CyberPatriot Windows Checklist

[Redacted] Team [Redacted]

| Version | Date | Author | Comments |
| --- | --- | --- | --- |
| 1.0 | 11/23/2018 | [Redacted] | Original Version |
| 1.0.1 | 1/10/2019 | [Redacted] | Added some server stuff, reorganized the checklist, and added more forensics |
| 1.1 | 1/29/2019 | [Redacted] | More forensics and some critical services |
| 2.0 | 12/12/2019 | [Redacted] | NATIONALS OR NOTHIN BITCHES |

# Competition Prep

* Bump up RAM to 4-8GB
* Increase CPU cores from 1 to 2 (or maybe even 3 if you’re feeling wild)
* Main Team ID: [Redacted]

# Starting the Competition

* READ THE README
  + Take notes on what is required
    - What programs need to stay?
    - What programs need to be enabled?
    - What user needs to be created?
    - Does a group have to be created?
    - Does a user have to be added to a group?
* Take a photo of the Readme before you start (Admin passes and hints) (Maybe use snipping tool)

# Updates

* Just start Windows update now to save time.
* Set Windows Update to Automatic download/install
  + Search **Windows Update**
  + Set it to Automatic download/install
  + Turn on “Receive updates for other Microsoft products when you update Windows”
  + Turn on “Download updates over metered connections”
  + Scroll down to the bottom and click “Delivery Optimization”
    - Turn off everything
* Server 2016
  + Control Panel
  + Search: **Windows Update**
  + Change settings
  + Check for updates
  + Install any service packs
  + Restart

# Forensics Questions

* Disable hidden files and folder
  + Search **File Explorer Options**
  + Go to the **View** tab
  + Set **Hidden files and folders** to **Show hidden files, folders, and drives**
  + Uncheck **Hide extensions for known file types**
* Read the question fully, if you do not understand the question ask another teammate
* Use Google dammit
* How to check if a user is a part of a group
  + Windows+R, type **lusrmgr.msc** and hit enter
  + Click **Groups**
  + Double-click the group that you need to check (Shows all users in group)
* Encoded message (CHECK ALL OF THESE!!)
  + Hex
    - <https://www.rapidtables.com/convert/number/hex-to-ascii.html>
  + Other bases (Run through all of these if hex did not work)
    - <https://www.geocachingtoolbox.com/index.php?page=asciiConversion>
    - Set **From:** to your desired option
    - Set **To:** to ASCII
  + Upload file through encoder
    - <https://www.base64decode.org/> (Scroll down the webpage)
  + You may have to use the links above to encode a message
* Find a port that a program is listening on (most commonly nc.exe)
  + Run CMD
  + run **netstat -ab**
* Checksum of a file
  + MD5
    - https://defuse.ca/checksums.htm
  + SHA1
    - https://defuse.ca/checksums.htm
  + SHA256
    - https://defuse.ca/checksums.htm
  + SHA384
    - https://defuse.ca/checksums.htm
  + SHA512
    - <https://defuse.ca/checksums.htm>
  + You might have to Google other hashes if needed
* SID of a user
  + Open CMD as an admin
  + Run this command **WMIC useraccount get name,sid**
* Revision number of a program or .exe
  + The revision number are the last few digits
  + vX.XX.XXX.XXXX
* Hidden text in photos
  + Run it through steghide.
* (Will add here as we continue)
* **TAKE PHOTO OF FORENSICS QUESTION**

# Script

* [Redacted]
* [Redacted]

# Users and Groups

* Accessed by doing Windows+R, type **lusrmgr.msc** and hit enter

## Users

* Make sure that **ALLOWED USERS AREN’T DISABLED**
* Make sure that users
* Disable unmentioned users (Make sure they aren’t an account that needs to be created)***DO NOT DELETE THEM!***
* For **EVERY** account
  + Follow the instructions in **How\_To\_Batch\_Reset\_Passwords.txt**
  + Make sure **Password never expires** is UNCHECKED unless specified by the readme
  + Make sure **Password must be changed on next login** is checked
  + Change password to Cyb3rPatri0t!

