

Critical Services:

- Remote Desktop Protocol (RDP)
- OpenSSH Server (SSH)

Read me:**WINDOWS 10**

It is company policy to use only Windows 10 on this computer. Management has decided that the default web browser for all users on this computer should be the latest stable version of Firefox. However, Internet Explorer must be made available to all employees as an alternative to Firefox.

After some consideration, the company has decided to give egagnan admin privileges. Please add egagnan to the administrators group at your earliest convenience.

Please update FileZilla Client and VLC to its most up-to-date version. Company policy has mandated that only the 64-bit versions of the software must be installed on this system.

One of our standard users noticed that Internet Explorer wasn't installed on this system. Please install Internet Explorer as it is our backup browser.

Authorized users must be able to access this computer remotely using ssh. As an added security measure for ssh, please change from listening on the default port 22 to now listen on port 223.

A few of our users have noticed that their Internet connection seems to "break" after a period of time. Some of the admins have been able to temporarily fix this issue, but after a short period of time the Internet connection on this system breaks again. If you find a permanent solution to this issue, it might make this system more usable for you and the other users.

Critical Services:

- Remote Desktop Protocol (RDP)
- OpenSSH Server (SSH)

AUTHORIZED ADMINISTRATORS AND USERS**Authorized Administrators:**

vberge (you)

password: (blank/none)

jcahill

password: scuba

jcousteau

password: Aqu@*Lung.

pdiole

password: s3a_expl0rAt1on

- Remote Desktop Protocol (RDP)
- OpenSSH Server (SSH)

AUTHORIZED ADMINISTRATORS AND USERS

Authorized Administrators:

vberge (you)

password: (blank/none)

jcahill

password: scuba

jcousteau

password: Aqu@*Lung.

pdiole

password: s3a_expl0rAtion

fdumas

password: Sp3ArE!\$hing

Authorized Users:

egagnan

ggentile

bgilliam

drutkowski

espence

rstenuit

ttesei

agabr

jchatterton

COMPETITION NOTE

Competition Status and CCS Server Score

Scoring Report:

30 out of 40 vulns for 80 points

80 out of 100 points received

[Click here to view the public scoreboard](#)

Connection Status: Scoring Data Uploaded Successfully: No Errors Detected

Internet Connectivity Check: OK
CCS Server Connection Status: OK
CCS Server Score Upload Status: OK

0 penalties assessed, for a loss of 0 points:

30 out of 40 scored security issues fixed, for a gain of 80 points:

- Forensic Question check passed - 8 pts
- Forensic Question check passed - 8 pts
- Forensic Question check passed - 8 pts
- User auditing check passed - 1 pts
- User auditing check passed - 1 pts
- User auditing check passed - 1 pts
- User auditing check passed - 1 pts
- Account policy check passed - 1 pts
- Account policy check passed - 1 pts
- Local policy check passed - 2 pts
- Local policy check passed - 2 pts
- Local policy check passed - 2 pts
- Defensive countermeasure check passed - 1 pts
- Defensive countermeasure check passed - 1 pts
- Uncategorized operating system setting check passed - 2 pts
- Uncategorized operating system setting check passed - 2 pts
- Service auditing check passed - 2 pts
- Operating system update check passed - 2 pts
- Application update check passed - 2 pts
- Application update check passed - 1 pts
- Prohibited file check passed - 3 pts
- Unwanted software check passed - 2 pts
- Unwanted software check passed - 3 pts
- Unwanted software check passed - 2 pts
- Malware check passed - 2 pts
- Application security check passed - 3 pts
- Application security check passed - 4 pts
- Application security check passed - 4 pts
- Application security check passed - 5 pts
- Application security check passed - 3 pts

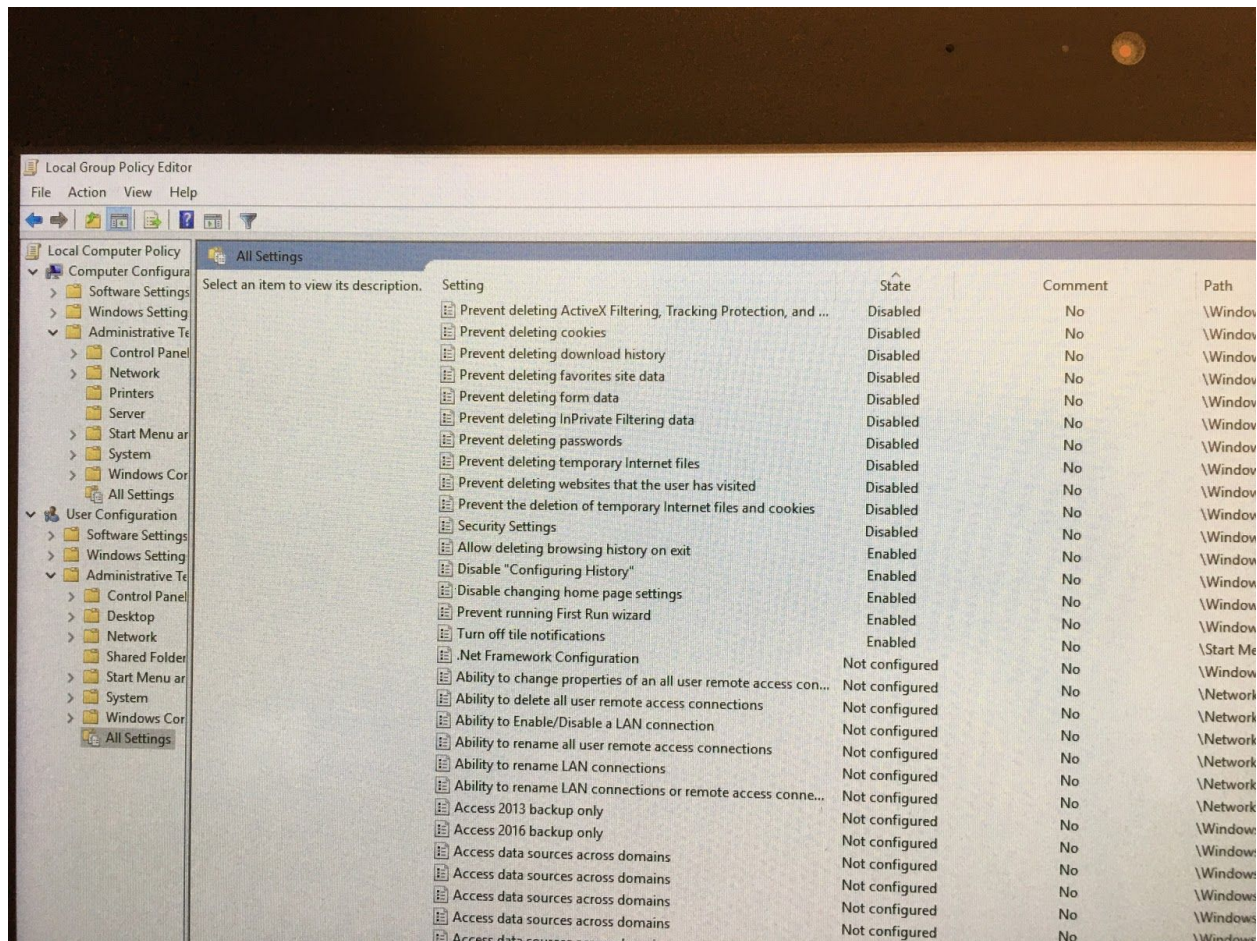
The CyberPatriot Competition System is the property of the Air Force Association and the University of Texas at San Antonio

