

Windows Hardening Guide

Made this in highschool for described competition. Made as a guide for my classmates. Take from it what you will but there are some things I would probably change, including the fact that linux security is more fun and probably better knowledge for the real world. Anyways...

Intro (Read me, if CyberPatriot Competitor)

First off, I want to make it very clear that when you sign up for cyber patriot **please** take it as a commitment. If you don't have the time to study and work with your team (nothing wrong with that) I suggest you don't join (you will probably just end up hindering the people that are actually committed). There is a lot of time to commit to cyber patriot, if you want to win I would say 3 - 5 hours a week at least. **If you ever feel like there is nothing to study you probably aren't going to perform very well; there is always something to study. Don't leave it till the last minute!** Team is also very important! Hold your team responsible and make sure they are putting in the effort required to win (if you want any shot at getting a national medal). It is important that you work as a team and everyone has specialties in different areas. Winning nationals comes down to how good you are as a team. Ideally all your scores should be close to equal in the qualifying rounds. If you are behind, ask your teammates for help and study harder. Everyone has it equally as hard as you so there's no excuse, get studying I promise you will see results! Your ability to work as a **team**, achieve as a **team** and ability to **get along** is probably the **single most important thing** in cyber patriot and winning nationals. **I strongly suggest you push each other to get better and have dedicated team practice like you would in any sport.**

About 50% of the stuff you will have to secure (at least in the later images) will come down to your intuition, knowledge on how you would attack one of these images and system administration knowledge. All the stuff here is just for memory, help if you are stuck and to give you a jumping off point of what to study. This will have all the stuff I've seen so far in Cyber Patriot.

This document focuses on how to actually secure things (mostly with windows) but there is also some other things I **strongly** suggest you learn about critical cyber security theory:

- CIA Triad
- Threat model (how to make one, <https://ssd.eff.org/en/module/your-security-plan>)
- Common offensive attacks (usually learnt through ctf's, more on this later)
- Encryption & Hashes (and how to check and get hashes on linux and windows)
- Least Privilege
- Zero Trust
- Attack Surface (most things in this document is reducing attack surface)
- Knowledge of hacking programs and tools (that you can use and what will be used against you. **Also make note of the type of evidence they leave on a system if it has**

been used on it. Can be learned with the help of ctf's. Wireshark and nmap are important)

- VPNs & Tor (maybe, at least a base knowledge)
- Making actual good passwords
- Privacy (maybe. links: <https://ssd.eff.org/>, <https://www.privacytools.io/>, https://www.youtube.com/playlist?list=PL3KeV6Ui_4CayDGHw64OFXEPHgXLkrtJO)

CTFs and stuff like them that teaches you an offensive approach are also very important.

First thing to do is install [Kali](#) on a vm as it is essential for most of these things. The sites I used mostly are <https://www.hackthebox.eu/> and <https://www.vulnhub.com/> (vuln hub is good because you can find solutions online if you're stuck.

Note: A lot of this says to remove remote stuff but this also LARGELY depends if the system is standalone or not. Sometimes you will get an image where it will ask you to allow remote services and it will be up to you to get that running securely.

Most of the stuff talked about for windows can also be applied to Linux. If you are working on Linux take note of what we are preventing with these different policies and settings and apply it to Linux!

Table of Contents

Windows Hardening Guide.....	1
Intro (Read me, if CyberPatriot Competitor).....	1
Team Makeup.....	4
Stuff Missing From This Document.....	6
How To Study.....	6
Before Comp.....	6
VM Configs & Usage.....	7
Start of Comp.....	7
Accounts.....	7
Passwords.....	9
Computer Properties.....	9
Control Panel/Windows Settings/General Stuff.....	10
General Settings.....	10
Action Center.....	10
Windows Defender.....	11
Updates/Patching.....	11
Java.....	11
Internet Explorer.....	11
Device Manager.....	11
Task Manager.....	11
Resource Monitor.....	11
Advanced Windows Configuration (MMC)/Sysinternals.....	11
Task Scheduler.....	12

Server OOBE (Configuration Panel).....	12
Process Explorer (procexp.exe).....	12
TCPView (tcpview.exe).....	12
Sigcheck (sigcheck.exe).....	13
Currports (currports.exe).....	13
Other Sysinternals Programs To Check Out.....	13
Antivirus.....	14
Programs/Viruses/Hacking tools.....	14
File System.....	15
Logs/Auditing/Event Viewer.....	15
Event Viewer info.....	15
How to Find Stuff.....	16
Hardening.....	18
Remote Event Log Viewing/Getting IPs of Computers Connected to AD.....	19
File Sharing.....	20
Searching/File Management.....	20
AccessEnums (accessenums.exe).....	21
Firewall.....	22
Services.....	23
Network/Internet Security.....	25
Securable Services.....	27
Insecure Services (Windows).....	28
A Baseline On Ports (Adding more when found).....	28
User Rights.....	29
Local Security Policy.....	30
Group Policy.....	30
Gpedit.msc (Some Important ones) > Outdated.....	30
Delegation (Access).....	31
Group Policy On Active Directory (gpmc.msc).....	31
CMD.....	32
Help.....	32
netstat.....	32
Saving data to txt.....	32
Dealing with tasks.....	32
Using findstr.....	33
Directory/File Things.....	33
Network Stuff.....	33
User Stuff.....	33
Useful Commands.....	34
PowerShell.....	34
Useful Commands.....	34
Hardening.....	34
SMB.....	34
Registry.....	35

Info.....	35
Hardening.....	35
Hardening Actual Keys.....	36
Remote (RDP Critical Service) Security.....	37
Remote Desktop Settings.....	37
Group Policy.....	38
Firewall.....	39
DNS.....	40
Configuring DNSSEC.....	40
DNS Socket Pool.....	42
DNS Cache Locking.....	42
Access and Permissions and Logging.....	42
Domain Zone Properties.....	43
Make sure IPv6 is Disabled (if Not in Use).....	43
Active Directory (Domain Controller).....	43
How To.....	43
Hardening.....	44
LAPS.....	47
Other.....	47
Secure Firefox!!!!.....	47
Linux Tips.....	47
Tips and Etiquette.....	48
Default Images.....	50
Groups (Win 10).....	50
Resources Helpful In Comp.....	50
Useful Links.....	51
Nationals.....	52

Team Makeup

From my knowledge of how nationals have gone down. I suggest you have 3 people on windows 2 on linux and 1 on cisco. Someone should also study offensive stuff (skills that mostly come from CTFs) if they are keen. Also if the third windows guy also feels the need to dual on linux that is a good idea too. Here is a chart (a good baseline I guess, keep in mind everyone should know the basics of cyber security and I suggest everyone do ctfs)

Person	Focus of study
Windows 1	Windows 10 hardening and security knowledge hard skills Securing Local and Group policies on a standalone system Slim down a system to its bare necessities for the scenario How to secure RDP What services to look out for (what is essential on a system and

	<p>what is not)</p> <p>How to secure Firefox (this comes in handy more and more)</p> <p>Windows firewall knowledge!!!</p>
Windows 2	<p>Windows server hardening and security hard skills</p> <p>How to secure popular critical services (dns, ftp, iis, dhcp etc..)</p> <p>How to use and secure Active Directory (Domain controller, later come round 4 and nationals)</p> <p>Securing Local and Group policies for a server system (domain controller or member server)</p> <p>What services to look out for (what is essential on a system and what is not.. What should be running in services.msc and what should be installed)</p> <p>Setting group policy knowledge (over AD, in depth)</p> <p>Windows firewall knowledge!!!</p>
Windows 3	<p>Digital forensics</p> <p>Puzzle solving and attention to detail</p> <p>How to interpret logs and what to look for in logs (You can export to .csv and search them in sheets)</p> <p>Scanning networks and finding suspicious activity</p> <p>Offensive knowledge (know what hacking tools leave behind and what type of attacks you would use on for example a windows DNS server. Can also transfer this to linux if have the time)</p> <p>Knowledge of encryption and how to check hashes</p> <p>Maybe: knowledge of wireshark</p>
Linux 1	<p>Ubuntu/Debian security and hardening hard skills</p> <p>Comfortable and familiar with linux (i.e knowing useful commands you would use daily on linux, uses it as main os perhaps)</p> <p>Knows how to secure and harden file permissions</p> <p>Offensive knowledge (in depth, see ctfs!)</p> <p>Checking linux logs, linux forensics</p>
Linux 2	<p>How to secure Linux critical services (ssh, web server (apache), etc..)</p> <p>Comfortable and familiar with linux (i.e knowing useful commands you would use daily on linux, uses it as main os perhaps)</p> <p>Offensive knowledge (see ctfs!)</p> <p>Knowing how to secure daemons and what is needed and what is not</p> <p>Knowledge of fedora (security, hardening, how to use, more into nationals)</p> <p>Checking linux logs, linux forensics</p>
Cisco	<p>Hard skills on making networks in cisco packet tracer (going through the provided cisco modules, has to be a big studier!)</p> <p>In depth knowledge of network security</p> <p>How to configure a firewall (an actual firewall!!!!) security and reduce attack surface (important for nationals)</p>

	Knowledge of wildcard stuff if has the time at least a foundation knowledge of an os of their choice.. You will learn some offensive tactics through your training that are good to apply.
Wildcard (important sub bits of knowledge)	Encryption & Hashes Securing firefox (shows up on both linux and windows very important) Use of wireshark and nmap (or other useful tools, everyone should know and at least one in depth i.e interpreting dump files if you want to win nationals)

Stuff Missing From This Document

- How to secure firefox
- IIS, FTP, DHCP
- Making scripts
- Wireshark and Nmap

How To Study

I find a lot of times people don't know what to study or where to get started. Really what you want to do is start with something broad and then if you don't know something learn about it. For example just look up "[your OS of interest] hardening guide/checklist" see what they are securing and learn about it in depth. Also check out my team make up chart. It has some good starting points. Also CTFs are strongly suggested, if you need a change of pace!!. If you are on windows I would say this document is a good starting point.

In short:

Start broad then boil down until you understand (know the what the why and how of every point you shouldn't be confused on anything) in your broad search.

Also join the cyber patriot discord and if you see something you are confused about study it (i.e people talking about it)!

Also don't be afraid to ask and build a relationship to your seniors. Honestly I wish younger teams talked to me more :(. On that note if you have any questions or want any help shoot me an email at sudosaturnrobot@protonmail.com.

Before Comp

Download updates (like the update files), usually cyber patriot will outline before the comp what updates will be needed. Just stick them on a usb and run them at the end of your point getting, or when you take a break. (Q: Save a heck of a lot of time and sometimes your updates just wont work through windows settings, so it is good to know where to get them and how to search for the update you are looking for)

Usually the main difference between a normal windows image (like windows 10 or something) compared to a server image is that a server has to be more secure. As it will have clients using it.

Create your own LGPO's and GPO's and then apply them using LGPO.exe. This will give lots of points. Make sure to have different ones for domain controllers, rdp, standalone and any other critical service specific ones you want to prepare for.

VM Configs & Usage

I usually give the image more than half the ram on my main PC (Leaving some left obviously for main functionality) and hopefully 2 cores if i have 4 cores in my system.

Use VMWare as part of your practice so you get used to using it

Install VMTools (Player > Manage > Install VMTools > Run Install Media In VM). You're welcome.

Make sure you have enough hard drive space for the comp image.

