	Setting
Account Policies	
Password Policy	**Secpol.msc (search bar)**
Enforce password history	5 passwords remembered
Maximum password age	90 days
Minimum password age	30 days
Minimum password length	14 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled
Account Lockout Policy	
Account lockout duration	30 min
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	30 min
Kerberos Policy	
Enforce user logon restrictions	Enabled
Maximum lifetime for service ticket	600 minutes
Maximum lifetime for user ticket	10 hours
Maximum lifetime for user ticket renewal	10 days
Maximum tolerance for computer clock synchronization	5 Minutes
Local Policies	
Audit Policy	
Audit account logon events	SF (success failure)
Audit account management	SF
Audit directory service access	SF
Audit logon events	SF
Audit object access	SF
Audit policy change	SF
Audit privilege use	SF
Audit process tracking	SF
Audit system events	SF
User Rights Assignment	
Access Credential Manager as a trusted caller	Default
Access this computer from the network	Users and administrators
Act as part of the operating system	Trusted users
Add workstations to domain	Authorized member of IT team
Adjust memory quotas for a process	Only users who could adjust memory quotas
Allow log on locally	Not Defined
Allow log on through Remote Desktop Services	Not Defined

Allow log on through Terminal Services	Default
Back up files and directories	Disabled
Bypass traverse checking	Not Defined
Change the system time	Not Defined
Change the time zone	Not Defined
Create a pagefile	Default
Create a token object	Not Defined
Create global objects	Disabled
Create permanent shared objects	Disabled
Create symbolic links	Not Defined
Debug programs	Only to trusted users/administrators
Deny access to this computer from the network	Default
Deny log on as a batch job	Not Defined
Deny log on as a service	Not Defined
Deny log on locally	Not Defined
Deny log on through Remote Desktop Services	Not Defined
Deny log on through Terminal Services	Not Defined
Enable computer and user accounts to be trusted for delegation	Not Defined/Admin.
Force shutdown from a remote system	Default
Generate security audits	localservice/Network service
Impersonate a client after authentication	Default
Increase a process working set	Users
Increase scheduling priority	Default Value
Load and unload device drivers	Not Defined
Lock pages in memory	Not Defined
Log on as a batch job	Default Value
Log on as a service	Minimize list of google accounts
Manage auditing and security log	Admins.
Modify an object label	Disabled
Modify firmware environment values	Default
Obtain an impersonation token for another user in the same session	Default
Perform volume maintenance tasks	Admins.
Profile single process	Default
Profile system performance	Admins.
Remove computer from a docking station	Default
Replace a process level token	Not Defined
Restore files and directories	Default
Shut down the system	Default

Synchronize directory service data	Not Defined
Take ownership of files or other objects	Admins.
Security Options	
Accounts	
Administrator account status	Default
Block Microsoft Accounts	Default
Guest account status	Disabled
Limit local use of blank passwords to console logon only	Enabled
Rename administrator account	Enabled
Rename guest account	Enabled
Audit	
Audit the access of global system objects	Disabled
Audit the use of Backup and Restore Privilege	Disabled
Force audit policy subcategory settings	Enabled
Shutdown system immediately if unable to log security	Disabled
Devices	
Allow undock without having to logon	Disabled
Allowed to format and eject removable media	Administrators
Prevent users from installing printer drivers	Enabled
Restrict CD ROM access	Enabled
Restrict floppy access	Disabled
Domain controller	
Allow server operators to schedule tasks	Dependent
LDAP server signing requirements	Require signature
Refuse machine account password changes	Disabled
Domain member	
Digitally encrypt or sign secure channel data (always)	Enabled
Digitally encrypt secure channel data (when possible)	Enabled
Digitally sign secure channel data (when possible)	Enabled
Disable machine account password changes	Disabled
Maximum machine account password age	30 days
Require strong session key	Enabled
Interactive logon	
Display user information when session is locked	Not Defined
Do not display last user name	Disabled
Do not require CTRL+ALT+DEL	Disabled
Machine account lockout threshold	Disabled
Machine inactivity limit	Disabled

