > Administrative Templates > Windows Components > AutoPlay Policies and then click on Turn off Autoplay and enable this.

Also in Windows Components go to Windows Defender Smart Screen > Explorer and for Configure Windows… click on it and enable it.

I got these from the answer key for the exhibition round so I don’t know if there are more vulnerabilities in Group Policy, but if you have time just look through and research. Or maybe I will do this before comps start, we will see.

**Group Policy**

* While looking through group policy I found something called “Settings Page Visibility” in Group Policy Editor > Computer Config. > Admin. Templates. If objects in settings seem to be hidden (eg. Windows Defender, Windows Updates) check here for something. Edit: It most definitely works. I tested it myself and it is really cool. Look at the help to find out how it works.
* If SMB is a crit service go to Group Policy Editor > Computer Configuration > Admin Templates > Network > Lanman Workstation > Enable insecure guest logons and set to Disabled
* Group Policy Editor > Computer Configuration > Admin Templates > Network > Network Connections > Windows Defender Firewall
* If updates aren’t working check Group Policy Editor > Computer Configuration > Admin Templates > System > Internet Communication Management > Internet Communication Settings > Turn off access to all Windows Update features
* If iSCSI is a crit service go to Group Policy Editor > Computer Configuration > Admin Templates > System > iSCSI
* I don’t exactly know what this does but it has stuff to do with passwords which are important Group Policy Editor > Computer Configuration > Admin Templates > System > LAPS
* Here’s something extra Group Policy Editor > Computer Configuration > Admin Templates > System > Logon >
  + Allow users to select when a password… set to Disabled
  + Turn on convenience PIN sign-in set to Disabled
  + Turn off picture password sign-in set to Enabled
  + Block user from showing account details on sign-in set to Enabled
  + Turn off app notifications on the lock screen set to Enabled
  + Do not display network selection UI set to Enabled
  + Do not enumerate connected users on domain-joined computers
  + Enumerate local users on domain-joined computers set to Disabled (maybe do this near the end)
  + Hide entry points for Fast User Switching (maybe do this near the end)
  + Run these programs at user logon (check this for anything unordinary)
* Group Policy Editor > Computer Configuration > Admin Templates > System > Sleep Settings > Require a password when a computer wakes (both plugged in and on battery) set to Enabled
* Group Policy Editor > Computer Configuration > Admin Templates > System > Trusted Platform Module Service (maybe configure some of the lockout stuff, I haven’t looked too deep into what it is)
* Group Policy Editor > Computer Configuration > Admin Templates > System > User Profiles
  + Do not check for user ownership of Roaming Profile Folders set to Disabled
  + Do not log users on with temporary profiles set to Enabled
* Group Policy Editor > Computer Configuration > Admin Templates > Windows Components > App Privacy (figure out which ones to disable by yourself)
* Group Policy Editor > Computer Configuration > Admin Templates > Windows Components > AutoPlay Policies > Turn off autoplay set to Enabled
* Group Policy Editor > Computer Configuration > Admin Templates > Windows Components > BitLocker Drive Encryption > Fixed Data Drives
  + Deny write access to fixed drives not protected by BitLocker set to Enabled
  + Enforce drive encryption type on fixed data drives set to Enabled
  + Configure use of passwords for fixed data drives set to Enabled
* Group Policy Editor > Computer Configuration > Admin Templates > Windows Components > Credential User Interface
  + Do not display the password reveal button set to Enabled
  + Require trusted path for credential entry set to Enabled
  + Enumerate administrator accounts on elevation set to Disabled
* Group Policy Editor > Computer Configuration > Admin Templates > Windows Components > Delivery Optimization > Download Mode > Set to Enabled with anything but the Internet
* Configure log access and Back up log automatically when full in Group Policy Editor > Computer Configuration > Admin Templates > Windows Components > Event Log Service
* Group Policy Editor > Computer Configuration > Admin Templates > Windows Components > File Explorer > Configure Windows Defender SmartScreen set to Enabled (warn and prevent bypass)
* Group Policy Editor > Computer Configuration > Admin Templates > Windows Components > Internet Explorer > Delete Browser History
  + Prevent deleting download history, websites that the user has visited set to Enabled
  + Prevent access to Delete Browsing History set to Enabled
* Group Policy Editor > Computer Configuration > Admin Templates > Windows Components > Internet Explorer > Internet Control Panel
  + Always send Do Not Track header set to Enabled
  + Check for signatures on downloaded programs set to Enabled
  + Turn on Enhanced Protected Mode set to Enabled
  + Automatically check for Internet Explorer updates set to Enabled
  + Allow software to run or install even if the signature is invalid set to Disabled