Start of Comp

Creating a system restore point on the vm is a good idea. I would make one at the start and after main point gain. Make sure you screen grab points before you load a restore point.

DO FORENSICS BEFORE ANYTHING (you could delete something important)
Get a sheet and pencil/pen ready!

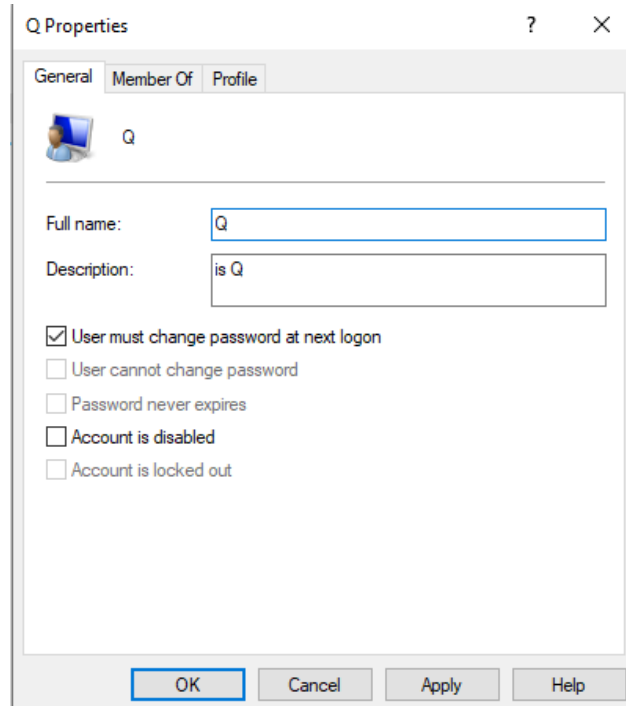
Good luck!

Remember when doing ANY group policy update, run the command `gpupdate /force` or restart

Accounts

- Check who is supposed to be on this PC (README)
- Purge all unauthorized accounts
- Create any necessary users
- Change any account types for users who need it
- Disable both guest and default admin)
- Delete or disable non authorized admin accounts (disable being the better option)
- Change any insecure passwords
- Make sure every user has a password (default guest & admin too?)
- Check group memberships
- Change default account names (not for CyPat)
- No auto login (Umm, actually it is oK)

- Check every users properties (in computer management or mmc)
 - Should look like:



Check groups and look for ones that shouldn't exist (just like users). Some groups actually hint at things that shouldn't be on the system, like remote users. I would go through and inspect things before deleting a group.

Check users properties, and change their settings. Make sure everything is unchecked, unless the account needs to be disabled, or locked out (anything practical). Usually I make sure that the user must change their password on next login because usually this gives password points and it is an extra layer of security for you knowing that the password has been changed AND the user will have to change the password (within your password policy of course).

Notes

Most if not all of this stuff can be done through computer management or mmc, if I see you in the windows 10 settings changing passwords I will be disappointed Just know how to use the program, changing passwords for users using computer management (or mmc) and changing settings in the properties drop down window.

I usually double check the groups to see if everyone is where they are supposed to be. I remember getting points once for removing a user from a group they weren't supposed to be in (that wasn't administrator or user).

Checking access rights in groups is also a good idea. Make sure a user has all the restrictions it should have. Make sure they don't have any privileges they shouldn't either. Same with any other group including admins.

Scripts are also good ;)

Some passwords I use: @f0r7n1t3@, J0k3rg@m3r, B&n&n&_T3xtur3

Passwords

- Secpol.msc (Length, complexity, history and lockout)
- Check password usage

Recommended (Account Lockout Policy):

Account lockout duration	30 minutes
Account lockout threshold	5 ~ 50 invalid logon attempts
Reset account lockout counter after	30 minutes

Note: Please write down your password so you don't fall victim to your own policies

Recommended (Password Policy):

Enforce password history	5 ~ 24 passwords remembered
Maximum password age	30-90 days
Minimum password length	8 ~ 10 characters
Minimum password age	15 days
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Notes

Usually passwords for administrators are different, for example it is usually good practice for administrators to have passwords at 14 characters long and a password age of 30 days. But as far as I know CyPat doesn't look for this.

Computer Properties

- Device Manager
- Remote settings (remove remote desktop and assistance)
- System Protection
- Advanced System Settings
- Computer does not stay awake (check power options)
- msconfig

Notes:

Securing remote settings can be more than just flipping a switch in settings. Powershell and SSH have remote access settings that should be locked down. Remote services and ports should be checked for.

Control Panel/Windows Settings/General Stuff

Anything that is disabled and doesn't turn on... throws an error or just doesn't work, the related service is probably disabled. The first thing I would do if this happens is to enable the service that is related to the thing that is not turning on.

General Settings

- Make sure smartscreen is turned on, and set it to the highest setting. (located at System and Security > Security and Maintenance > Change Windows SmartScreen. If not there go to Windows Security (app in windows 10, replace windows defender and go to App and Browser Control).
- Windows security app
 - Virus & Threat Protection
 - Turn on all types of protection (in threat protection settings)
 - Check for updates
 - Turn on: Ransomware Protection > Controlled Folder Access
 - App and browser control
 - Check apps and files (Block or Warn depending on system)
 - Smart Screen for Microsoft Edge (Block)
 - Smart Screen for Microsoft Store (Warn)
 - Isolated Browsing (Install it)
 - Exploit Protection > System Settings > All On. Check program settings for anything sketchy or unnecessary.
 - Device Security
 - Core Isolation (On)
 - Device Health (Check it but it almost never has leads)
- Privacy Settings
 - All things off

Action Center

- Check it
- Change UAC to HIGHEST ULTIMATE EPIC SETTING but if you don't get points move it back down to normal because its annoying as heck.
- Make sure it is on and notifications are on.

Note

I would make sure notifications are on at the start of the competition because it might actually give hints to other flaws.

Windows Defender

- Turn it on
- Put it on highest security
- Check and update definitions

Updates/Patching

- Run updates and restart
- Other program updates (i.e java, notepad++, anything that the README says to keep. Use ninite?)
- Check browser for anything sketchy
- Reset settings on browsers (clear cookies and other settings to default and stuff)
- Enable updates (security updates and updates for other programs)
- Enable automatic updates

Java

- Set its security to highest (If it is allowed, usually is)

Internet Explorer

- Turn on Internet Explorer Enhanced Security Configuration. Go to Add/Remove Windows Programs and turn it on. (In server it will be in the OOBE)
- Make sure it is not a default browser

Device Manager

- Just check it and make sure everything isn't sketchy or corrupt. Drivers hold all the code for hardware components in the computer and there is a possibility that they can be malicious. (This has never yielded results in CyPat)

Task Manager

- Check it. Anything with no description/looks out of place should be inspected. (Also check the details tab and do "Analyze wait chain" to chase any leads)
- Options > App History to view the history of everything that has run since start up
- Check StartUp (look for anything suspicious)
- Check Users to see who is currently logged in

Resource Monitor

- Check it for any suspicious things like programs with high CPU time and resources usage
- Check the network. It will show open TCP connections!!!

Advanced Windows Configuration (MMC)/Sysinternals

Most of this stuff can be found in Microsoft Management Console. Just do WinKey + R and type "mmc"

Get SysinternalsSuite: <https://docs.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite>

Documentation:

<https://docs.microsoft.com/en-us/sysinternals>

Task Scheduler

Check them, if events are being run as administrator (any scripts or something) and location of what is being executed. Disable anything you don't want, like remote things etc...

- Look for tasks outside of the default Windows Tasks
- Look for tasks without a description
- Check file path of what's being executed
- Check the tasks quickly. Do I need this? (is it a remote service, on a standalone system?)

Server OOBE (Configuration Panel)

This is for SERVER images.

- Don't set the time
- IPv6 should be off (unless required)
- Enable automatic updates
- A lot of default windows services are handled here so any add and remove windows program stuff will be taken care of here.

Process Explorer (procexp.exe)

You need Sysinternals for this.

This is great for checking running programs and stuff. It is basically a super task manager. It gives a lot of info on processes running on your computer. Really good to get scope of your computer and checking for any viruses/hacking tools or any other suspicious activity on your computer.

Going to Options > Verify Image Signature also helps a lot with suspicious items. If it does not match the publishers signature, it is probably a faulty program.

Options > virustotal.com is also a good check to run.

TCPView (tcpview.exe)

You need Sysinternals for this.

This shows what things are connecting to the internet. Shows the processes and the ports they are using and much more.

Local Port - This would be the port it is using

Remote Address - This would be where it is connecting to

This will help with a lot of netstat like stuff, makes everything more visual.

Sigcheck (sigcheck.exe)

You need Sysinternals for this. Need to open with CMD

This is for easily verifying files. This just makes the process a lot quicker if you are suspicious of files. You have to go to the directory of this EXE to run it.

Here is the use of the command:

```
Sigcheck <file/directory>
```

Flags:

-e check only executables
-u reports only problems with the files' signature
-v, -vt (use both, please) will check the file with virustotal.com

Examples:

```
Sigcheck -e -u C:\Windows\System32
```

```
Sigcheck -v -vt C:\Users\EpicGamer\Downloads\epicgamer.exe
```

Currports (currports.exe)

Will need to download.

Currports is a lot like TCPview but gives you a lot more control.

Currports lets you: close connections, shows remote info, shows process' path, lets you kill a process that opened a certain port, shows a connection's state and highlights suspicious connections.

Other Sysinternals Programs To Check Out

[AccessChk](#) (accesschk.exe). CMD Application.

- Is like AccessEnum but for checking specific users and groups.

[Autologin](#) (autologin.exe).

- Disable auto login for specific accounts. To turn off auto login hit disable.

[PsLoggedon](#) (psloggedon.exe). CMD Application.

- Shows users logged on locally and remotely (which net session does not)

[Autoruns](#) (autoruns.exe).

- Shows autorunning services and programs. Good for looking for software/services/programs that shouldn't be installed/enabled.

Antivirus

Run scan... look for viruses

Antivirus (windows defender is on)

Notes

I would check the system performance and see how the ram is running. It might indicate a virus running. Also check processes and the task manager.

From what I've read and used at work BitDefender, Malwarebytes and Avast seem to be the best ones. But I rarely use them in CyPat unless I suspect something is up but I can't find it. Just doing an entire scan is all you need to do in CyPat.

Usually I run them as one of my last things if I am struggling for points. I have gotten points from this so it can be worth it to run.

Programs/Viruses/Hacking tools

- Remove unauthorized programs (add/remove programs)
- Hacking tools
- Sketchy programs

Check the task manager and see what is running. Also check performance and see if the computer is running slow (might indicate a virus, anything not in ProgramFiles or Windows directory should be checked out. Also check CPU time, if it has been active since the CPU started it maybe be a backdoor or some other PUP. High network usage is something I've seen also long cpu time. I've heard of a program that keeps changing but I have never seen one like that in CyPat)

Check other programs for viruses. Like bad add ons and the like. I would definitely check the browsers. Often I just reset them completely and check for any PUPs like bad browser add ons. Also check the installed windows features. This is where you can usually get rid of IIS, FTP, Telnet or whatever else shouldn't be there. Disabling media and anything related to that is also good practice but I never got points for it (of course if the README calls for "no media files")

Stuff that should not be uninstalled (don't give points):

- Microsoft Visual Frameworks
- VMWare based programs
- **Anything needed for CyberPatriot (Scoring Engine)**

Some tips on this:

Check programs in control panel (this probably won't show all of them)

Literally just open up the start menu, sometimes they just straight up hide a shortcut in there

Check /ProgramFiles/ and /ProgramFiles86x/

Root around the file system a bit, do this when you're bored or need a break (DON'T SPEND ALL YOUR TIME ON THIS YOU SHOULD KNOW WHERE TO LOOK). Sometimes you might just find something though, even if it's just a hint.