All rights reserved.

Pre-Installed GPOS: Computer Configuration:

Setting	State	Comment	Path
Configure Automatic Updates	Disabled	No	\Windows Components\Windows Update
Require secure RPC communication	Disabled	No	\Windows Components\Remote Desktop Services\Remote
Show first sign-in animation	Disabled	No	\System\Logon
Do not display network selection UI	Enabled	No	\System\Logon
Don't launch privacy settings experience on user logon	Enabled	No	\Windows Components\OOBE
Enumerate administrator accounts on elevation	Enabled	No	\Windows Components\Credential User Interface
Prevent the usage of OneDrive for file storage	Enabled	No	\Windows Components\OneDrive
Set client connection encryption level	Enabled	No	\Windows Components\Remote Desktop Services\Remote
Set the default behavior for AutoRun	Enabled	No	\Windows Components\AutoPlay Policies
Turn off real-time protection	Enabled	No	\Windows Components\Windows Defender Antivirus\Real-t
Turn off Windows Defender Antivirus	Enabled	No	\Windows Components\Windows Defender Antivirus
[Reserved for future use] Cache Server Hostname	Not configured	No	\Windows Components\Delivery Optimization
Absolute Max Cache Size (in GB)	Not configured	No	\Windows Components\Delivery Optimization
Access 2013 backup only	Not configured	No	\Windows Components\Microsoft User Experience Virtualiza
Access 2016 backup only	Not configured	No	\Windows Components\Microsoft User Experience Virtualiza
Access data sources across domains	Not configured	No	\Windows Components\Internet Explorer\Internet Control Pa
Access data sources across domains	Not configured	No	\Windows Components\Internet Explorer\Internet Control Pa
Access data sources across domains	Not configured	No	\Windows Components\Internet Explorer\Internet Control Pa
Access data sources across domains	Not configured	No	\Windows Components\Internet Explorer\Internet Control Pa
Access data sources across domains	Not configured	No	\Windows Components\Internet Explorer\Internet Control Pa
Access data sources across domains	Not configured	No	\Windows Components\Internet Explorer\Internet Control Pa
Access data sources across domains	Not configured	No	\Windows Components\Internet Explorer\Internet Control Pa
Access data sources across domains	Not configured	No	\Windows Components\Internet Explorer\Internet Control Pa
Access data sources across domains	Not configured	No	\Windows Components\Internet Explorer\Internet Control Pa
Access data sources across domains	Not configured	No	\Windows Components\Internet Explorer\Internet Control Pa
Action on server disconnect	Not configured	No	\Network\Offline Files
Activate Internet printing	Not configured	No	\Printers
Activate Shutdown Event Tracker System State Data feature	Not configured	No	\System

User Configuration:



Notes:

- Disabled Local security policy just like how they did in state round this current year CPXII 2019-2020 **Security Settings**
- Turned off task manager

Forensics Questions:

- 1) For security purposes, an admin has changed the port this computer's remote desktop (RDP) server listens on. What port number does this computer's remote desktop (RDP) server listen on?

ANSWER: 4500

FIX TEXT: Get-ItemProperty -Path

HKLM:\SYSTEM\CurrentControlSet\Control\TerminalServer\WinStations\RDP*CP\ -Name
PortNumber

2)

- a) **ANSWER: bgilliam**
- b) **ANSWER: espence**
- c) **ANSWER: agabr**

NOTE: 2 may be incorrect

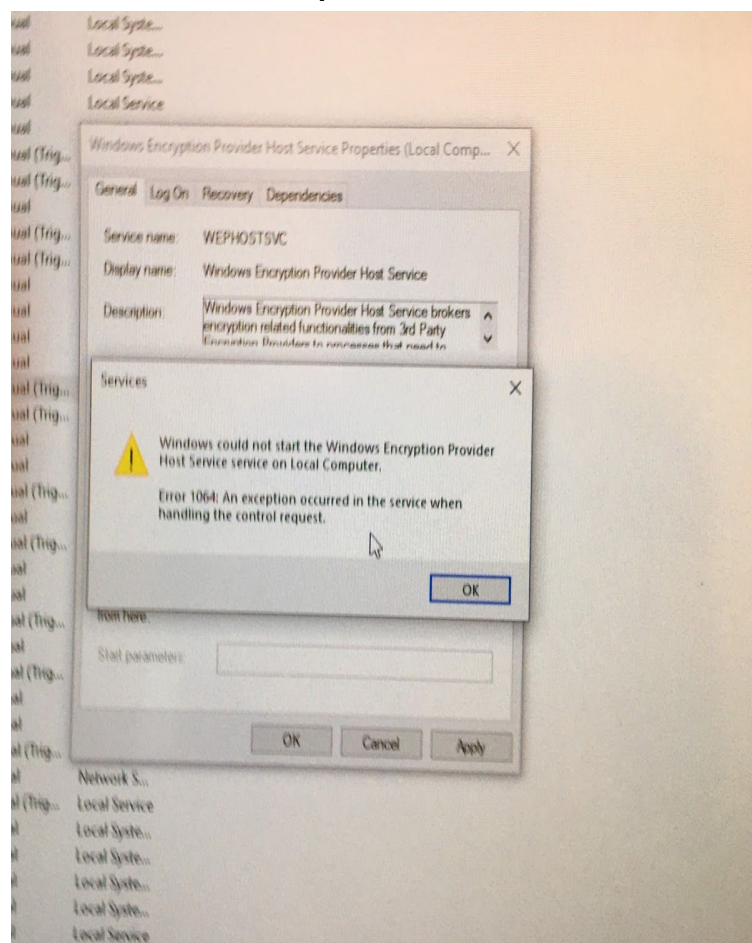
FIX TEXT: Win + R, gpedit.msc, user configuration, 'Security Settings' change to [enabled], close, open local group security policy, security options, 'allow users access with RDP', → gives two users. To find the third user you must hit the windows key once, type in remote desktop protocol, turn this on, and click on the bottom on 'add users to RDP' or something of that sort, then you will see bgilliam