Message text for users attempting to log on	Restricted to authorized users
Message title for users attempting to log on	Authorized users
Number of previous logons to cache	Do not change
Prompt user to change password before expiration	5 days
Require Domain Controller authentication to unlock	Enabled
Require smart card	Require smart card
Smart card removal behavior	Lock Worksation
Microsoft network client	
Digitally sign communications (always)	Enabled
Digitally sign communications (if server agrees)	Enabled
Send unencrypted password to third party smb servers	Disabled
Microsoft network server	
Amount of idle time required before suspending session	15 minutes or less
Attempt S4U2Self to obtain claim information	Not Defined
Digitally sign communications (always)	Disabled
Digitially sign communications (if server agrees)	Enabled
Disconnect clients when logon hours expire	Enabled
Server SPN target name validation level	Off
Network access	
Allow anonymous SID/name translation	Disabled
Do not allow enumeration of SAM accounts	Disabled
Do not allow anonymous enumeration of SAM accounts and shares	Enabled/Not Defined
Do not allow storage of passwords and credentials (for network authentication)	Disabled
Let Everyone permissions apply to anonymous users	Disabled
Named Pipes that can be accessed anonymously	Null value (enabled but no info)
Remote accesible registry paths	Null value (enabled but no info)
Remote accesible registry paths and sub paths	Null value (enabled but no info)
Restrict anonymous access to named pipes and shares	Enabled
Shares can be accessed anonymously	Null value (enabled but no info)
Sharing and security model for local accounts	Classic - local users authenticate as themselves.
Network security	
Allow Local System to use computer identity for NTLM	Not Defined
Allow Local System NULL session fallback	Default
Allow PKU2U authentication requests to this computer	Disabled/do not configure the policy
Configure encryption types allowed for Kerberos	Not Defined
Do not store LAN manager hash value on next password change	Enabled
Force logoff when logon hours expire	Disabled
LAN manager authentication level	Not Defined

LDAP client signing requirements	Require Signature
Minimum session security for NTLM SSP based (including secure RPC) clients	Enabled
Minimum session security for NTLM SSP based (including secure RPC) servers	Enabled
Add remote server exceptions	Not Defined
Add server exceptions in this domain	Not Defined
Audit incoming NTLM traffic	Not Defined
Audit NTLM authentication in this domain	Not Defined
Incoming NTLM traffic	Not Defined
NTLM authentication in this domain	Not Configured
Outgoing NTLM traffic to remove (remote?) servers	
Recovery console	
Allow automatic administrative logon	Disabled
Allow floppy copy and access to all drives and all folders	Disabled
Shutdown	
Allow system to be shutdown without having to logon	If server, disabled - if client, enabled
Clear virtual memory page file	Enabled
System cryptography	
Force strong key protection for user keys stored on computer	User must enter password each time key is used
Use FIPS compliant algorithms for encryption, hashing, and signing	Not Defined
System objects	
Require case insensitivity for non windows subsystems	Enabled
Strengthen default permissions of internal system objects	Enabled
System settings	
Optional subsystems	Null value
Use certificate rules on windows executables	Enabled
User Account Control	
Admin Approval Mode for the Built-in Administrator account	Disabled
Allow UIAccess applications to prompt for elevation	Disabled
Behavior of the elevation prompt for administrators in Admin Approval Mode	Prompt for consent for non-Windows Binaries
Behavior of the elevation prompt for standard users	Prompt for credentials
Detect application installations and prompt for elevation	Disabled
Only elevate executables that are signed	Disabled
Only elevate UIAccess applications that are installed in secure locations	Enabled
Run all administrators in Admin Approval Mode	Enabled
Switch to secure desktop when prompting for elevation	Enabled
Virtualize file and registry write failures to per-user locations	Enabled

NOTES

Services : computer programs that operat in the background

- Examples : DNS Client, Parental Controls, Windows Firewall

SERVICE STATES

- Automatic (Windows Firewall, Windows Update, Windows Defender)

Disabled ; IP Helper, SNMP Trap, MOST remote services(RPC is necessary), Server (If it is not a server).

- Manual

Configuring services : mmc > Services snap-in, Win+R > services.msc

* Go to services of your choice and double-click

- Cyberpatriot scoring engine checks if the service is started/stopped as the actual point

- Set to setup setting you dseire, and start/stop if needed

SHARING WITH COMPUTER USERS

- Sharing with computer's users, sharing with domain, sharing with FTP programs, sharing over the cloud.

(Sharing is giving access)

Run -> fsmgmt.msc

Default shares

- ADMIN$
- C$
- IPC$

Unshare anything not specified by the readme and is not one of the default shares

Add any shares if needed by right clicking and selecting "New Share..."