Look for README in search, pretty much exposes all sketchy programs, but not 100%
MAKE SURE EVERYTHING IS STRIPPED AS LEAN AS POSSIBLE. TRY TO MAKE SURE ONLY THE NECESSARY PROGRAMS/PACKAGES/WINDOWS FEATURES/DEFAULT APPLICATIONS ARE INSTALLED

Services/Programs that should be uninstalled (unchecked):

- SMB v1
- Telnet
- FTP (unless stated otherwise)
- IIS (unless stated otherwise)

File System

- In NTFS (all FAT to NTFS)
- Correct drive letter (Diskpart > list volume (verify drive letter))
- Check partitions

Check for proof of ownership and naming of computer (Valid copy of windows?)

Ask Self: Who has access to whatever you're checking (setting, file, group etc...) and What privileges are allowed/denied to this thing

Logs/Auditing/Event Viewer

Always check the logs no matter what. okay?

Event Viewer info

System Log
The System Log records events that are logged by the Operating System segments. These events are frequently pre-established by the working OS itself. System log files may contain data about hardware changes, device drivers, system changes, and all activities related to the machine.
Security Log
The Security Log contains Logon/Logoff activity and other activities related to windows security. These events are specified by the system's audit policy. The security log is the best and last option to detect and investigate attempted and/or successful unauthorized activity.

Application Log

The Application Log records application related events that are installed in the system. This records the errors that occur in an application, informational events, and warnings from the software applications.

Other Important Event Logs

Directory Service Events — Domain controllers record any Active Directory changes.

File Replication Service Events — For File Replication service events; Sysvol changes

DNS Events — DNS servers record DNS specific events

How to Find Stuff

Basically what you are going to want to look for is these event records. (Note: Event ID is important more on that later)

Event Type	Event ID	Location
Logon/Logoff	Windows 10: 4624/4647 Server 2016: 4624/4647	Security
Remote Access Event Logs (Success/Fail)	Windows 10: 4624/4625 Server 2016: 4624/4625	Security
Attempt Was Made To Access An Object	Windows 10: 4663 Server 2016: 4663	Security
A registry value was modified	Windows 10: 4657 Server 2016: 4657	Security
Permissions on an object were changed	Windows 10: 4670 Server 2016: 4670	Security
Attempt to use explicit credentials	Windows 10: 4648 Server 2016: 4648	Security
Special privileges assigned to new logon	Windows 10: 4672 Server 2016: 4672	Security
Account Lockouts	Windows 10: 4740 Server 2016: 4740	Security
New process has been created	Windows 10: 4688 Server 2016: 4688	Security
New user created/enabled	Windows 10: 4720/4722	Security

	Server 2016: 4720/4722	
Attempt was made to reset password	Windows 10: 4724 Server 2016: 4724	Security
Event log service stopped	Windows 10: 6006 Server 2016: 6006	System
Unexpected system shutdown	Windows 10: 6008 Server 2016: 6008	System
Unexpected system shutdown	Windows 10: 1100 Server 2016: 1100	Security
Audit log cleared	Windows 10: 1102 Server 2016: 1102	Security
Networking Events	Windows 10: 4000 & 6100 Server 2016: 4000 & 6100	System
User Plug n Play Event Logs	Windows 10: 6416 Server 2016: 6416	System
GPO edits and changes	Windows 10: 5137/5136/5138/5130 Server 2016: 5137/5136/5138/5130	Security
Security-Enabled group Modification	Windows 10: 4735	Security
Failure to Load Group Policy	Windows 10: 1129	Security
Firewall Rule Changes	Windows 10: 4946/4947/4948/4949/4950	Security
Group changes	Windows 10: 4728/4729/4964	Security
New Software Installation	Windows 10: 11707 & 1033	Application
App Error	Windows 10: 1000	Application
App Hang	Windows 10: 1002	Application
Computer added to AD	Server 2016: 4741	Security

Bigger list: <https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/appendix-l--events-to-monitor>

If you get a forensics question that something happened.. (I.e user is attempting to logon) look up it's event id and find it either by filtering it by the found id or exporting the log to csv and searching it in google sheets. This can really help speed up the process!

Hardening

- Enable logging (firewall, login attempts [Secpol.msc > auditing], shutdown/login logging)
- Enable backing up logs?
- Change log sizes to 20480 kB to 4194240 kB ([Microsoft Recommended](#))
 - Computer Configuration > Policies > Administrative Templates > Windows Components > Event Log Service.
 - Edit Specify the maximum log file size
 - For other logs go to: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog
 - Now you can create a registry policy in Group Policy Management if that method is preferred (This is more for a whole domain of servers but it is good to know)
- Enable DHCP Logging.
 - Event Viewer tree > Applications and Services Logs > Microsoft > Windows.
 - Expand DHCP
 - Right click Operational and go to properties
 - Enable Logging
 - Set size to 4194240 kB
 - Make sure it is Overwrite events as needed (oldest events first).
- Enable persistent time stamp
 - Goto gpedit.msc
 - Computer Configuration > Administrative Templates > System > Enable Persistent Time Stamp
 - Set to enabled

Set KEY_LOCAL_MACHINE\SOFTWARE, HKEY_LOCAL_MACHINE\SYSTEM and HKEY_USERS\DEFAULT auditing to "successful"

What should be checked:

- Set Value
- Create Subkey
- Delete
- Write DAC
- Write Owner

To do this:

- Go to each key in "regedit"
- Right click the key and go to Permissions, Go to Advanced..., Go to the auditing tab
- Select Add
- Set the principal to Everyone
- Set Type: "success" and Applies to: "This key and subkeys"
- Click Show advanced permissions and check what is above.

Notes

Most of the forensic questions will point here (at least later on). Most of the things they point to will be able to be found in the security tab.

The best way to learn about the event viewer is to mess around with it in my opinion.

Remote Event Log Viewing/Getting IPs of Computers Connected to AD

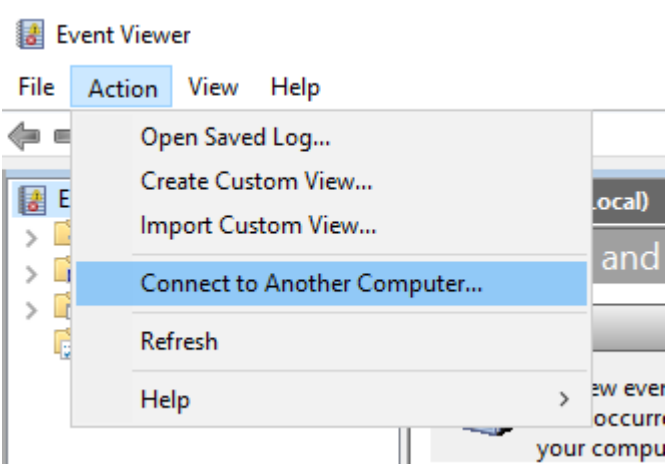
This is good if you are on an AD and want to look at event logs of other computers without having to log into it and look at the event logs that way.

First off you need to get the ips of the workstations connected to the AD. The easiest way to do that using a gui is to go to Server Manager > Tools > DNS. This will list the connected computers and on each one you can left click then select properties and it will display the ip. Or with powershell you can run:

```
Get-ADComputer -Filter * -Properties ipv4Address, OperatingSystem, OperatingSystemServicePack | Format-List name, ipv4*, oper*
```

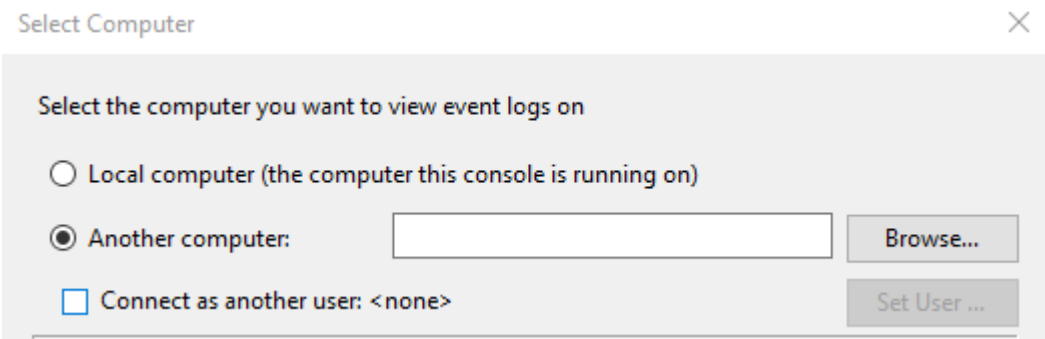
After that open up Event Viewer as admin

Go to Action > Connect to Another Computer...



The screenshot shows the Event Viewer application window. The 'Action' menu is open, and the 'Connect to Another Computer...' option is highlighted. Other menu items include 'Open Saved Log...', 'Create Custom View...', 'Import Custom View...', 'Refresh', and 'Help'. The background shows a tree view of event logs.

Then type in the IP of the computer you want to view



The screenshot shows the 'Select Computer' dialog box. It has a title bar with a close button. The main text says 'Select the computer you want to view event logs on'. There are three radio button options: 'Local computer (the computer this console is running on)', 'Another computer:', and 'Connect as another user: <none>'. The 'Another computer:' option is selected. To the right of this option is a text input field and a 'Browse...' button. Below the 'Connect as another user' option is a 'Set User ...' button.