- 3) Someone is trying to remotely brute force their way into this system. What is the workstation name that they were trying to remote in from?

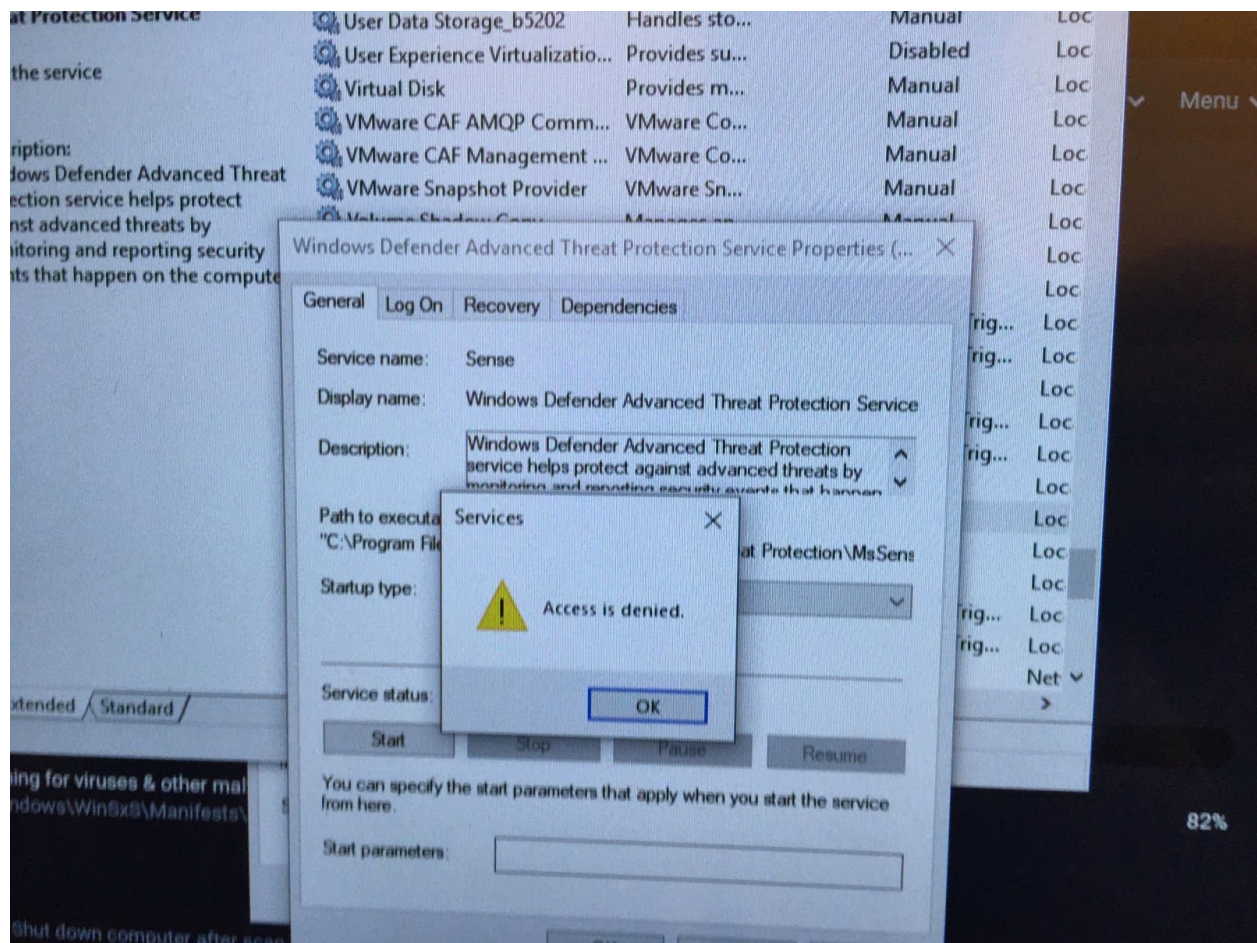
ANSWER: DESKTOP-OJNTU9C

FIX TEXT: open event viewer, filter by audit failures, find the many audit login fails, right click, properties, view the workstation of the user (computer name)