* Group Policy Editor > Computer Configuration > Admin Templates > Windows Components > Internet Explorer > Internet Control Panel > Security Page
  + Use Pop-up Blocker set to Enabled
  + Logon options set to Enabled and set to prompt user for name and password
  + Turn on SmartScreen Filter scan set to Enabled
  + Turn on Protected Mode set to Enabled
  + Show security warning for potentially unsafe files set to Enabled
* Group Policy Editor > Computer Configuration > Admin Templates > Windows Components > Internet Explorer > Internet Settings > Component Updates > Periodic check for updates… Enable both options
* Group Policy Editor > Computer Configuration > Admin Templates > Windows Components > NetMeeting > Disable remote Desktop Sharing set to Enabled
* Group Policy Editor > Computer Configuration > Admin Templates > Windows Components > Push to Install > Turn off Push to Install Service set to Enabled
* Group Policy Editor > Computer Configuration > Admin Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Allow users to connect remotely by using Remote Desktop Services set to Disabled ONLY IF RDP IS NOT A CRIT SERVICE
* Group Policy Editor > Computer Configuration > Admin Templates > Windows Components > Smart Card
  + Allow time invalid certificates set to Disabled
  + Allow user name hint set to Disabled
* Group Policy Editor > Computer Configuration > Admin Templates > Windows Components > Windows Defender Antivirus
  + Exclusions (set everything to disabled except Auto Exclusions which should be Enabled)
  + MpEngine
    - Select cloud protection level set to Enabled (High+ blocking level)
  + Real-time Protection
    - Turn off real-time protection set to Disabled
    - Turn on behavior monitoring set to Enabled
    - Scan all downloaded files and attachments set to Enabled
    - Monitor file and program activity on your computer set to Enabled
    - Turn on process scanning whenever real-time protection is enabled set to Enabled
    - Configure monitoring for incoming and outgoing file and program activity set to Enabled (bi-directional)
    - Disable all local setting overrides
  + Scan
    - Check for the latest virus and spyware definitions before running a scheduled scan set to Enabled
    - Scan archive files set to Enabled
    - Scan packed executables set to Enabled
    - Turn on heuristics set to Enabled
  + Signature Updates
    - Check for the latest virus and spyware definitions on startup set to Enabled
    - Turn on scan after signature update set to Enabled
  + Windows Defender Exploit Guard
    - Network Protection > Prevent users and apps from accessing dangerous websites set to Enabled
  + Allow antimalware service to remain running always set to Disabled
  + Turn off routine remediation set to Enabled
  + Turn off Windows Defender Antivirus set to Disabled
* Group Policy Editor > Computer Configuration > Admin Templates > Windows Components > WIndows Defender SmartScreen
  + Explorer
    - Configure App Install Control set to Enabled (Warn me before…)
    - Configure Windows Defender SmartScreen set to Enabled (Warn and prevent bypass)
  + Microsoft Edge
    - Configure Windows Defend SmartScreen set to Enabled
    - Prevent bypassing Windows Defender… set to Enabled
* Group Policy Editor > Computer Configuration > Admin Templates > Windows Components > Windows Installer
  + Allow user control over installs set to Disabled
  + Allow users to browse for source while elevated set to Disabled
  + Allow users to patch elevated products set to Disabled
  + Allow users to use media source while elevated set to Disabled
  + Always install with elevated privileges set to Disabled (do this in User Config. too)
  + Prevent Internet Explorer security prompt for Windows Installer scripts set to Disabled
  + Prevent users from using Windows Installer to install updates and upgrades set to Enabled
  + Prohibit non-administrators from applying vendor signed updates set to Enabled
  + Prohibit removal of updates set to Enabled
* Group Policy Editor > Computer Configuration > Admin Templates > Windows Components > Windows Logon Options > Sign-in last interactive user automatically after a system-initiated restart set to Disabled
* Group Policy Editor > Computer Configuration > Admin Templates > Windows Components > Windows Remote Shell > Allow Remote Shell Access set to Disabled
* Group Policy Editor > Computer Configuration > Admin Templates > Windows Components > Windows Security > App and browser protection > Prevent users from modifying settings set to Enabled
* Group Policy Editor > Computer Configuration > Admin Templates > Windows Components > Windows Update
  + Allow Automatic Updates immediate installation set to Enabled
  + Allow non-administrators to receive update notifications set to Enabled
  + Allow signed updates from an intranet Microsoft update service location set to Disabled
  + Configure Automatic Updates set to Enabled (Auto Download and notify for install)
  + Remove access to use all Windows Update features set to Disabled
  + Turn on recommended updates via Automatic Updates set to Enabled
* Group Policy Editor > User Configuration > Control Panel > Add or Remove Programs set all to not be hidden/removed
* Group Policy Editor > User Configuration > Control Panel > Programs set all to not be hidden/removed