## Groups, THIS IS VERY IMPORTANT TO LISTEN UP CHILDREN

* Administrator Group
  + THIS IS THE MOST IMPORTANT GROUP
  + Add authorized users to the group
  + Remove any unauthorized users
* Users Group
  + Purge malicious users
  + Add authorized users
* Remote Users Group
  + This is for the remote desktop users, etc.
  + Replace **Everyone** with **Users,** this is more secure.
* Do not delete any groups related to CyberPatriot
* No one should be in any groups unless specified by the readme
* If you discover “custom” groups, ensure the users in the groups are not being granted “extra” rights by being embedded in other groups or through explicit User Rights Assignment in Local Security Policy

# Windows Programs and Features

* Windows+R, type **optionalfeatures**
* Uncheck:
  + Games
  + Media Features
  + Anything IIS (unless specified by readme)
  + Active directory lightweight directory services
  + Hyper-V
  + RIP Listener
  + Telnet (unless specified by readme)
  + SMB (unless specified by readme)
  + File and Printer Sharing
  + File-sharing
  + TFTP Client
  + Kill anything else that looks weird.
* Check:
  + Internet Explorer 11

# Privacy

* Search **Privacy**
  + Turn off everything

# Server Roles: IIS, FTP (This is meant for Server versions of Windows)

## IIS

* Configuration is accessed under the IIS Manager (assuming IIS is installed)
* Accessible from Server Manager, with the Role of Web Services

## Install/Modules

* IIS has over 40 modules, so this is tricky because the modules may be needed.
* That said, check against readme and google to see if any may be “unnecessary” or unwanted

## Request Filtering

* Ensure that request filtering rules are enabled (With the default settings)

## Authentication

* Basic, Windows Authentication, Forms Authentication, Anonymous
* If you use Windows authentication, turn on extended protection.
* If Basic Authentication is enabled, ensure the system is using SSL certs
* It is generally not advisable to allow Anonymous authentication along with another authentication type for the same website
* Disable anonymous access to server directories and resources.
* Do not allow anonymous writes to the server.

## FTP

• Configuration is accessed under the IIS Manager (assuming IIS is installed)

• Accessible from Server Manager, with the Role of Web Services

• Network Protocol = SSL

• Account running the service

• Users granted access

• Permissions to directory

• CyberPatriot will want you to disable anonymous right unless explicitly mentioned

## File Server

Configuration is accessed under Server Manager (assuming it is installed)

You can also get a quick peek under ‘net share” command from the CMD prompt

• Share permissions / Users granted access

• Permissions to directory

# Software

* Windows+R, type **appwiz.cpl**
  + Purge any applications not specified by the readme (Use your head with this)
* Program Files (x86), Program Files, and Program Data
  + Look for suspicious folders or weird names.
    - Gibberish names
    - Keylogger
    - -crack, password, ninja, logger, etc.
    - Hidden folders (Except the **Default** one)
    - Or just anything you’ve never heard of
  + CHECK THE README BEFORE DELETING
* Install any software specified by the readme, **DO THIS NOW**
* Verify the following programs are **not on the system**
  + TightVNC Server, BitTornado, John the Ripper, Advanced Port Scanner, Chicken invaders, KNCTR, Beware IRC server, Hashcat, Itunes, TeamViewer, Driver Support, Angry Ip scanner, uTorrent, Kodi, Nmap, Reimage Repair, BitComet, Arcade Lines, ophcrack, MyCleanPC PC Optimizer, Wireshark, Tonido Server, BoomBox Radio Player, Abyss Web Server, Home Web Server, SuperScan, HTTP Explorer, Open TFTP Server
* Verify that the latest verions of required software is installed

# Media Files

## ShellBagsView

* So shellbags show last open folders. For some reason CP doesn’t clear this before comp.
  + Download here: <https://www.nirsoft.net/utils/shellbagsview.zip>
  + So yeah, find them media files

## Everything

* So everything indexes the entire file system almost instantly. Basically you type in the filename you want to search for at the top.
  + \*.mp3, \*.zip, \*.csv, \*.bat, \*.exe, \*.gif, \*.jpeg, \*.jpg, \*.mp4, \*.msi, \*.png, \*.php, \*.txt, \*.sh, \*.wav, \*.ps1, audio:, zip:, exe:, doc:, pic:, video:, !. (Files with no extension)