File Sharing

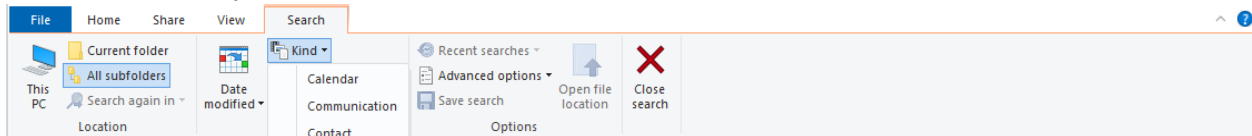
- Go through Computer Management
- Check out the Shared Folders snap in MMC. Check out open shares and the allowed share. This can also be found in computer management.
- Stop sharing in shares folder
- No file sharing between accounts (Check homegroup, network and sharing center>advanced sharing settings)
- Make sure “Everyone” does not have access to each share, restrict it to remote users/administrators

Check Access to SAM File (C:\Windows\System32\Config\SAM)
IPC\$, C\$, and ADMIN\$ in computer management cannot be removed

If you have to have a folder shared check its file permissions make sure it is hardened (i.e Everyone = Read)

Searching/File Management

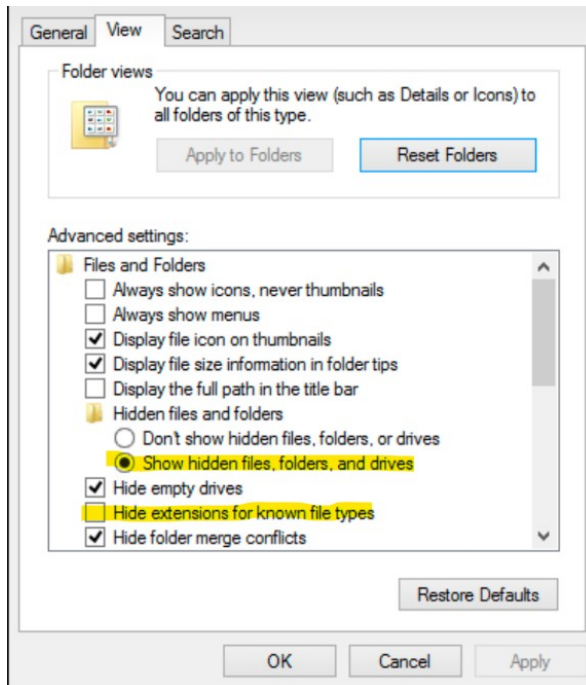
Search tools really help (press on the search bar, and it comes up as a tab, then click kind):



- File extensions in user files (search *.txt, *.png, *.mp3 etc... can also use “kind:”) Files Types (You would be looking for in CyPat):

Music	.mp3, .wav, .m4a, .ogg
Video	.avi, .mp4, .flv, .wmv, .mov, .webm, .mpg
Documents	.pdf, .docx, .txt
Compressed	.zip, .7z, .arj, .rar, .deb, .pkg, .tar.gz
Executables	.exe, .bat (.cmd), .ps1, .jar, .py, .wsf, .bin
Image	.bmp, .gif, .jpeg or .jpg, .png, .psd
Disc/Media	.iso, .vmdk, .dmg, .bin, .vcd

- Turn on show file extensions (hidden and protected files also) Windows Explorer>Organize>Folder & Search Options>View tab
Should look like this (Highlighted what you may need to change):



- Search “README”
- Look through C:\Users\ is definitely a must. Also look through C:\ProgramFiles\ and StartMenu folders Checking C:\ is also good to do, but it will take longer.
- Check users folders (especially for administrators folders, Only the user (whose folder it is), SYSTEM and Admins should have access to their folder)
- Check permissions on Windows folder (Trustedinstaller, SYSTEM and Admins should only have access)

File Permissions Reference:

Read	used to read files and look into the contents.
Write	used to edit and make changes to the file, you cannot Write without Read
Execute	is the ability to execute and operate the program, you cannot Execute unless you can Read

- Turn on DEP for all programs (Control Panel>System and Security>System>Advanced System Settings>Advanced Tab>Performance>Settings>Data Execution Prevention)
- Check startup files (check task manager or even better check Autoruns in Sysinternals). Also check the startup folders:
C:\Users\USERNAME\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
- Check msconfig.exe (check startup and services)

[AccessEnums](#) (accessenums.exe)

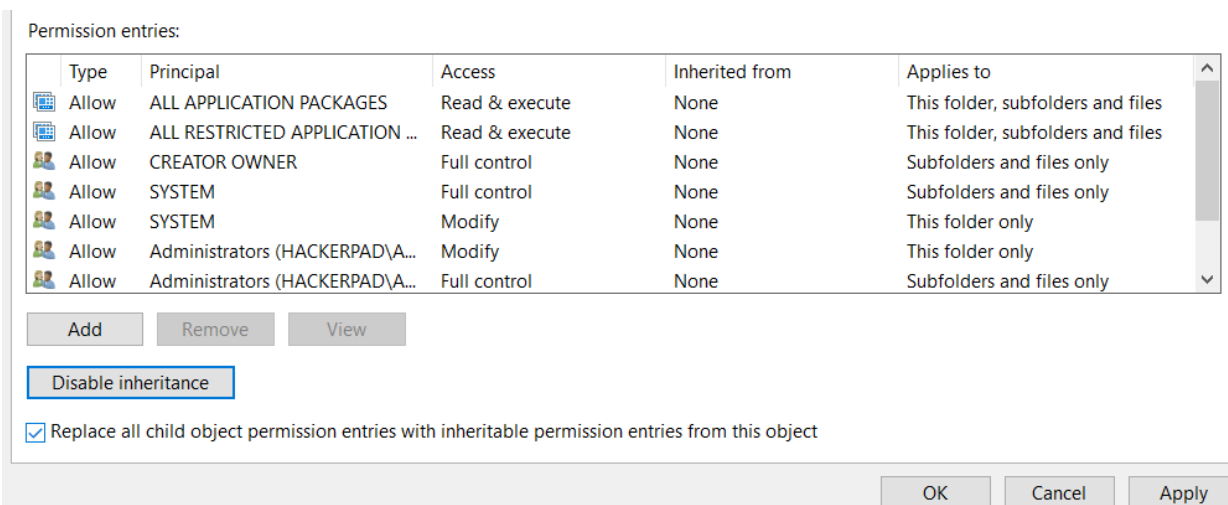
You need Sysinternals for this.

This helps show you the permissions of files and folders. It is really useful to use when checking permissions.

If you see something out of place just Right Click and go to Properties. Then change the security settings in the Security Tab.

Notes

Make sure to enable inheritance so all subfolders and files will inherit the changed you made on the folder.



These changes will take a bit so make sure you have some time to do them

When searching in C:/ windows will have some default files (like media files) I have deleted them in past competitions and got no points. Usually any of these default testing files are located in the C:/Windows/ file and are owned by TrustedInstaller. They are usually just okay to leave. If you search for images here be ready to sort through a ton of icons too.

If someone has access to another person's files/folder they should not be allowed.

If you can't change the permissions on a file/folder, check the owner. If it's not you, that is probably why you can't change anything. You will have to reassign the owner to yourself or "Administrators" to change settings around at this point.

How do I know if something is suspicious?

- Unsigned
- Has a blank description
- Exhibits suspicious behaviour
- No idea what it is even for
- Has a weird name
- Has a long cpu time

Firewall

- Turned on, set on highest security (blocking all inbound ports)

- Adding rules (<https://www.digitalcitizen.life/manage-rules-windows-firewall-advanced-security>)
- How to block ports: <https://www.thewindowsclub.com/block-open-port-windows-8-firewall>
- Logging/auditing (Enable logging in firewall properties)
- Look at programs allowed through the firewall
- All/Most inbound ports should be closed. Only keep bare minimum, whatever is absolutely necessary for anything inbound
- Limit outbound connections as much as possible
- Check for anything unknown or suspicions (in outbound and inbound too)
- Check firewall settings in group policy Location: Computer Configuration > Administrative Templates > Network > Network Connections > Windows Firewall

Use `netsh advfirewall reset` to reset the firewall back to stock settings. But I highly suggest you look through it first for any leads/rabbit holes, or do everything manually. Definitely make a restore point before this (or in the advanced firewall go to Action>Export policy...).

Block bad ports and check for insecure open ones. (Q: I would also check the event viewer, wireshark and netstat and look for activity on ports. Most stuff can be found that way, often can lead to big point gain. Sometimes it will be a random port like 12134 that is being used and connected to, it would be best to close that)

Make sure you know how to also set these settings in a group policy!

Notes

If you want to look more deeply into firewall rules, anything that is empty, has protocols you don't want/need/are insecure, sketchy programs use them, or have remote protocols should be looked into.

Services

Services.msc

- Disable unnecessary services: IIS, Telnet, Web Services, FTP
- Stop Web Server Clients such as Telnet, TFTP & VNC. Turn off IIS (Internet Information Services)
- Disable IPv6 if not required
- Check out add/remove windows programs (either in the OOBE for server or in the Add/Remove programs tab on windows 10)

Stuff to look out for (there are more charts in the resource folder and in the OS specific folders): https://drive.google.com/open?id=1frtjuez2iKWW_pC-AIxKZw5stLfewOEwU7Iblzn6IWk

Service	Notes
---------	-------

DNS Client	If not DNS server (will get rid of scoring)
DHCP Client	If not DHCP server (might get stop scoring from working)
TCP/IP NetBIOS Helper	THIS SHOULD BE DISABLED
Background Intelligent Transfer Service	If auto update is not enabled
Computer Browser	Disable time
Diagnostic Policy Service	Set to manual.
IP Helper	This is used for IPv6 stuff, yeet it if you don't need IPv6
Print Spooler	Printing gone, disable this bad boy. Common example of a redundant service.
Remote Registry	Disable if standalone, you'll usually have to disable this.
Server	If there is no need for file sharing (this will get rid of the \$ shares)
Windows Remote Management (WS-Management)	Disable this dude
Windows Font Cache Service	Disable
WinHTTP Web Proxy Auto-Discovery Service	Disable
Windows Error Reporting Service	Disable. At least for privacy reasons ;)

Remove anything with "remote" (i've got points for this) just don't get rid of Remote Procedure Call. Make sure to check README though, like if it says you need the remote desktop or admin or whatever.

Anything without a description should be deleted, check the properties first and go to the path of the .exe and check if that is sketchy. Look for anything not required to run the system and disable it. Last but not least, check for any services that are unavailable/insecure, disable those too. There's a ton of rabbit holes here, just do it, become services.msc and your mind will awaken.

Windows 8 defaults (<https://www.winhelponline.com/blog/windows-8-services-default-startup-type/>)

Service start-up types reference:

Automatic	Automatically started when the computer is turned on (boots to windows). This is good for things like the firewall and typing.
Manual	When the service is started it will work. It will remain stopped unless it is started.
Disabled	Will never be started. Unless it is changed in services.msc

Notes

Bruh, DON'T TOUCH THE ESSENTIAL STUFF... educate yourself a bit, even though it's boring it is helpful, I put some links below.

I would also get rid of any services not being used (and are therefore not necessary) IPv6 is a popular one for this, I would especially check network services (like IPv6).

It is also good to use `findstr` in cmd or better yet exporting all the services to a text file. Action > Export List... in services.msc to do this. (You can also search status & service type in the applet)

If you want to get to know services open a VM and disable things and see what happens. Maybe even read some of the descriptions and get to know what is what. Making your own list of default services could be a good start.

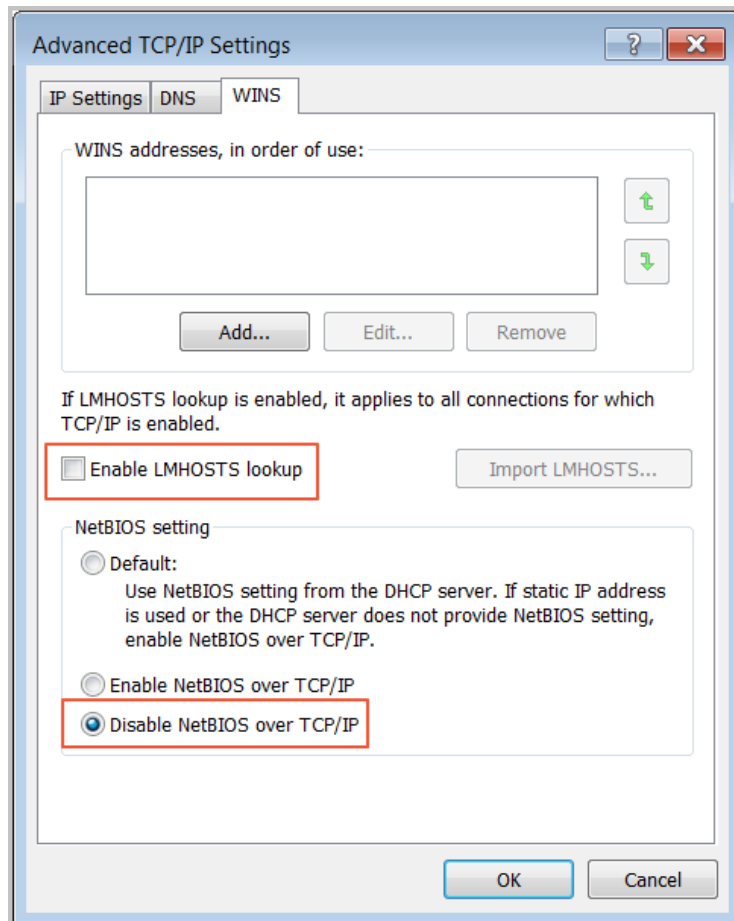
When securing a service or application go through these questions:

1. What is being accessed?
2. Who is accessing what?
3. How are they accessing it?
4. How can it be abused?
5. What can I do to stop them?