**Things to check if things aren’t working correctly**

* Programs - Group Policy Editor > Computer Configuration > Admin Templates > System > Logon > Run these programs at user logon
* Settings - Group Policy Editor > Computer Config. > Admin. Templates > Settings page visibility
* Updates - Group Policy Editor > Computer Configuration > Admin Templates > System > Internet Communication Management > Internet Communication Settings > Turn off access to all Windows Update features
* Updates - Group Policy Editor > Computer Configuration > Admin Templates > Windows Components > Windows Update > Remove access to use all Windows Update features set to Disabled
* Event Viewer - Group Policy Editor > Computer Configuration > Admin Templates > Windows Components > Event Viewer
* Windows Installer - Group Policy Editor > Computer Configuration > Admin Templates > Windows Components > Windows Installer > Turn off Windows Installer
* Windows Security/Defender - Group Policy Editor > Computer Configuration > Admin Templates > Windows Components > Windows Security

**Remote Desktop**

If Remote Desktop is a critical service here are configurations for Group Policy:

* Group Policy Editor > Computer Configuration > Admin Templates > Windows Components > Remote Desktop Services > Remote Desktop Connection Client
  + Allow .rdp files from unknown publishers set to Disabled
  + Do not allow passwords to be saved set to Enabled
  + Prompt for credentials on the client computer set to Enabled
  + Configure server authentication for client set to Enabled (Do not connect if auth. fails)
* Group Policy Editor > Computer Configuration > Admin Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host
  + Connections
    - Allow remote start of unlisted programs set to Disabled
  + Device and Resource Redirection
    - Do not allow drive redirection set to Enabled
  + Security
    - Set client connection encryption level set to Enabled (High Level)
    - Always prompt for password upon connection set to Enabled
    - Require secure RPC communication set to Enabled
    - Do not allow local administrators to customize permissions set to Enabled
    - Require user authentication for remote connections… set to Enabled
  + Temporary Folders
    - Do not delete temp folders upon exit set to Disabled

**Windows Logs Event IDs (Forensics)**

* 4723,4724 - Change Password
* 4720,4726,4738,4781 - Delete, Change Accounts
* 4608,4609 - Startup, Shutdown
* 4613 - Clear Security Log
* 4616 - Change System Time
* 4617 - Unable to Log
* 4714,4705 - Privilege assigned or removed
* 4708,4714 - Change audit policy
* 4717,4718 - System access granted or removed
* 4739 - Change domain policy
* 16390 - Administrator account lockout
* 4727-4730,4731-4734,4735,4737,4784,4755-4758 - Group changes
* 4624,4636,4803,4801 - Account logons
* 4625,4626,4627,4628,4630,4635,4649,4740,4771,4772,4777 - Logon failures ( KEYWORD: Audit Failure )
* 4672 - Admin account logons
* 4698 - Schedule new job
* 4656 - Access refused to object
* 4664 - Create hard link to audited file
* 865,866,867,868,882 - Software restriction triggered
* 1000 - Application Error ( Event Level: CHECKMARK "Error" )
* 1002 - Application Hang ( Event Level: CHECKMARK "Error" )
* 7031 - Service terminated unexpectedly
* 4697 - Install a Service
* 4663 - Access audited file
* 11707,11742 - Application Install or Uninstall