# Screen Saver

* Windows+R, **control desk.cpl,,@screensaver**
* Screen Saver
  + Blank
  + Wait **1 minute**
  + Turn on **On resume, display logon screen**

# Data Execution Prevention

* Windows+R, **SystemPropertiesAdvanced**
* Click the **settings under performance**
* Click the **Data Execution Prevention** tab
* Click **Turn on DEP for all programs and services except those I select:**

# Automatic Updates

## Firefox

* Click at the top right and click options
  + General Tab
    - Check **Automatically install updates**
    - Check **Use a background service to install updates**
    - Check **Automatically update search engines**

## Notepad++

* First update Notepad++
  + Click **?** on the top (very right)
  + Click **Update Notepad++**
* Click **Settings** (Middle top)
  + Click **Preferences**
  + Go to **MISC.**
  + Check **Enable Notepad++ auto-updater**

## Thunderbird

* First update Thunderbird
  + Click 
  + Click **Help**
  + Click **About Thunderbird**

## PuTTY

* Download latest version here: <https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>

## LibreOffice

* Open LibreOffice Writer
* Tools > Options > Online Update
  + Turn on **Check for updates automatically**
  + Check **Everyday**
  + Click **Download updates automatically**
  + Uncheck **Send OS version and basic hardware information**
  + Click **Check Now**

## IfranView

* You can install a new version over the old one, no need to uninstall
  + <https://www.irfanview.com/main_download_engl.htm>

## VLC

* First update VLC, **Help > Check for Updates**

## Java

* Open **Configure Java** as **administrator**
* Goto **Updates**
  + Check **Notify before installing**
  + Check **Automatic Updates**
  + Click **Update Now**

## GIMP

* Download latest version here: <https://www.gimp.org/downloads/>

## FileZilla

* Edit > Settings > Updates

## TortoiseHG

* Download latest version here: <https://tortoisegit.org/download/>

## Adobe Reader

* Help > Check for Updates
* Verify that HKLM\SOFTWARE\WOW6432Node\Policies\Adobe\(product name)\(version)\FeatureLockdown\bUpdater is set to 0