Network/Internet Security

- Taskbar - Network icon or Search
- Check Network and Sharing Center
- Advanced Sharing Settings
- Be sure to look at all network profiles
- Make sure C:\Windows\System32\drivers\etc\hosts commented out with '#' (follow any leads, before deletion, if you choose to)
- Go to "Internet Options" and make sure settings check out
 - Reset Internet Explorer
 - HIGHEST (MOST EPIC) security level, protect mode (on all zones)
 - Privacy setting set to highest
 - Never allow websites to request info ON
 - Pop up blocker ON

- Disable toolbars and extensions ON
- Check Connections>Lan Settings..
 - Make sure there are no proxies
 - No automatic script configuration (Automatically detect)
- Use netstat -a (and other netstat commands, wireshark too can help)
- Check network settings and make sure it's set to private
- Make sure the network is not shared in Network and Sharing Center
- look at common list of ports:
 - http://packetlife.net/media/library/23/common_ports.pdf
 - <https://www.tenable.com/sites/drupal.dmz.tenablesecurity.com/files/images/blog/vbcpdashboard.png>
- Disable LMHOSTS (unchecked) and Disable NetBIOS over TCP/IP
 - Network Sharing Center > Click the connection that shows up > Properties > Internet Protocol Version 4 (TCP/IPv4) > Properties > Advanced > go to the WINS tab.
 - Do as follows



- Remove ncaen_ip_tcp.
 - Run Dcomcnfg.exe (Component Services)
 - Select the following: Component Services > Computers > My Computer
 - Right Click and select the Properties menu item

- Select the Default Properties tab
 - Uncheck "Enable Distributed COM on this computer" option.
 - Select the Default Protocols tab
 - Remove "Connection-oriented TCP/IP" from the list of DCOM protocols.
- Remove ncacl_ip_tcp (registry version, use to verify)
 - Run regedit
 - Select the key "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole"
 - Set the value EnabledDCOM to N
 - Select the key HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Rpc
 - Edit the value DCOM Protocols (This may have a bunch of strings)
 - Delete the string ncacl_ip_tcp
- Remove file and print sharing
 - Goto network and sharing center
 - Goto current connection setting
 - Goto properties
 - Uninstall File and Printer Sharing for Microsoft Networks

Notes

Learn how to see suspicious activity when using netstat and make sure to learn the command. I will try to remember to collect pictures as I find a vulnerability in an image here.

I think you can actually check ports through other vms so the win 10 image can ping the linux image. I haven't tried this yet but i'm pretty sure you can do this. Would be a really helpful tool for double checking things and changed settings. I WILL ADD MORE ON THIS LATER AS I TRY IT.

Securable Services

SSH (linux, very frequently shows up, a must study)

SMB (windows, sometimes)

FTP (windows and linux, usually around r2, usually shows up)

Apache, mysql, php [Web Server] (can be windows, will definitely be on linux, usually around r4, securing a web server is a must study for linux people)

DNS (windows and linux, r4, very common, a must study for server people)

RDP (usually win 10 sometimes on early server, win 10 people should study this)

IIS (windows, likely to show up)

If you are doing windows server get familiar with these services and make sure you are familiar and know how to secure them beforehand. They give big points especially in later images!

Look up how to secure critical service outlined in README if you haven't studied or don't know it!

DNS	Port: 53
-----	----------

	TCP & UDP Domain Network System (DNS) is a protocol that enables users and devices to discover websites using human-readable hostnames instead of IP addresses.
SMB	Port: 139/445 SMB, which stands for Server Message Block, is a protocol for sharing files, printers, serial ports, and communications abstractions such as named pipes and mail slots between computers.
FTP	Port: 21
RDP	Port: 3389
Apache, mysql, php	Port: 80/443, 3306, 80/443 Learn by making and securing your own linux image!
SSH	Port: 22 Learn by making and securing your own linux image!
DHCP	Port: 67 & 68 UDP
SMTP	Port: 25, 587 (with SSH) TCP
HTTP/ HTTPS/SSL	Port: 80, 443, 443

Common Trojan Ports:

<https://www.pcsecurityworld.com/75/common-trojan-ports.html>

Insecure Services (Windows)

IIS

SMB

SMTP

FTP (FileZilla)

DNS

RDP

Active Directory (Domain Controller)

A Baseline On Ports (Adding more when found)

MUST BE KEPT

80	Used for scoring and stuff. HTTP
443	Again scoring and stuff. HTTPS

Common ports to keep OPEN (usually just cause errors when closed, and aren't usually insecure or worth points when closed)

7	Echo (ping... pong...)
25	SMTP (E-mail)
88	Kereberos (Authentication system)
137-139	NETBIOS (Network discovery, printer sharing, etc.)
143	IMAP (email but this time only uses central server)
161-162	SNMP (Network management)
445	AD, DS (Group policy)
587	More SMTP
631	Internet Printing

Common ports that should be CLOSED (if not specified otherwise)

20-21	FTP (File transfers)
23	Telnet (unless it says its a telnet server, or has telnet as a critical service)
135	RPC (Remote port)
3389	RDP (remote desktop)
411-412	Direct Connect (Peer-to-peer)
445, 139	SMB (file sharing)

(I will add more as I find them)

User Rights

- Configure user rights to be as secure as possible follow the [Principle of Least Privilege](#)
- Remove Guest, Everyone, and ANONYMOUS LOGON from user rights list
- Ensure IIS is not being run as the System User

- Ensure scheduled tasks are run with a dedicated Service account and not a Domain Administrator account
- Check User Rights Assignment in secpol.msc and secure

Local Security Policy

I made a list:

https://docs.google.com/spreadsheets/d/1p-kz-SRDcM54Y0QDR_719lqx192pvKIAzj24o5hicqc/edit?usp=sharing

Group Policy

gpedit.msc

- Check remote access
- File sharing
- Check for any startup or shutdown scripts in Computer Configuration/User Configuration > Windows Settings > Scripts (Startup/Shutdown)

List: <https://docs.google.com/spreadsheets/d/1K1s4o-LrArtW1BJwNNRcfUwu7JxGoUKRgd3uE-xTh7A/edit?usp=sharing> (took a long time damn)

Gpedit.msc (Some Important ones) > Outdated

Name	Location	Value
Recovery console: Allow automatic administrative logon	Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options	Disabled
Accounts: Block Microsoft accounts	Computer Configuration > Windows Settings > Security Settings > Local Polices > Security Options.	Users can't add or log on with Microsoft accounts
Password protect the screen saver and screen saver timeout	User Configuration > Administrative Templates > Control Panel > Personalization	Enabled
Enable Screen Saver	User Configuration > Policies > Administrative Templates > Control Panel > Personalization	Enabled
Force specific screen saver		Enabled, %windir%\system32\rundll32.exe user32.dll, LockWorkStation
Password protect the screensaver		Enabled
Screen Saver timeout		Enabled - 900 seconds

		Note: This is annoying, so just do it to check if you get points.
Set client connection encryption level setting	Computer Configuration > Administrative Templates > Windows Components > Terminal Services > Encryption and Security	Enabled
Turn on virtualization based security	Computer Configuration > Administrative Templates > System > Device Guard	Secure Boot and DMA Protection Enable with UEFI Lock Enable with UEFI Lock
Restrict delegation of credentials to remote servers	Computer Configuration > Administrative Templates > System > Credentials Delegation	Prefer remote credential guard

Delegation (Access)

Your GPO delegation should look like this unless specified otherwise:

Name	Allowed Permissions	Inherited
NT AUTHORITY\Authenticated Users	Read (from Security Filtering)	No
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Read	No
NT AUTHORITY\SYSTEM	Edit settings, delete, modify security	No
SECURITY\Domain Admins	Edit settings, delete, modify security	No
SECURITY\Enterprise Admins	Edit settings, delete, modify security	No

Group Policy On Active Directory (gpmc.msc)

It is the same as gpedit but you have to select your domain.

It is good practice to split your rules into new gpo policy files when making them. For example every policy should have its own gpo like the screen lockout gpo should have its own group policy object. Stuff like password policy GPOs should just be one group policy object though. Just use common sense.

CMD

Help

Use /? after every command to get more info on it

netstat

Documentation: <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/netstat>

Proto: This is the protocol being used by the connections they can either be TCP or UDP

Local Address: This shows your pc's local ip address (you computer). This is assigned by the router. And the port number being used for this connection.

Foreign Address: This is the ip and port number of the address this connection is "talking" to. This can be your own pc. This is why 0.0.0.0 shows up because it is listening on all network interfaces, this is all local!

State: Listening means it's waiting for a connection, Established means a connection is already made, closed is closed.

```
netstat - a
```

Shows all active TCP connections and all open TCP and UDP ports

```
netstat -ab
```

Shows all active TCP connections (all open ports) and the processes (name) using them

```
netstat -ao
```

Shows all active TCP connections (all open ports) and the PIDs using these active connections

-n will show all the ports as numbers (I add this to all my flags because it just helps incase you don't remember ports and their protocols)

-p protocol just specifies the protocol (i.e tcp and udp), I never really use this.

Saving data to txt

Just do somecommand > Desktop/file.txt (I usually save the file to the desktop, it would be c:\Users\\Desktop if you are in administrator)

Dealing with tasks

Can use task manager for all of this but it is faster through cmd

Use tasklist (lists processes)

Use Taskkill (to kill process, if you want to find it and stop it quickly)

```
/PID 0 /F
```

```
/IM name /F
```

Services can also be accessed with wmic service

Using findstr

Just add `| findstr x` to the end of a command like `netstat` or `tasklist` to find what you are looking for. (replace "x" with a port or a PID).

"|" or pipes are pretty important as they let you run a command immediately after another. They are often useful for other things than just `findstr`.

Directory/File Things

Use `cd` to go to change the directory you are in

`cd ..` is used to go back in a directory

Use `dir` to list the contents of a directory you are in (you can specify one in the command if you like)

Some switches:

`/a` (shows hidden files, pretty useful in CyPat)

`/p` (will pause every screenful, good for large directories)

`/T:A` (time last accessed), `/T:W` (time last written), `/T:C` (time created), `/Q` (file owner) are also useful for CyPat.

`sfc /scannow` will check for any bad windows files, it's a pretty good one to run on your image.

Network Stuff

Use `ipconfig` (better yet `ipconfig /all`) to view network information on the computer. This isn't really useful for CyPat but it can be good to know. This will have information of the systems IP, MAC address, Subnet and other related stuff. I had to use this a lot in SHSM comps and stuff.