($ = Default share)

Admin, C, IPCs are all default ($)

Remove all unneccesary shares (unless specified otherwise) (Win+R -> Fsmgt.msc -> shares

Win+R -> Fsmgt.msc -> shares

Windows updates is a software update (rollout of security and software updates)

Keep up to date with patches for bugs that could poitentially break your system or let hackers in

UPDATING WINDOWS 10
- "Windows Update"{ in the search bar
- Settings -> Update & Security
- Updates are always automatic in Windows 10

Give me updates for other Microsoft products when I update Windows (Disa Disabled
Defer feature updates (Enabled) Enabled

Patch = Update
Service Pack - group of patches
Hotfix - file(s) that fix software problems (and fixes updates)

APPLICATION UPDATES
Google search
Might need to remove the older version first, before installing
Some programs don't have installers; you'll need to extract a zip, build your installer...

Every program allowed on the "readme" Update (Enabled) Enabled

APP UPDATE (BEWARE)
For some programs, you should hnot remove critical configurations or data thart are essential to whatever function your compu

SHOWING HIDDEN FILES
-view tab
-uncheck "hide protected operating systems files"
Delete Sketchy Files
-Any unauthorized media files
-Any txt files that say "cre3dit cards" or "password" etc.
-Check program files for things that aren't in programs and features
-Use ultrasearch (https://www.jam-software.com/ultrasearch/)

FILE PERMISIONS
-Right click on a folder or file -> properties -> Security
-Only needed to be done when specified to do so

R Can view (see contents) of a file

W — Can change information in a file
X — Can run the program

Basic Forensics — Looking at specific details for information
-Answers can be found through the use of Google;
-Basic Informaton about system
*Computer name, certain groups, certain users
*Can easily be searched through the image or the system information
-Decryption
*asks you to decrypt a certain image or file
*example: steganography of a picture — (using binary data in photo to hide information)
-File searching and file permissions
*asks about a certain file that is on the computer
*asks about who has certain rigfhts to a certain folder
*Example : who has access to (insert folder or file)
-Ports, PIDs, IPs, etc.
*harder level of forensics
* examples include
^what a port does (insert program) run on
^what an IP is (insert program) trying to connect to
^what is the PID of a backdoor

LOG YOUR ACTIVITY

INSTALLING
Feature > Internet Explorer

GETTING INTO SETTINGS
1. Gear icon
2. click on "Internet options"

SECURITY TAB
Security>>
-All should be in protected mode
Privacy>>
-Pop-up blocker
-Cookies set to second highest, or to accept first-party and block third-party

UPDATE (Sadly) About internet explorer > Install new versions auto

Plugins
-Internet Explorer > Gear icon > Manage Plug-Ins (remove all plug-ins)

FIREFOX
- Is a browser
- Doesn't consume as much processing power
- More secure
- A lot more focus on privacy than Google Chrome
- You can disable video autoplay
- Third-party cookies, cryptomining blocked by default
- Fingerprinting can be blocked
- Doesn't eat all your RAM

Updating>>
- You can simply run he installer, and Firefox will be automatically uninstall and reinstall for you as lo9ng as you don't have any
- Alternatively, you can update through menu (icon -> Help -> About Firefox)

How to get to settings (plugins)>>
1. Click on the 3 bars icon in the top right and then click Add-ons
2. Keep only necessary ones and update them

Firefox Quantum>>
- New look that Firefox got a little more than a year ago
- Firefox qQuantum is not supported for Windows 2008 or below

General Tab>>
-Set Firefox as defau;lt browser'
- Allow firefox to automatically install updates
- Set network settings

Home Tab>>
-Ensure that the homepage and new tabs are not leading into malicious sites

Search Tab>>
- Ensure search engine is a good one
- Do not provide search suggestions Setting: Do not provide

Security Tab>>

- Ensure content blocking is set well (use logic)
- Send "Do Not Track" signal
- Do not use a master password
- Do not autofill addresses
- When using the address bar, don't suggest
- Block pop-up windows
- Warn you when websites try to install add-ons
- Prevent accessibility services from accessing your browser
- Block dangerous and deceptive content
- Block dangerous downloads
- Warn you about unwanted and uncommon software

Administrator access link : https://www.technipages.com/windows-administrator-account-login-screen

56d7006ea618f208290b502749c441d9

Forensics questions 1, 2, 3 (10 pts each)
Remove unauthorized user (5 pts each)
Create user accouts ()