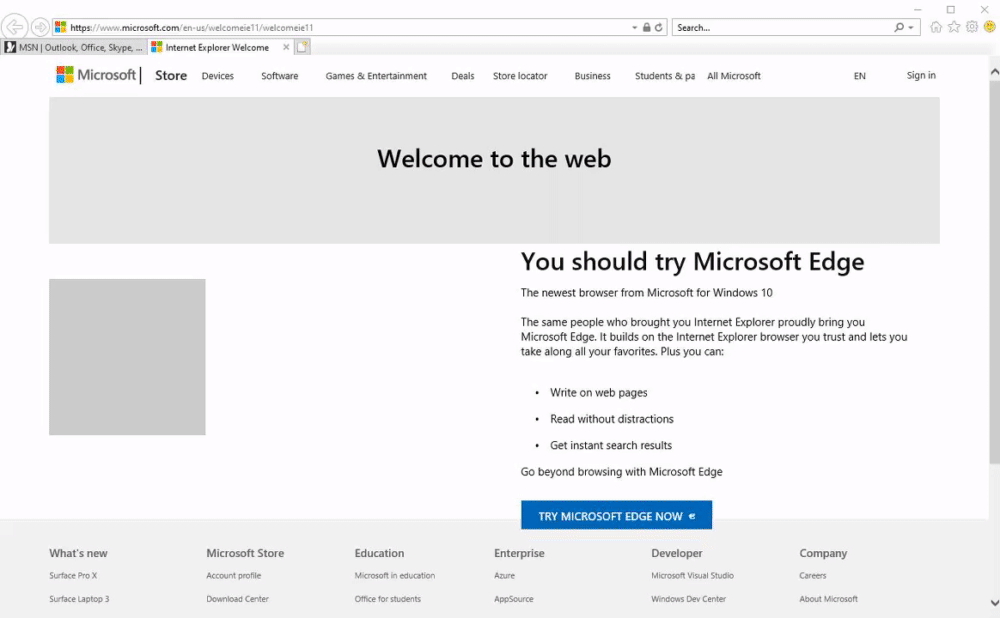
# Web Browsers

## Firefox

* Pre-Quantum (Rounded tabs)
  + Click the at the top-right of the screen
  + Click the question mark (May be under “help”)
  + Click **About Firefox**
  + Update it as many times as you need too (You may need to repeat this process)
  + Move onto the Quantum section to secure the browser
* Quantum
  + Click at the top right and click options
    - General Tab
      * Check the **Always check if Firefox is your default browser** (one of the first options)
      * Search **Homepage**
        + Set **Homepage and new windows** to **Blank Page**
        + Set **New tabs** to **Blank Page**
      * Search **Updates**
        + Check **Automatically install updates**
        + Check **Use a background service to install updates**
        + Check **Automatically update search engines**
    - Privacy & Security Tab
      * Forms & Passwords
        + Uncheck **Ask to save logins and passwords for websites**
        + Uncheck **Use a master password**
        + Uncheck **Autofill addresses**
      * History
        + Firefox will **Never remember history**
      * Address Bar
        + Uncheck **Browsing history**
        + Uncheck **Bookmarks**
        + Uncheck **Open tabs**
      * Permissions
        + Check **Block pop-up windows**
        + Check **Warn you when websites try to install add-ons**
      * Firefox Data Collection and Use
        + Uncheck **Allow Firefox to send technical and interaction data to Mozilla**
        + Uncheck **Allow Firefox to send backlogged crash reports on your behalf**
      * Security
        + Check **Block dangerous and deceptive content**
        + Check **Block dangerous downloads**
        + Check **Warn you about unwanted and uncommon software**
      * Certificates
        + Check **Ask you every time**
        + Check **Query OCSP responder servers to confirm the current validity of certificates**
    - Type **about:addons** in the address bar
      * Disable everything under the Add-ons tab (Unless specified in readme)
      * Disable everything under the plugins tab (Unless specified in readme)

## Internet Explorer

* Tap ALT and hover over **Tools** 
  + Hover over **Windows Defender SmartScreen**
  + Click **Turn on Windows Defender SmartScreen**

****

* Click the gear icon in the top right
* Select **Internet Options**
* General Tab
  + Click **Use default** for the homepage
  + Check **Delete browsing history on exit**
* Security Tab
  + Set the security bar to high for all settings
  + Check **Enable Protected Mode** for all settings
* Privacy Tab
  + Check **Never allow websites to request your physical location**
  + Check **Turn on Pop-up Blocker**
  + Check **Disable toolbars and extensions when InPrivate Browsing starts**
* Advanced Tab
  + Accelerated Graphics
    - Uncheck everything
  + Accessibility
    - Uncheck everything
  + Browsing
    - Check **Disable script debugging (Internet Explorer)**
    - Check **Disable script debugging (other)**
    - Uncheck **Tell me if Internet Explorer is not the default web browser**
    - Underline links
      * Set it to **Always**
  + HTTP settings
    - Check all of the options
  + International
    - Don’t change
  + Multimedia
    - Don’t change
  + Security
    - Uncheck both **Allow active content…**
    - Uncheck **Allow software to run or install even when…**
    - Check all three **Check for…** options
    - Check **Empty temporary internet files…**
    - Check **Enable Windows Defender SmartScreen**
    - Enable everything through **Send Do Not Track requests…**
    - Uncheck **Use SSL 3.0**
    - Uncheck **Use TLS 1.0**
    - Check Use **TLS 1.1**
    - Check Use **TLS 1.2**
    - Check all **three Warn…** options
    - Check **Enable Enhanced Protected Mode**
* Click the gear icon
  + Click **Manage add-ons**
    - Disable everything not mentioned in the readme
* FOR SERVER ONLY
  + Open **Server Manager**
  + Click **Local Server**
  + In the properties textbox, find **IE: Enhanced Security Configuration**
    - Turn it on for Admins and Users