Using `ipconfig /displaydns` will show the contents of the window's hosts file. This can be poisoned/changed so it's good to check. The file directory is `C:\Windows\System32\Drivers\etc\hosts` if you want to look at some leads and stuff before you clear it. It's definitely a good thing to check.

When you want to clear it (hosts file) do `ipconfig /flushdns` (Still can be poisoned after this may require further checking)

`ping`, `nslookup` and `tracert` are also useful to know, but aren't really needed for CyPat

`net session` to view connected remote sessions. If you see any use `net session \\computername /del` to delete them

User Stuff

Useful commands to get to know for this:

net user

net localgroup

net share

Useful Commands

gpupdate /force	Update your policies!!
dcdiag /q	Check if you workstations are syncing to your AD
net share	Check what is being shared and harden
icacls <dir>	View access and perms of folders/gpos easily. icacls /help shows what the codes mean.
winver.exe	To check if windows version is up to date

PowerShell

Useful Commands

netstat -abno	Netstat but on powershell.

Hardening

Get-ExecutionPolicy -List

If any are not restricted, set them back to restricted! Set-ExecutionPolicy -ExecutionPolicy Restricted -Scope WhateverScope

SMB

Check for SMBv1

- Run Get-WindowsOptionalFeature -Online -FeatureName SMB1Protocol

- If it is enabled, disable it with: `Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol`

Check for SMBv2 and SMBv3

- Run `Get-SmbServerConfiguration | Select EnableSMB2Protocol`
- If disabled, enable it with: `Set-SmbServerConfiguration -EnableSMB2Protocol $true`

Registry

Info

HKEY_CURRENT_USER (HKCU)	Data on currently logged in user
HKEY_USERS (HKU)	Data on all user account on host
HKEY_CLASSES_ROOT (HKCR)	Data on object linking and embedding (OLE) registrations
HKEY_LOCAL_MACHINE (HKLM)	System related data (this is where you will set most of your security settings, if you are into doing it through the registry)
HKEY_CURRENT_CONFIG	Data on host's current hardware profile

Hardening

Check startup paths:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce

Things can hide here that won't show up in windows start-up.

NOTE: BEFORE ANY REGISTRY CHANGES THE REGISTRY SHOULD BE BACKED UP

FILE > EXPORT for backup

FILE > IMPORT for restore

(Or just make a restore point)

- Check and configure permissions on each key (just the main ones and set them to "Applies to: this key and subkeys")
 - Right click and go to permissions and it's just the same as folders

Hardening Actual Keys

Key	Value(s)	Notes
<u>Enable kerberos event logging</u>		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters	Registry Value: LogLevel Value Type: REG_DWORD Value Data: 0x1	If the parameters key does not exist just create it. These logs can be found in the system log.
SYN attack protection (Only for later versions of windows)		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect	2	
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxHalfOpen	500	
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TcpMaxPortsExhausted	5	2008 and before
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TcpMaxHalfOpenRetried	400	2008 and before
Disable Disk Sharing (before 2012)		
HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters\AutoShareServer	0	This stuff can now be handled in Computer Management > Shared Folders
<u>Configure NTP</u> (prevent clock drift which affect some security protocols) - Probably won't give points (relies on external servers, good to know anyway)		
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters\Type	"NTP"	
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config\AnnounceFlags	5 (DWORD)	
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NtpServer	1 (true, DWORD)	

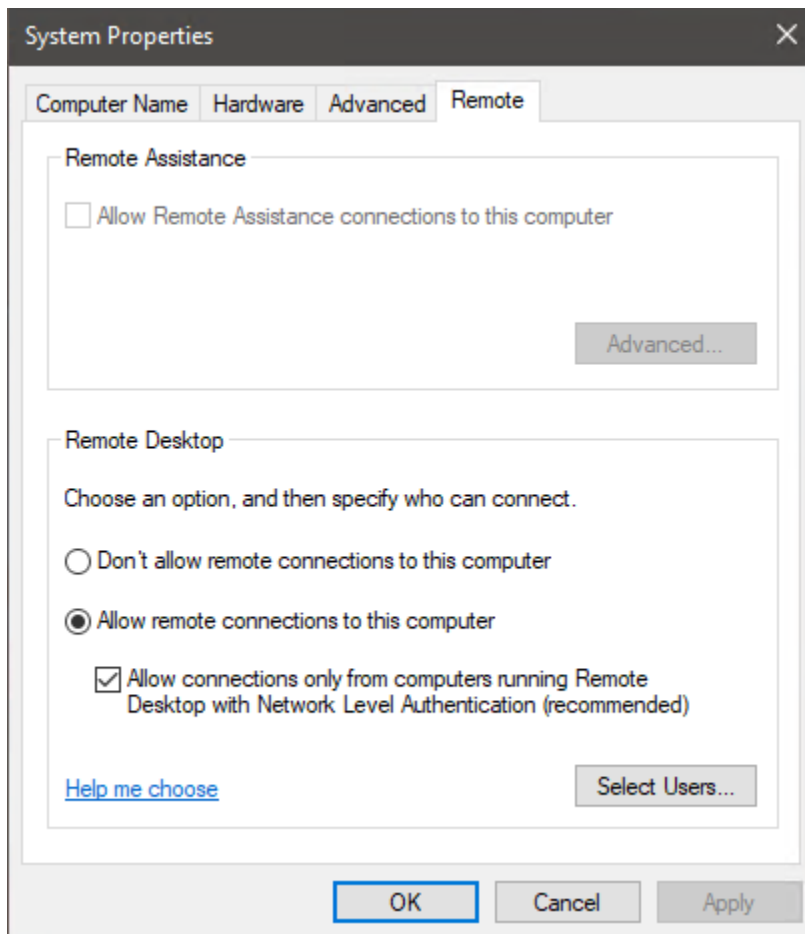
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters	Enter DNS' in link. Append with 0x1 at end of each DNS	https://www.ntppool.org/en/use.html
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NtpClient\SpecialPollInterval	900 (recommended, time in seconds)	
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config\MaxPosPhaseCorrection	1800 (recommended, seconds)	
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config\MaxNegPhaseCorrection	1800 (recommended, seconds)	
Run command net stop w32time && net start w32time to restart, and allow changes to take effect		
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\	Value Name: NoDriveTypeAutoRun Type: REG_DWORD Value: 0x000000ff (255)	If not there add it. This is autoplay.
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NetBT\Parameters:NodeType	DWORD 0x2	NetBIOS node type
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TCPIP6\Parameters:DisabledComponents	DWORD 0xff	Ipv6 exchange over internet

There's a lot more so I suggest you make your own chart for the ones you find that you think are important

Remote (RDP Critical Service) Security

Remote Desktop Settings

They should look like this:



Group Policy

Goto: Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Security

Server authentication certificate template	(blank)
Set client connection encryption level	High Level
Always prompt for password upon connection	Enabled
Require secure RPC communication	Enabled
Require use of specific security layer for remote (RDP) connections	SSH
Do not allow local administrators to customize permissions	Disabled
Require user authentication for remote connections by using Network Level Authentication	Enabled

Goto: Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Connection Client

Do not allow passwords to be saved	Enabled
------------------------------------	---------

Goto: Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Device and Resource Redirection

Do not allow drive redirection	Enabled
--------------------------------	---------

Goto: Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Session Time Limits

Set time limit for active but idle Remote Desktop Services sessions	300
Set time limit for active Remote Desktop Services sessions	Enabled

Go to Computer Configuration > Administrative Templates > Network > Network Connections > Windows Firewall then Domain and Standard profiles and enable Allow inbound remote administration exception.

Change RDP Port:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TerminalServer\WinStations\RDP-Tcp\PortNumber

Firewall

Enable below inbound rules:

- Remote Event Log Management (NP-In)
- Remote Event Log Management (RPC)
- Remote Event Log Management (RPC-EPMAP)
- Windows Management Instrumentation (ASync-In)
- Windows Management Instrumentation (DCOM-In)
- Windows Management Instrumentation (WMI-In)
- Network Discovery (NB-Name-In)
- File and Printer Sharing (NB-Name-In)
- Remote Service Management (NP-In)
- Remote Service Management (RPC)
- Remote Service Management (RPC-EPMAP)
- Performance Logs and Alerts (DCOM-In)
- Performance Logs and Alerts (Tcp-In)

Note:

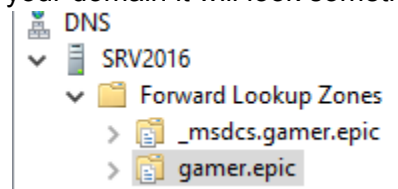
I am missing some stuff here so do some of your own research. The stig can be found here https://www.stigviewer.com/stig/remote_access_policy/

DNS

You will always see DNS on windows server and most likely it will also be in nationals (usually see it round 4) so this is a must study!

Configuring DNSSEC

1. Open server manager and go to tools > DNS
2. Select your domain it will look something like this:

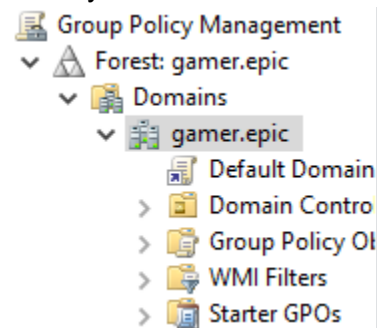


3. Then right click and click DNSSEC > Sign the Zone
4. Hit next
5. Make sure **Customize zone signing parameters** is selected then hit next
6. Make sure **The DNS server CLOUD-SERVER is selected as the Key Master** is selected then hit next
7. Hit next
8. On the key signing key (KSK) interface click add.. Make sure the properties are what you want (usually defaults are okay but make sure you go through each setting) then hit okay and next
9. Hit next ... then do the same as you did with the KSK page but this time on the ZSK page (add > look at settings > ok > next)
10. Make sure NSEC3 is selected then hit next
11. On the trust anchors page make sure **check the Enable the distribution of trust anchors for this zone checkbox** is checked (unchecked by default) as well as the one below it
12. Hit next again on the Signing and Polling Parameters interface
13. The hit next to finalize
14. Now in the DNS console go down the **Trust Points** directory and make sure both keys are (under status) valid should look something like this

Name	Status	Type	Algorithm	Valid From
(same as par...	Valid	DNS KEY (DNSKEY)	RSA/SHA-256	6/7/2020 5:51:59 PM
(same as par...	Valid	DNS KEY (DNSKEY)	RSA/SHA-256	6/7/2020 5:51:59 PM