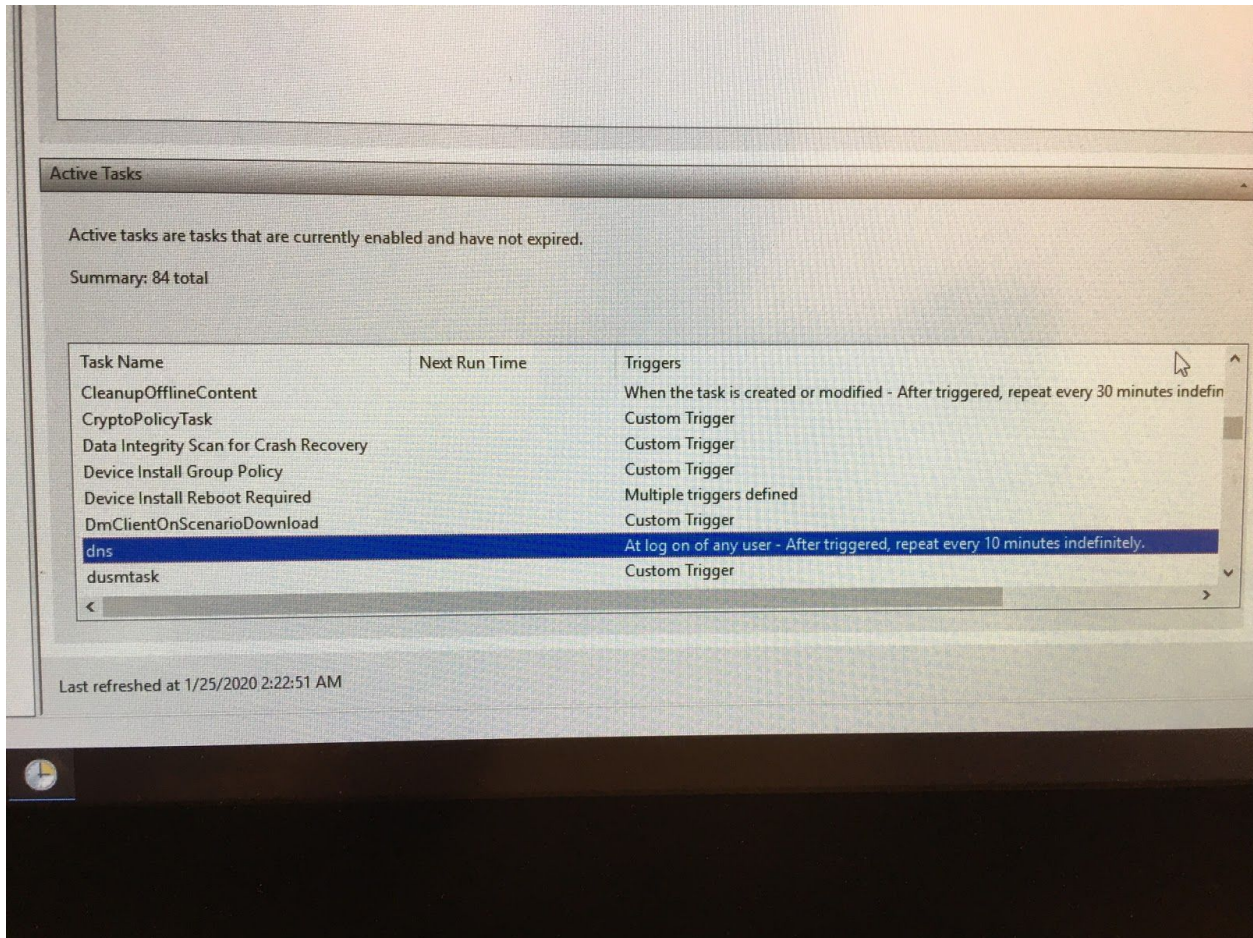
Other defaults on computer:



NOTE: look into this this may be a vuln @Rainbow because Encryption provider service should be started

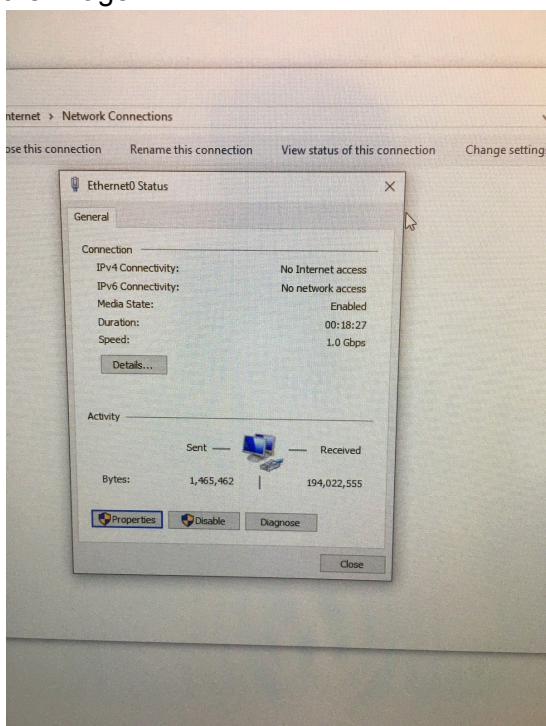


NOTE: Defender Advanced Threat Protection Service did not allow you to start the service (most likely a registry key/gpo that you'd have to configure in order to start the service).



NOTES:

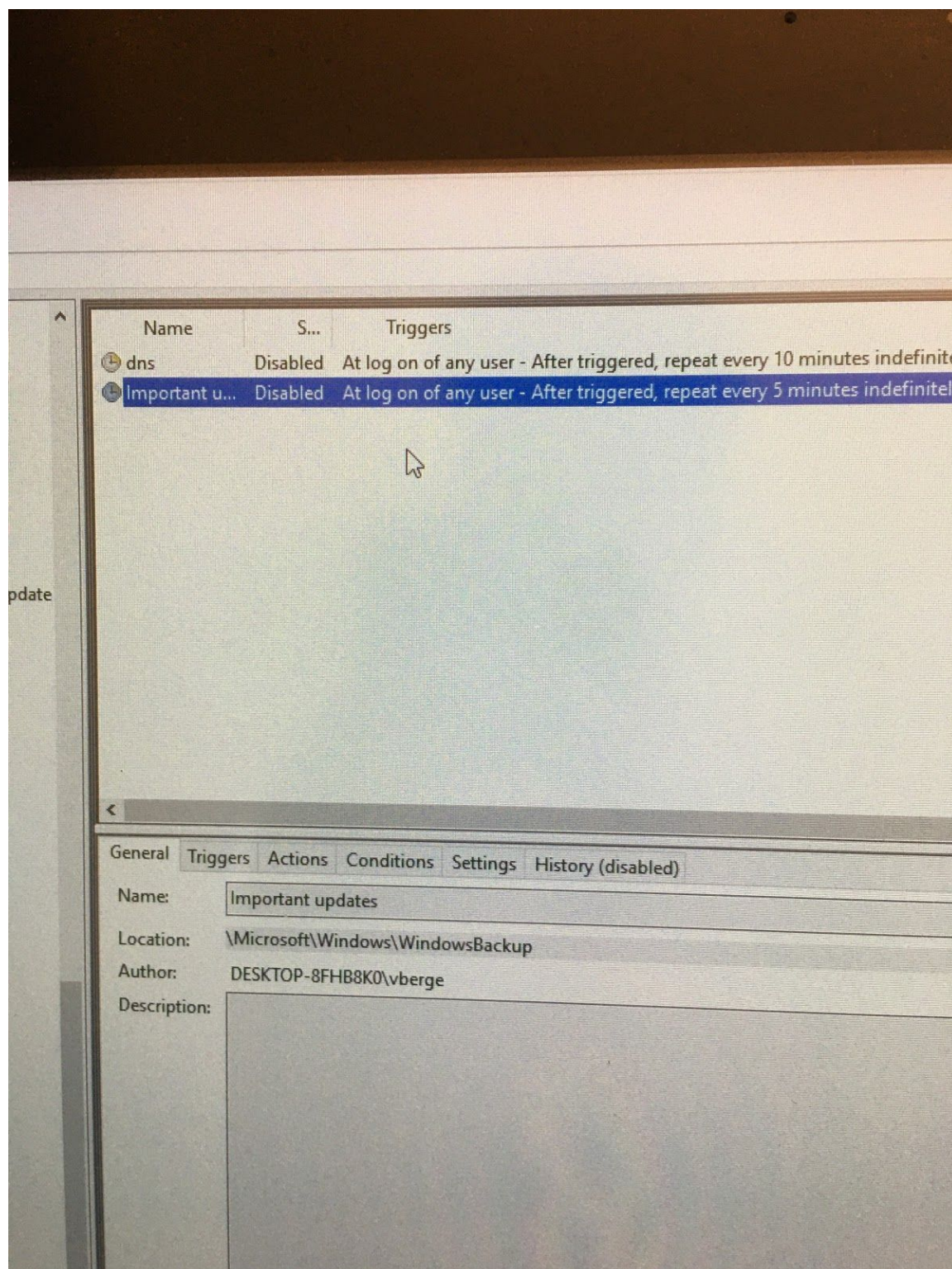
Found in task scheduler, must delete task in order to stop the internet connectivity problem with the image.