ADD/DELETE USERS
GUI:
- Use lusrmgr.msc or compmgmt.msc
CMD:
Adding > net user (user) add
Removing > net user (user) delete
POWERSHELL
Adding: New-LocalUser
<nlu - name (username)>
Removing: Remove-LocalUser
<rlu -name (username)>
DO NOT REQUIRE CTRL/ALT/DELETE
Password> CleanFish749
Security settings > password policies
Secpol.msc (search bar)
Read "ReadMe" for reference

d

FILE SHARING

run : compmgmt.msc
Direstions >Computer Managment>System Tools>Shared Folders

PROGRAMS
Run : control.exe
Directions > Control Panel> Programs>Programs an Features

COMPETITION
1. Firewall (on)
2. Compare computer users vs. README
a. delete unauthorized
b. switch admin and user accounts to correct authority

lusrmgr.msc
secpol.msc

uscyberpatriot.org/competition/current-competition

Control Panel
Security + Maintenance tells what's up with PC
User Account Control (under Sec + Main) lets you choose when to be notified of changes
Local Users:
-Can only be logged on by one computer
-Managed through Local Users and Groups
LUaG accessed by:
Control Panel-> System & Sec ->Admin tools ->
Checking user properties
-Add users: User folder -> Right click New user
-Remove users: user folder, right click on a user, delete user
-Make admin: groups folder, click on Administrators group, click add, type in user name
-Remove admin: Groups folder, Click on Administrators group, Click user name, Click remove

-Checking groups: Groups folder, double click on group name to configure
Default Guest and Default Administrator Configurations:
-Disable
-Rename, Password expires, or User cannot change password
Local User Configuration: READ THE README, Remove/Disable any unauthorized users, Add any needed users,
Local Group Management: Groups folder, double click on group name to configure, Remove/Add administrators/us
Managing users using CMD:
-Check users: net user
-Check groups: net localgroup
-Add user: net user [username] [password] /add
-Change password: net user [username] [new password]
-Delete user: net user [username] /delete
-Add User to Group: net localgroup [groupname] [username] /add

Local Security Policy

Run: Win+r, secpol.msc
Control Panel: System & Sec, Administrative tools, Local Security Policy
MMC: Win+R, mmc, Add/remove snap-in, Local Security Policy

Password Policies

Enforce password history: 10
Maximum password age: 90
Minimum password age: 30
Minimum password length: 14
Password must meet complexity requirements: True
Store with reversible encryption: False

Account Lockout Policy

Account Lockout duration: 30 minutes
Account lockout threshold: 10 attempts
Reset lockout counter after: 30 minutes

Local Policies

Audit: Everything Success/Failure
Security Options: Do not require CTRL+AlT+DEL [disabled]
Security Options: Clear virtual memory page file [enabled]

Services

Anything that keeps running no matter what
Examples: DNS Client, Parental Controls, Windows Firewall
Service States: Automatic (service starts automatically), Manual (service will not run until called), Disabled (Service
Disable unless specified: Telnet, IP Helper, SNMP Trap, MOST Remote services (RPC is necessary), Server (if not
Automatic unless specified: Windows Firewall, Windows Update, Windows Defender

Configuring Services:
mmc > services snap-in
Win+R > services.msc
Go to service of choice and right-click for properties

Shares
Hidden shares are important, and you need to search the full file name to find it
Permissions found in Properties
Updates
Positives are keeping up to date with patches for bugs that can let hackers in.
Update whenever possible during competitions.
Check box: give me updates for other Microsoft products
Update an app
Use google search
File Management
Hidden files
View tab> show hidden files and folders >uncheck hide protected operating system files
Win+R command is control.exe folders
Delete unauthorized media files such as .mp3, .mp4, .txt, etc
Delete sketchy files, you'll know them when you see them
Show extensions by clicking File Type and it will be organized.
Search *.mp3 and .mp3
File Permissions
Right click on a folder or file > properties > Security
Only do when specified to do so
Programs/Tools
Programs help secure or monitor your system
Some malware bytes help find the backdoor for you
Everything, UltraSearch are file searching
Avast, MalwareBytes are security
Notepad++, MBSA (security) are possible requirements
LSP/Services Template
Open MMC
Add Security Config and Security Template
Set up like LSP, save, and import file
Click Configure Computer Now and do stuff i guess?
Other stuff?
Windows Server Manager replaces the control panel