15. Now go to Server Manager > Tools> Group Policy Management

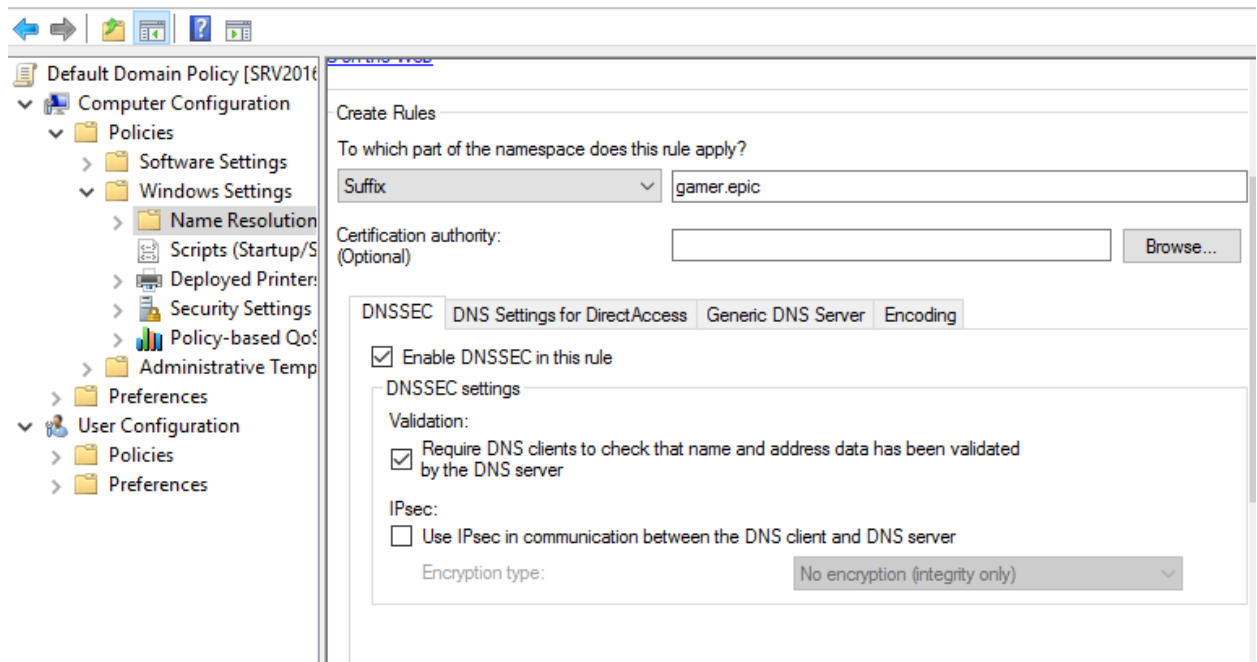
16. Go to your domain



17. Right click the Default Domain Policy and click edit

18. Now go to Computer Configuration > Policies > Windows Settings > Name Resolution Policy

19. Type the domains name in the **To which part of the namespace does this rule apply?** Input. Check **Enable DNSSEC in this rule** and **Require DNS clients**. Then hit create.



20. Then restart or run `gupdate /force`

DNS Socket Pool

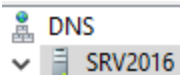
1. Open powershell (admin) and run `Get-DNSServer`
2. Take note of the `SocketPoolSize` variable default is 2500
3. In this case I am going to set it to 5000 the max is 10000. The larger the pool the higher the security
4. Run `dnscmd /config /socketpoolsize 5000` in powershell to change it to a pool of 5000
5. Restart dns server (cmd in admin run `net stop dns` then `net start dns`)

DNS Cache Locking

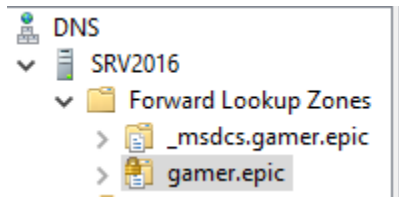
1. Open powershell (admin) and run `Get-DNSServer`
2. Take note of the value of the DNS cache lock
3. Run `Set-DnsServerCache -LockingPercent 100` to make sure it is at 100 percent

Access and Permissions and Logging

Right click on the DNS itself (look below) and hit properties. Go to the security tab. Check over it and make sure no one is there that should not be there (i.e users / a random user). Also make sure debug logging is on as well

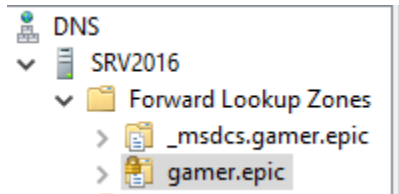


Do the same for your domain zone (it wont have logging)



Domain Zone Properties

Go to your domain and hit properties (may want to do it on both of the Forward lookup zones also reverse lookup zones but usually there aren't any)



Right click then hit properties

1. In general make sure Dynamic updates is set to secure only
2. In Zone Transfers make sure zone transfers are not allowed
3. In name servers if you are on the AD make sure it only has yourself

Make sure IPv6 is Disabled (if Not in Use)

1. Go to Control Panel > Network Connections
2. Right click and Properties on the LAN connection
3. Make sure IPv6 is unchecked
4. Check the readme. I find usually Cyberpatriot like IPv6 enabled.

Active Directory (Domain Controller)

You see this in the later rounds and usually in nationals. Pretty much always accompanied by a DNS server.

How To

Active Directory?

Tool on windows server to organize users and configuring access control

Minimum of two AD Domain controllers in a network environment. (Fault tolerance and ability to perform maintenance without impacting the working AD)

Installing AD?

Add roles and features > Select server > Active Directory Domain Services (Install DNS server as well if needed).

After installation, promote the server to the Domain Controller and add new forest. Check Global Directory. Set Password.

DNS delegation (check if you have a second dns controller, creates a sync between your ad and the dns controller)

Add workstations to the AD (Windows 10 and 7 etc...)?

Go To System > System Properties (change settings link) > Change domain > type in domain name you gave AD (will ask user and pass)

Note: if the network adapter was marked as a public it may have problems. just change the network type to private!

Hardening

Make sure to check over active directory users and computers (under tools in server manager) and make sure users don't have access to OUs (the directory things) they shouldn't (left click > properties > security). Also check permissions as well. When you do this make sure: view menu > Advanced Features is selected.

Here is general rules of thumb when checking these users:

To view a better summary click the advanced button on the security tab. Select an entry and hit edit or view.

- CREATOR OWNER - Special permissions
- Self - Special permissions
- Authenticated Users - Read, Special permissions
- The Special permissions for Authenticated Users are Read type. If detailed permissions include any Create, Delete, Modify, or Write Permissions or Properties, this is a finding.
- SYSTEM - Full Control
- Domain Admins - Full Control
- Enterprise Admins - Full Control
- Key Admins - Special permissions
- Enterprise Key Admins - Special permissions
- Administrators - Read, Write, Create all child objects, Generate resultant set of policy (logging), Generate resultant set of policy (planning), Special permissions
- Pre-Windows 2000 Compatible Access - Special permissions
The Special permissions for Pre-Windows 2000 Compatible Access are for Read types. If detailed permissions include any Create, Delete, Modify, or Write Permissions or Properties, this is a finding.
- ENTERPRISE DOMAIN CONTROLLERS - Read, Special permissions
- Directory data of non-public directory must be configured to prevent anonymous access

Check over Group Policy Management permissions and make sure they are valid!

To check it go to group policy management (under tools in the server manager). Go to the domain. And for each group policy object (under the domain) click on it and click the delegation tab and then click advanced to view permissions.

Make sure:

- There are no standard users

- Authenticated Users are only read type (no create, delete, modify, write permissions or properties)
- Their permissions look like this (unless specified otherwise)
 - CREATOR OWNER - Special permissions
 - SYSTEM - Read, Write, Create all child objects, Delete all child objects, Special permissions
 - Domain Admins - Read, Write, Create all child objects, Delete all child objects, Special permissions
 - Enterprise Admins - Read, Write, Create all child objects, Delete all child objects, Special permissions
 - ENTERPRISE DOMAIN CONTROLLERS - Read, Special permissions
- The Domain Admins and Enterprise Admins should not have the "Delete all child objects" permission on the two default Group Policy objects: Default Domain Policy and Default Domain Controllers Policy.

Non-public directory must be configured to prevent anonymous access. (no anonymous access to your AD)

Testing:

- On the AD open command prompt
- Run ldp.exe (Ldp.exe)
- Connection menu > Bind
- Clear everything in there
- Select Simple Bind then OK
- Should say:
res = ldap_simple_bind_s
Authenticated as: 'NT AUTHORITY\ANONYMOUS LOGON'
- Browse menu > Search
- enter the DN of the domain naming context (eg "dc=hostname,dc=afterdot") in the Base DN field.
- Clear all attributes and select Run
- Error message should display (if it does not anonymous access is enabled)

Solution:

- Open ADSI Edit (under tools in server manager)
- Make sure there isn't a configuration connected.
 - If you need that config go to CN=Configuration > CN=Services > CN=Windows NT > Then left click properties on CN=Directory Service.
 - Make sure dSHeuristics is not set
- Go to active directory users and computers (under tools in server manager)
- Select the properties of each folder and makes sure that ANONYMOUS LOGON does not have any access (or any other users that shouldn't)

Check SYSVOL directory access control permissions.

To find this folder run net share in the command prompt by default the location is \Windows\SYSVOL\sysvol.

Make sure no standard user accounts have permissions greater than Read & Execute
Run `icacls c:\Windows\SYSTEM32` (or whatever dir it is located) to check access.

It should display:

```
NT AUTHORITY\Authenticated Users:(RX)
NT AUTHORITY\Authenticated Users:(OI)(CI)(IO)(GR,GE)
BUILTIN\Server Operators:(RX)
BUILTIN\Server Operators:(OI)(CI)(IO)(GR,GE)
BUILTIN\Administrators:(M,WDAC,WO)
BUILTIN\Administrators:(OI)(CI)(IO)(F)
NT AUTHORITY\SYSTEM:(F)
NT AUTHORITY\SYSTEM:(OI)(CI)(IO)(F)
BUILTIN\Administrators:(M,WDAC,WO)
CREATOR OWNER:(OI)(CI)(IO)(F)
```

Permissions on the Active Directory data files only allow system and administrator access.

To do this you must:

- Go to the registry (run `regedit`)
- Go to `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters`
- For each directory listed there run "icacls" on it. Icacls should display:
NT AUTHORITY\SYSTEM:(I)(F)
BUILTIN\Administrators:(I)(F)
- If it doesn't change the permissions.

Make sure all local volumes are NTFS (can be ReFS too). This does not include Recovery and Boot (EFI) partitions.

Check that certificates are issued by Dod PKI or something else trusted. To check:

- Run `mmc` and add the Certificates snap in (Computer account then local)
- Go to Certificates (Local Computer) > Personal > Certificates and check "Issued By"
- Also run "Get-ADUser -Filter * | FT Name, UserPrincipalName, Enabled" in powershell
- User accounts and upn should be valid and unique (in the case of the UPN)

Check audit policies of gpos by going to group policy management > any group policy object > delegation > advanced > advanced again > auditing.

Set:

Type - Success

Principal - Everyone

Access - Special (Permissions: Write all properties, Modify permissions; Properties: all "Write" type selected)

Inherited from - Parent Object

Applies to - Descendant groupPolicyContainer objects

Type - Success

Principal - Everyone

Access - blank (Permissions: none selected; Properties: one instance - Write gPLink, one instance - Write gPOptions)

Inherited from - Parent Object

Applies to - Descendant Organization Unit Objects

LAPS

(Mostly you would want this for an AD. Doubt it is scored in cyber patriot but I have never tried it)

LAPS is:

Local Administrator Password Solution (LAPS) tool, which is free and supported software that allows an organization to automatically set randomized and unique local Administrator account passwords on domain-attached workstations and Member Servers.