Additional information ← on Ethernet issue

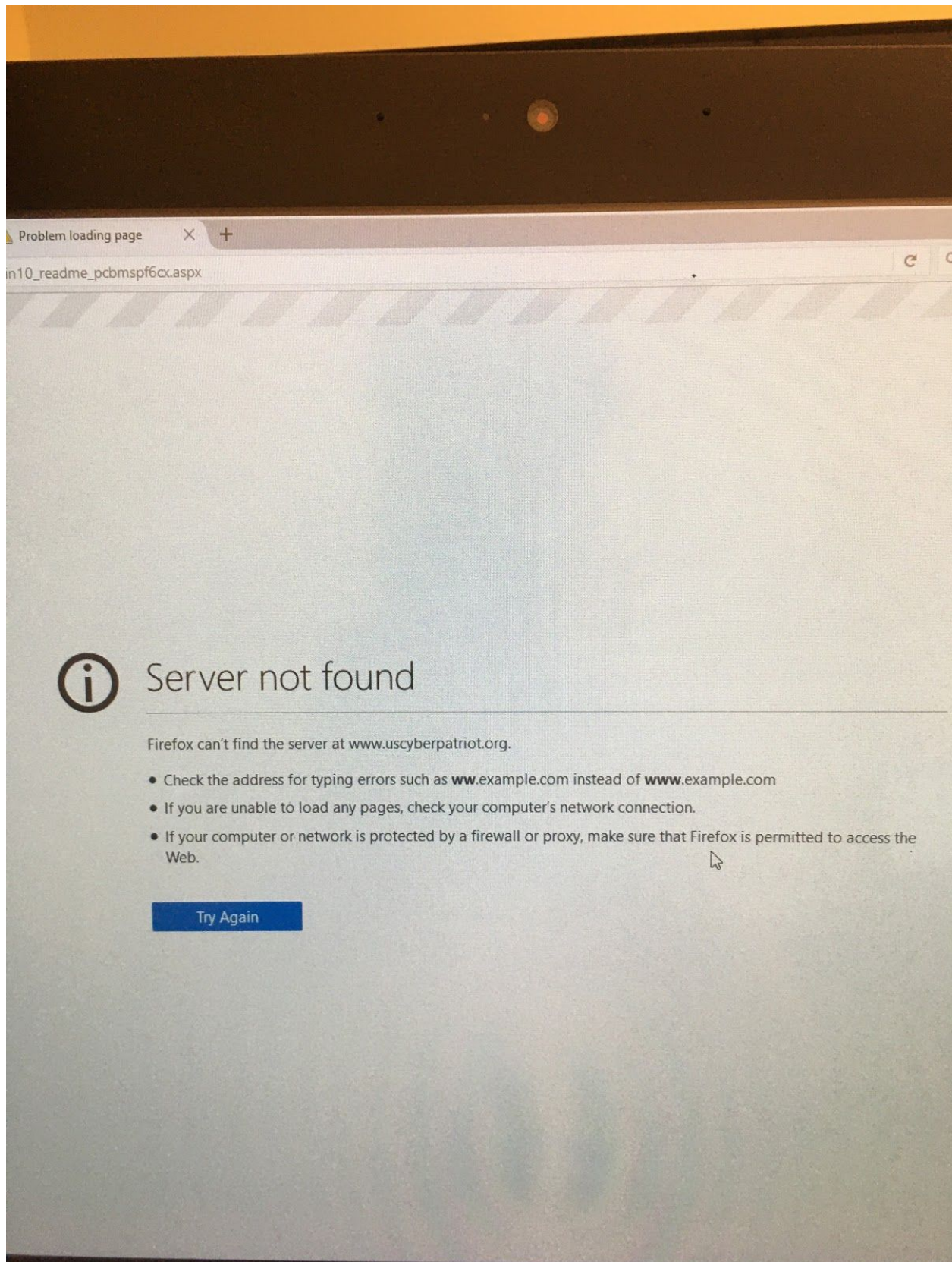
`ipconfig /release`
`ipconfig /renew`

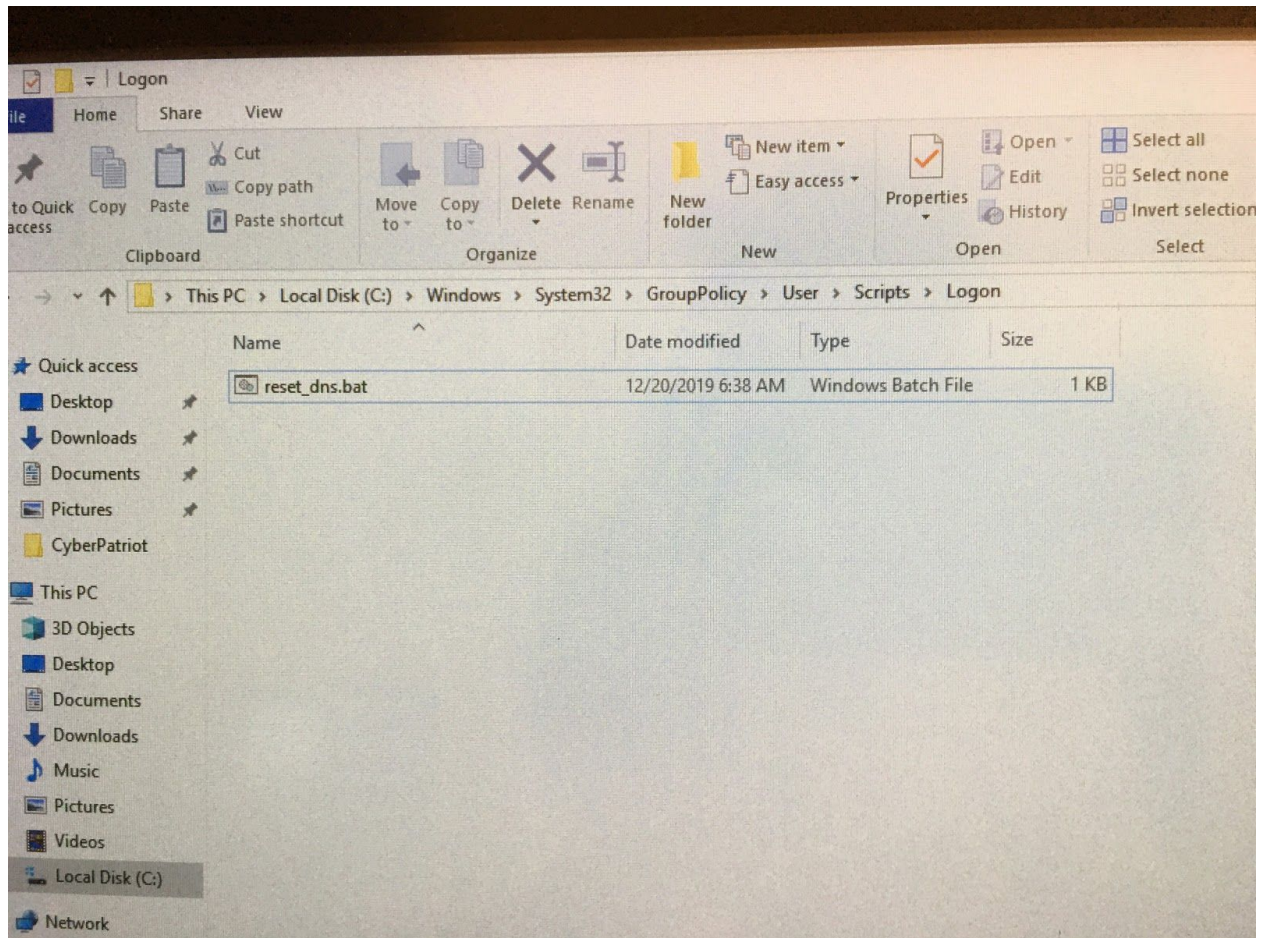
click "Open network & internet settings", change adapter options, right click your network adapter, click properties, click "Internet Protocol Version 4 (TCP/IPv4)", properties, obtain dns server address automatically



NOTE: Delete these two task schedulers to fix internet problem

Internet Problem:





NOTE:

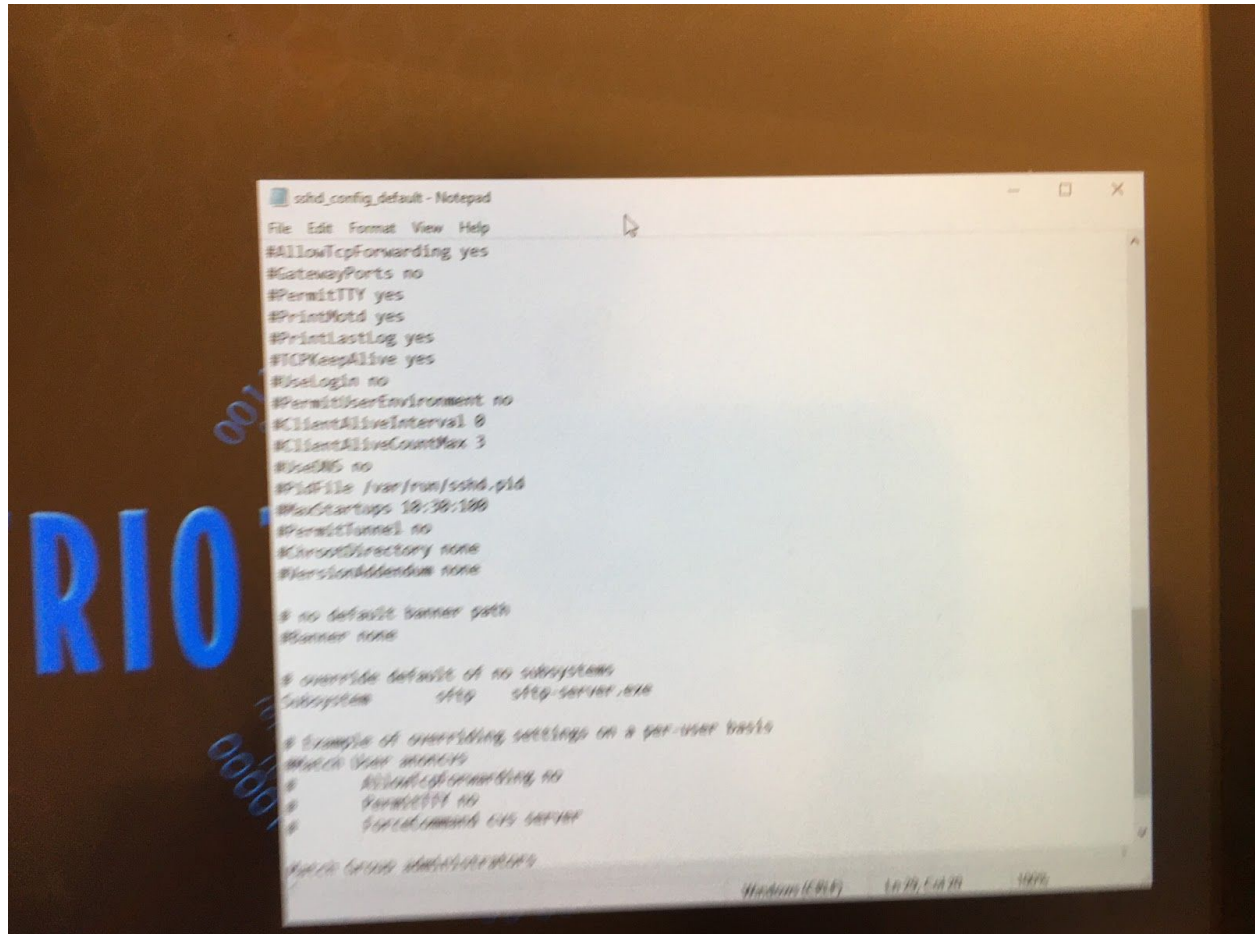
Delete this!!