Remove features through server manager
On Windows Server turn on ESC?
Server 2019 includes ATP and
Windows Server notes (v. important since I'm the server person)
Roles + Features
Features are stuff like bitlocker, telnet, rip listener, powershell
Manage using appwiz.cpl or go under manage and use add/remove roles and features
Server
Configuring and securing web browsers
Internet explorer- use recommended security settings
Windows 10 check the box on Windows Features to install Internet Explorer if not already installed.
Set internet explorer settings by clicking gear icon and clicking internet options
Set all to highest except for trusted sites, which should be set to medium
All should be in Protected mode
Privacy tab: cookies to second highest, accept first-party and block third-party
Pop-up blocker should be on
Plugins:
IE>Gear icon> Manage plugins
Update to latest version and restart
FIREFOX:
Update by going to menu>help>about Firefox
Or, uninstall and re-install
Get to settings by hitting 3 bars in top right
General>Startup>Set Firefox as default browser, Allow Firefox to automatically install updates, set network settings
Firefox Quantum is a thing
Search tab>Ensure search engine is a good one, Do not provide search suggestions
Security>content blocking is set well, send do not track signal, DO NOT USE A MASTER PASSWORD, do not auto
Plugins>click 3 bars and click add-ons, keep only necessary ones and update them
IF STUCK
Checklist
Reread README
Compare scoring reports
Get a Linux and/or Cisco person to look at it
Take a break (run away with us for the summer lets go upstate)
Go to the band room and scream
Anti-virus stuff
MalwareBytes
Avast

Task Scheduler

Task Scheduler can be compromised and anti-virus programs won't catch it.

Task Scheduler can be opened by mmc or WinR> taskschd.msc

Show hidden tasks under view

Create tasks on the right side using wizard

Active window shows tasks that have been started

Identify bad task and get rid of it

Look for name, trigger, and action

If it is called malware, is triggered whenever you log on, and turns your firewall off, it's probably a backdoor of some

GPEDIT

GPEDIT is the rest of the stuff that Secpol doesn't show SEARCH GPEDIT STUFF -->

Frickin ton of settings but most are obvious View settings on scale of severity -->

LSP is a part of GPEDIT

WinR>gpedit.msc

Turn off autoplay (Computer Configuration > Administrative Templates > Windows Components > Autoplay Policies

Disable users connect remotely using remote desktop unless remote is required. How to disable: (Computer Config

"Allow Cortana" disabled

Comp config>Admin templates> windows components>search

User config>Admin temps>control panel>personalization

"Enable screen saver" enabled

Comp config>admin temps>network>network connections>windows firewall

Set "Windows firewall:protect all network connections" to enabled

Comp config>Admin temps>Windows Components>Remote Desktop Services>RD session host>security

Require secure RPC communication Enabled

Require user authentication for remote connections by using Network Level Authentication Enabled

Comp config>windows settings>security settings

Restart computer or run gpupdate/force (cmd)

LPGO

Tool for importing and exporting group policy settings

Search online and download

Command-line utility, ask Linux for help if tricky

Download LGPO.exe at https://www.microsoft.com/en-us/download/details.aspx?id=55319

Open cmd with admin privileges and go to directory with LGPO.exe

Type: lgpo /b <path where you want to save policy>

Event viewer

Its cool i guess

Each log will have headers that contain information about event

It's in mmc

Backdoors

Hard to find right away but it gets easier over time

Find active backdoors using task manager and look for netcat/nc.exe/netstat/whatever

Admin cmd>netstat-anbo

Backdoors try to hide as regular stuff

Also called rootkits, can hide from task manager, netstat, and registry

Nc.exe proably backdoor

Other stuff

Figure out how to get antimalware onto image

disable autoplay in settings or gpedit

winR wf.msc make sure firewall is on for all but inbound more important

Servers need to have ports open

Suspicious ports, programs, and locations must be blocked

netstat -ano

Update 7-zip web and Notepad ++

NetCat + CCleaner + Epic Games Launcher Remove

Unauthorized media and hidden stuff removed

Show hidden files = file explorer and hidden files

Default user is disabled(guest, admin, etc. (unless its you))