To see if it is installed go to:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions\{D76B9641-3288-4f75-942D-087DE603E3EA}:DIName

If that exists it is there. If not install it: <https://www.microsoft.com/en-us/download/details.aspx?id=46899>

Group Policy Client Side Extension (CSE) must also be on all workstations attached to the AD Make sure AdmPwd.dll is installed here: C:\Program Files\LAPS\CSE\AdmPwd.dll

Other

- Use MBSA
- Enable BitLocker encryption in System and Security (control panel). This is an optional one because I've never had it give points. Just do it if you hit a real wall on one last point or something. WRITE DOWN YOUR PASSWORD SOMEWHERE FOR THIS.
- Screensaver password. Enable screen saver, set the wait time to five minutes, and enable On resume, display logon screen.
- ~~Check in Safe Mode~~

Secure Firefox!!!!

Look it up!! It is trending more and more to be used in cyber patriot as something to secure. VERY IMPORTANT.

Linux Tips

Learn how to secure OpenSSH and apache web server. The best way I can suggest doing this is to do it yourself, set up a linux VM and make the server and secure it (**this is the best way to learn this so please do it**). I also suggest you force yourself to use Linux for your normal

desktop computing. Since the competition uses ubuntu I would suggest you use that on a laptop or something that you use for school. If you actually want to move to Linux full time I would suggest arch or an arch based distro like manjaro. It is very important that you familiarize yourself to Linux. From my own experience (I use linux on all my systems now) it is so much less bloated and actually easier to operate once you get a handle on the terminal. And this also makes it easier to secure (don't fall for everyone has a hard time with Linux meme)! If you want an easy way to get started install ubuntu on the machine you use most and get started, if you have two hard drives you can dual boot (wouldn't suggest dual booting on one drive). And just use it for everything. You can also use this to help solidify a foundation:

<https://linuxjourney.com/>.

If you want to switch to linux full time and want a place to start <https://distrochooser.de/?l=2> is a great resource to get started with your research. Also some other things is you should definitely learn permissions [chmod] on linux (this can be done in like less than 30 mins, I suggest you make a cheat card). And learn what folders should have what permissions, usually this can be done with [stigs](#). Also remember a lot of the things people are securing on windows can transfer to what you need to secure and vice versa. So take note of the points your team are getting. If you are really keen on securing linux do what I did and make a study document when you teach back what you are studying so you can remember better and other people can use it when you are gone.

Linux is always where people are behind so if you want to win being ahead in linux is crucial.

Tips and Etiquette

On later images you **will** and **should** be working the whole time! If you are bored and not working and you are not at 100 you aren't studying enough and (if you are under 85) you are missing something crucial. You are **definitely** missing essential security stuff if you are under 70. This is important because in nationals you don't have the score and you should be working the **whole** time so you need to have the knowledge and discipline to look deeper.

I would suggest using Microsoft management console for all your administrative usings. Just do Win + R and type "mmc". Then do file > Add/Remove Snap-In. This will let you do all your administrative stuff in one place. Like group policy, shares and user management to name a few. You can save your consoles onto the desktop making your customized admin consoles have easy access (File>Save As). MMC is probably one of the best tools (built-in to windows) for CyPat.

God mode can be helpful for finding little settings. Just make a folder and rename it to GodMode.{ED7BA470-8E54-465E-825C-99712043E01C}

Creating a restore point on windows is always a good idea, especially when you start getting dangerous with your changes. I.e registry edits and such. I would create a restore point right when you start your image. This seems to be common practice for the more competitive teams.

It seems like when they are stuck they just reset the image and redo it. I would also create a restore point after main point gain and then create others via your own discretion. (I advise doing one before major changes that you are iffy about). To find it just search "create restore point".

Keep a list of things you've done on a second monitor. You don't have to do this after every single thing but just do it as a little break (and before you forget the stuff you did). This helps when other people check your image and it's good to have it up so it helps prevent the next thing I am going to mention.

STOP SAYING "DID YOU CHANGE ALL THE PASSWORDS, DID YOU CHECK FOR MP3s ETC...". If you are trying to help someone that is stuck don't just go through some random checklist you found online and annoy them with the simple stuff they already have done. It is good to do this if someone is stuck but try to jog someone's memory on stuff but just blurting it out when they probably checked it 3 times already is not helpful. If you are really hell bent on doing the easy stuff just do it yourself when they need a break. I am really tired of this stuff as a competitor and it really makes you unlikable. I want to stress that reminders are good but, just talk to your teammates and go through it with them after you're done your research. Maybe write things down as you do your research and make a little customized checklist for them (look at the points they already have first). Just don't be annoying and blurt out stuff and get mad at your teammates for not listening to you, be a good teammate and work AS a team.

There will most definitely be some points you have never seen before. No checklist or anything you will ever find online will be able to give you 100% on an image so don't rely on them. Build up your skills and practice, and you'll be able to know where to look naturally.

If you have more than one forensics question, tell your Cisco lead (as they usually have nothing to do at the start) or anyone that is doubling on a computer. Almost all forensics can be solved using google searching. You just have to know how to search and use windows tools. Sometimes it will even ask for powershell or regedit or some command in linux you don't know but the person in charge of that specific image should know how to use that stuff.

Compare the scoring report on images they are always closely related especially linux and windows.

Default Images

Groups (Win 10)

Name	Description
Access Control Assist...	Members of this group can remotely query aut...
Administrators	Administrators have complete and unrestrict...
Backup Operators	Backup Operators can override security restrict...
Cryptographic Operat...	Members are authorized to perform cryptogra...
Distributed COM Users	Members are allowed to launch, activate and u...
Event Log Readers	Members of this group can read event logs fro...
Guests	Guests have the same access as members of th...
Hyper-V Administrators	Members of this group have complete and unr...
IIS_IUSRS	Built-in group used by Internet Information Se...
Network Configuratio...	Members in this group can have some admini...
Performance Log Users	Members of this group may schedule logging ...
Performance Monitor ...	Members of this group can access performanc...
Power Users	Power Users are included for backwards comp...
Remote Desktop Users	Members in this group are granted the right to...
Remote Management...	Members of this group can access WMI resour...
Replicator	Supports file replication in a domain
System Managed Acc...	Members of this group are managed by the sy...
Users	Users are prevented from making accidental or...

Resources Helpful In Comp

Note: do the main grind first, once you find that you are hitting a wall start using tools. It is just good to do your own work first because you can keep track of what is done so you aren't checking over things.

A Must

Meh

MBSA, really good for finding simple stuff you missed. Just shows basic security flaws

<https://www.microsoft.com/en-ca/download/details.aspx?id=19892>

Automatically sets tedious security policies

[https://docs.microsoft.com/en-us/previous-versions/tn-archive/cc677002\(v=technet.10\)?redirectedfrom=MSDN](https://docs.microsoft.com/en-us/previous-versions/tn-archive/cc677002(v=technet.10)?redirectedfrom=MSDN)

For searching group policies

<https://gpsearch.azurewebsites.net/>

<https://docs.google.com/spreadsheets/d/>

<1VCNYr04QmsTgs2iNTIyclYMUITKwJLqEDBEAGDiaLIE/edit?usp=sharing>

An uninstaller that GIVES POINTS. (When using the windows uninstaller things will be left

behind, this program usually gets all of it, CCleaner can be used for this but it's hit or miss) Use

moderate for normal programs and Advanced for scary and spooky stuff

<https://www.revouninstaller.com/>

I used this at my work for patching software and application, much more efficient than going to every programs website

<https://ninite.com/>

Windows Analysis Software (has a bunch of useful analysis software for windows)

<https://docs.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite>

Good for netstat like stuff

<https://www.nirsoft.net/utils/cports.html>

System hardening tool, may cause crash:

<https://www.novirusthanks.org/products/syshardener/>

Privacy hardener, may help get some points for security. Privacy and security are closely related.

<https://www.winprivacy.de/deutsch-start/download/>

Somewhat helpful advanced tools, just to check over what you missed and stuff

<https://www.glarysoft.com/glary-utilities/download/>

For managing group policies, there are some points here but it has a bit of a learning curve and can be useless

<https://blogs.technet.microsoft.com/secguide/2016/01/21/lgpo-exe-local-group-policy-object-utility-v1-0/>

Useful Links

Information on services as of windows 2018. Has some security info here

<http://www.blackviper.com/service-configurations/black-vipers-windows-10-service-configurations/>

Some security essential powershell scripts

<http://techgenix.com/essential-powershell-scripts/>

Must look at security benchmarks for lots of different OS' (mostly all the same)

<https://www.dropbox.com/sh/1oj0kzetl4nws1o/AABURdupWQ9IIWhIPLsCUocya?dl=0>

<https://www.cisecurity.org/cis-benchmarks/>

<https://learn.cisecurity.org/benchmarks>

MUST READ windows hardening guide helps build knowledge

<https://drive.google.com/open?id=1x8wIBOxuLAOKmxV1qLXllgPiTPGtdHHO>

Crypto site for encryption and description (Q: I used this to solve a lot of forensic questions)

<https://cryptii.com/>

Has a pretty good checklist but also some other good info

https://riverview-cyberpatriot.fandom.com/wiki/Riverview_CyberPatriot_Wiki

Practice with vulnerable images that aren't related to CP but are more advanced and good for practice

<https://www.uscybersecurity.net/csmag/developing-cyber-skills-with-puzzles-and-hacking-challenges/>

<https://www.vulnhub.com/>

How keys are used in cryptography (two way encryption)

<https://www.di-mgt.com.au/cryptokeys.html>

<https://www.the-art-of-web.com/php/two-way-encryption/>

Good for research on windows backdoors

<http://m.alloraconsulting.com/it-solutions/440-windows-backdoors-hacking-and-how-to-remove-common-ones>

Even if you do windows mostly CHECK OUT THIS

<https://linuxjourney.com/>

For powershell reference

<https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.security/?view=powershell-6>

Microsoft security documentation (good for group policy options):

<https://docs.microsoft.com/en-us/windows/security/threat-protection/>

List of third party remote programs to look out for

https://en.wikipedia.org/wiki/Comparison_of_remote_desktop_software

Practice images

<https://support.ca-cyberhub.org/support/solutions/folders/33000201655>

Port document

<https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml>

Other Checklists (Would not suggest, but if you're stuck on points it doesn't hurt to look at)

A useful checklist for windows, has some stuff I missed before

http://www.lacapnm.org/Cadets/STEM/CyberPatriot/SeasonVIII/CyberPatriot_Windows_Checklist.pdf

A popular one for linux

<https://github.com/Forty-Bot/linux-checklist>

Old checklists found online for windows and linux

<http://r2d2.cochise.edu/guilmetted/CyberPatriot/>

Has some obscure stuff to try on windows. I recommend you look at it for research purposes

<http://r2d2.cochise.edu/guilmetted/CyberPatriot/>

Nationals

The nationals I attended were a little weird due to the pandemic but I will explain my experience here.

Really all it comes down to is how good you are as a team. You can't do it all yourself as far and you have to put a lot of trust in your team to perform. In nationals I did not have enough time to do what I wanted.

There were 4 windows and 2 linux. One windows system was a domain controller which I spent the most of my time on. I spent a long time securing gpos. We didn't win so I didn't know if they were important. But they had a seminar on gpos and AD so I assume my work was getting

somewhere but I would need more experience to tell you actually how important gpos are (they are important in a real world context so honestly I couldn't tell you).

In Linux it was securing web server stuff (my sql, apache, php)

The rest was forensics and looking for breach of entry evidence. And the normal removing hacking tools and chasing leads as well as hardening os. All stuff you do normally in the competition.

Anyway we lost probably because of how we were as a team...

Haha n00b