Found in C:\Windows\System32\GroupPolicy\User\Scripts\Logon

Application security vulns: SSH and RDP

For SSH:

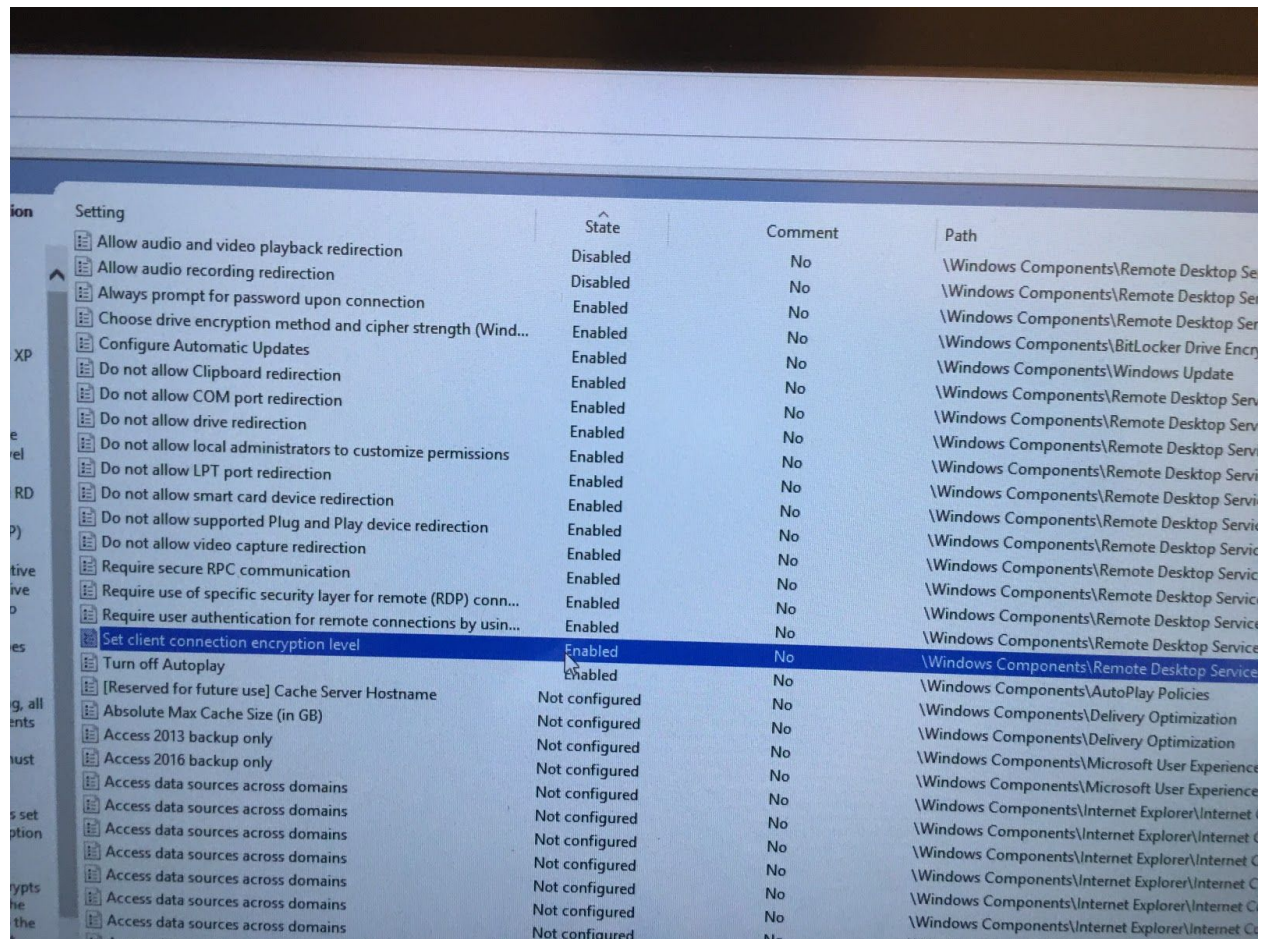
This is the configuration file: **sshd_config_default**



sshd_config_default:

- Here's what I did you can probably do more:
- I uncommented all of the commented things
- 'PermitRootLogin' no
- 'Protocol' 2 REMOVE 1
- PubkeyAuthentication
- Anything else the readme says
- And also do extra because they're configured the same way as linux
- **NOTE:** there are 3 files of this on the system
 - Pick the one that is the actual ssh config file you can do this by searching through C: ***sshd_config_default**
 - And clicking the one that is correct (you'll know when you see it)
 - Be sure to configure then save your file