Turn off Ctrl Alt Del

Don't run Autoplay

Cortana Search disabled

Password 14 characters

IP service disabled

Unshared c: drive

Only if readme says, disable search, but depends

Enable block dangerous FireFox stuff

Block popup ads

5 points-Success Failure audit policies

Forensics Question 1 Correct - 7 pts

Forensics Question 2 Correct - 7 pts

Forensics Question 3 Correct - 7 pts

Removed cbakis from users - 8 pts

User zdang removed from Egg Inc Employees - 7 pts

Account management successes and failures are logged - 5 pts

Prohibit access to Control Panel and PC settings

Remove access to use all Windows Update featur

CD-ROM access us restricted to locally logged-on users only - 5 pts

Clear virtual memory page file has been enabled - 5 pts

A secure minimum password age has been set - 5 pts

A secure lockout threshold exists - 5 pts

C: drive unshared - 6 pts

Removed unauthorized keylogger - 5 pts

CCleaner is uninstalled - 10 pts

Remote Assistance has been disabled via GPEDIT - 5 pts

Windows 7 Games are uninstalled - 10 pts

ROM : Read only memory

Forensics Question 1 Correct - 7 pts
Forensics Question 2 Correct - 7 pts
Forensics Question 3 Correct - 7 pts
Removed cbakis from users - 8 pts
User zdang removed from Egg Inc Employees - 7 pts
Account management successes and failures are logged - 5 pts
A secure minimum password age has been set - 5 pts
A secure lockout threshold exists - 5 pts
Start Buttons folder is removed - 10 pts
CCleaner is uninstalled - 10 pts
Windows 7 Games are uninstalled - 10 pts

Remote desktop

To gain access to Control panel and Settings, go through "gpedit.msc"

3 main types of networking-NAT, Host-Only, and bridged

If SMB1 is on..... TURN IT OFF

Use SMB2 or SMB3

hi

imagine scrolling down here

Notes
Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy
Necessary
Necessary
Necessary
Necessary
Necessary
Necessary
Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy
Necessary
Necessary
Necessary
Computer Configuration\Windows Settings\Security Settings\Account Policies\Kerberos Policy
Security Settings\Local Policies\Audit Policy
Necessary
Necessary
Necessary
Necessary
Necessary
Necessary
Necessary
Necessary
Necessary
Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment

https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/enable-the-lock-pages-in-memory-option-windows?view=sql-server-ver15

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options

By default, this setting is Not Defined on domain controllers and Enabled on stand-alone servers.

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options

Necessary

IIIII

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options

Necessary

Necessary

If you run applications that are not Windows Vista-compliant, enable this security policy to prevent the possibility that these older applications could write data to unsecure locations.
If you only run at least Windows Vista–compliant applications, this feature is unnecessary so you can disable this policy.

Win+R -> Fsmgt.msc -> shares

Animal farm george orwell, anythign by brandon sanderson especially stormlight archive (3k pages each, really good dystopian fantasy novel)

uter serves. It's never a bad idea to BACKUP THE PROGRAM FOLDER beforte you start updating

matically

firefox windows open\

Change passwords of all users (except self), Password expires

ers as required, ONLY GUEST should be in Guest group, Unless specified no one is in Remote Desktop Users group

cannot start until set to Automatic or Manual)

needed, Scorpio needs Server)

fill addresses, block pop-up windows, warn when websites try to install add-ons, prevent accessibility aervices from accessing browser, block dangerous and decep

e sort

https://gpsearch.azurewebsites.net/

https://www.stigviewer.com/

- Computer Configuration > Administrative Templates > Windows Components > Autoplay Policies
  - "Turn off Autoplay" – Enabled for All Drives
- Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Connections
  - "Allow users to connect remotely by using Remote Desktop Services" – Disabled
  - // * IF REMOTE IS NOT REQUIRED, else Enabled

)

guration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Connections "Allow users to connect re

- User Configuration > Administrative Templates > Control Panel > Personalization
  - "Enable screen saver" - Enabled
- User Configuration > Administrative Templates > Control Panel > Personalization
  - "Password protect the screen saver" - Enabled
- Computer Configuration > Administrative Templates > Network > Network Connections > Windows Firewall
  - For all profiles, set "Windows Firewall: Protect all network connections" to Enabled

- Computer Configuration > Administrative Templates > Components > Remote Desktop Services > Remote De Session Host > Security
  - "Require secure RPC communication" – Enabled
  - "Require user authentication for remote connectio Network Level Authentication" – Enabled
- Computer Configuration > Windows Settings > Securit
  - GPEDIT LSP

Don't forget to either restart your computer OR run "gpupdate /force" (as a command)

es

otive content, block dangerous downloads, warn about unwanted and uncommon software

emotely using Remote Desktop Services" Disabled)