For RDP:



Setting	State	Comment	Path
Allow audio and video playback redirection	Disabled	No	\Windows Components\Remote Desktop Se
Allow audio recording redirection	Disabled	No	\Windows Components\Remote Desktop Ser
Always prompt for password upon connection	Enabled	No	\Windows Components\Remote Desktop Ser
Choose drive encryption method and cipher strength (Wind...	Enabled	No	\Windows Components\Remote Desktop Ser
Configure Automatic Updates	Enabled	No	\Windows Components\BitLocker Drive Encr
Do not allow Clipboard redirection	Enabled	No	\Windows Components\Windows Update
Do not allow COM port redirection	Enabled	No	\Windows Components\Remote Desktop Serv
Do not allow drive redirection	Enabled	No	\Windows Components\Remote Desktop Serv
Do not allow local administrators to customize permissions	Enabled	No	\Windows Components\Remote Desktop Serv
Do not allow LPT port redirection	Enabled	No	\Windows Components\Remote Desktop Servi
Do not allow smart card device redirection	Enabled	No	\Windows Components\Remote Desktop Servi
Do not allow supported Plug and Play device redirection	Enabled	No	\Windows Components\Remote Desktop Servi
Do not allow video capture redirection	Enabled	No	\Windows Components\Remote Desktop Servic
Require secure RPC communication	Enabled	No	\Windows Components\Remote Desktop Servic
Require use of specific security layer for remote (RDP) conn...	Enabled	No	\Windows Components\Remote Desktop Servic
Require user authentication for remote connections by usin...	Enabled	No	\Windows Components\Remote Desktop Servic
Set client connection encryption level	Enabled	No	\Windows Components\Remote Desktop Service
Turn off Autoplay	Enabled	No	\Windows Components\Remote Desktop Service
[Reserved for future use] Cache Server Hostname	Not configured	No	\Windows Components\AutoPlay Policies
Absolute Max Cache Size (in GB)	Not configured	No	\Windows Components\Delivery Optimization
Access 2013 backup only	Not configured	No	\Windows Components\Delivery Optimization
Access 2016 backup only	Not configured	No	\Windows Components\Microsoft User Experience
Access data sources across domains	Not configured	No	\Windows Components\Microsoft User Experience
Access data sources across domains	Not configured	No	\Windows Components\Internet Explorer\Internet
Access data sources across domains	Not configured	No	\Windows Components\Internet Explorer\Internet
Access data sources across domains	Not configured	No	\Windows Components\Internet Explorer\Internet
Access data sources across domains	Not configured	No	\Windows Components\Internet Explorer\Internet
Access data sources across domains	Not configured	No	\Windows Components\Internet Explorer\Internet
Access data sources across domains	Not configured	No	\Windows Components\Internet Explorer\Internet
Access data sources across domains	Not configured	No	\Windows Components\Internet Explorer\Internet

Gpedit.msc → configure them according to DISA STIG or CIS whatever

NOTE: Idk if these are right or good so you should only look at these to see if you've got them or if you have any different settings

If you have a different setting try yours if you get points good

If not try mine if you get points good

I pretty much did all these local policies because **LGPO was a recurring problem for me and my GPO imports work went to waste**, but it did help in making sure I knew my GPOs.

User Auditing:

- **I added egnan to administrators group**
- I did FUCK, i forgot to make the users' password expire
- I don't think the accounts were locked out
 - But you should probably double check
- Disable administrator account
- Disable guest account
- Rename administrator
- Rename guest account
- **Change password for jcahill**
- **I think i removed espence from a lot of things**
- Do your own user auditing, you should be fine

Account Policies:

Password policies → literally if you don't know how to do these you're screwed

Lockout policies → literally if you don't know how to do these you're screwed

NOTES: you had to enable local security policy first 'Security Settings' [enable] then you could apply the policies and get points. Apply all of them because that's best practice.

Local policies:

I did all the common ones like

- Ctrl + alt + delete
- And like 8 more other than that I kinda stopped because I had to do 3 other images so like you can most likely clear this image if you import your GPOS
- Good luck with that because LGPO is fucked up unless you're a genius which you are

Defensive countermeasure:

- **I enabled firewall**
- **I turned on bitlocker encryption service automatic and started**

Uncategorized operating system:

- I have no fucking clue
- I did DEP
- Screensaver
- Etc it should be easy for you because I figured it out :p

Service Auditing:

- Go through the services
- Ensure like the critical services are enabled and automatic
- Look for anything not critical service related and disable it
- Idk i think SSH was the service but I forget

Operating System update:

- Probably windows checks for updates automatically (Group policy)

Application update:

- Did the stuff in the readme (FileZilla and VLC)

Prohibited File:

- Remove C:\Program Files (x86)\Windows 10 on Windows 10
 - HASHCAT

Unwanted software:

- Install revouninstaller
- Uninstall all the bad applications it will show you and you just delete all the regkeys and shit

Malware:

- Nc.exe backdoor on desktop
 - Remove netcat backdoor (C:\Users\midoriya\Desktop\nc.exe)
- Folder options → view hidden → view system folders → show extensions
- Use OSforensics shell bags
- Use security exploded hidden file finder
- Use task manager
- ANY OF THE THINGS ABOVE HELP

Application Security: see above

For augustus: self reflection

Was I prepared as much as i could be? No, I didn't know my shit inside and out, I knew like 80% of my shit, but not all of it like the internet problem. I have a feeling that I missed vulns on local security policy, service auditing, and probably user auditing because i'm a fucking dumbass.

What do i wish could've gone better? LGPO imports, resolving internet issue faster, drivers on usb loading, working on one image knocking them out one by one instead of jumping.

What will I do for next year? Create a manageable checklist that is easy to follow, one that is quick to do manually, and or is automated for me. Work efficiently and manage my time well, finish the forensics questions in half the time it took us.

Do I blame anyone for what happened? No it was all on me, not my team for not ever practicing, not my coach for fucking up the virtual machine, but me for not being able to still clear the images regardless of any issues or new critical services that i don't have intelligence on