# Windows Firewall

* Make sure firewall is on. (Security Center/Action center)
  + Can be disabled in snap-in, make sure to check there if it doesn’t work before escalating to group policy as below
* Access through Windows Key R -> mmc.exe -> File -> Add/Remove Snap-In -> Windows Firewall with Advanced Security
  + Make sure all profiles are enabled
  + Disable exceptions and inbound connections
    - Inbound connections -> Ctrl A -> Right Click -> Disable Rule is pretty dang good
  + Only Inbound connections allowed should be for specific services required by readme
  + If possible, add an exception for the application instead of enabling the firewall rule
* Might be able to fix errors by going through event viewer
* Troubleshooting
  + Group Policy
  + Can be disabled through gpedit.msc in administrative templates -> Network -> Network Connections -> Firewall -> Standard Profile, Domain Profile
  + After the change, run gpupdate /force in administrator powershell
* Right click on Windows Firewall with Advanced Security, -> Properties
* Under Logging, Select Customize, and ensure logging of Dropped packets is set to Yes
* Log file is located at “%systemroot%\system32\LogFiles\Firewall\pfirewall.log”
* Also check for errors by going through event viewer
* If the service is disabled, the snap in will not open.
* If the snap-in (wf.msc) will not open, the firewall is disabled in policy.

## Malwarebytes

* Install (if not already) and run it
* Setup automated scans
* Look at results and delete malware
* doawnload avast

## HitmanPro

* This is a very OP tool. It finds literally everything wrong in terms of malware
* <https://www.bleepingcomputer.com/download/hitmanpro/>

## Windows Defender (Windows 10)

* ***NEEDS TO BE ENABLED!***
* Control Panel > Windows Defender
  + Then go to **Updates and Security** (This is in another windows)
    - Set options for Real Time Protection, Cloud-based protection, and Enhanced Notifications
    - Also enable Windows Defender Offline (About a 15 minute process)
  + Launch Tools - Options
    - Enable **Automatically scan my computer**
    - Use Default **Recommended Actions**
    - Enable **Real Time Protection**
    - Advanced
      * Enable **Use Heuristics**
      * Enable **Scan Archive Files**
    - Update definitions
    - Run a quickscan.

# Users Account Control

* Windows+R, type **C:\Windows\System32\UserAccountControlSettings.exe** and run
  + Set the bar to the highest setting possible

# Services

* Windows+R, type **services.msc** and run
* Verify the following services are running, if they are not start them and set them to auto
  + Windows Defender Firewall
  + Security Center
  + Windows Update
  + Windows Event Logger
  + Mozilla Maintenance Service
* Be careful, disabling one of these can screw things up hard.
* If you are wondering what a service does, check this link out.
  + <http://www.blackviper.com/windows-services/>
* The following list may look intimidating, but remember these are **VERY IMPORTANT TO DISABLE**

| Service Name | Function | State |
| --- | --- | --- |
|  |  |  |
| Adobe Update |  | Enabled |
| Application Host Helper Service | Application Experience functionality | Disabled |
| Application Management | Manages UX | Disabled |
| ASP.NET State Service | Monitors ASP.NET framework | Disabled |
| Bitlocker Drive Encryption | Bitlocker functionality | Disabled unless needed on image |
| Bluetooth support service | Bluetooth | Disabled |
| Branchcache | Cross-host caching | Disabled |
| Certificate Propagation Service | Smart card cryptography | Disabled |
| Computer Browser | Network discovery protocol | Disabled |
| HomeGroup listener | Homegroup functionality | Disabled |
| HomeGroup provider | Homegroup functionality | Disabled |
| IIS Admin Service | Web server administration | Disabled unless needed on image |
| IIS | Web server | Disabled unless needed on image |
| IP Helper | IPv4 and IPv6 autoconfig/help | Disabled |
| Internet connection sharing (ICS) | Internet connection sharing | Disabled |
| LPD Service | Legacy printing. | Disabled |
| Media Center Extender Service | Media server mirroring | Disabled |
| Message Queuing | Messaging over IP | Disabled |
| Microsoft FTP Service | File Transfer Protocol | Disabled unless needed on image |
| Microsoft iSCSI Service | iSCSI | Disabled |
| Mozilla Update Service |  | Enabled |
| Net.Msmq Listener Adapter | MSMQ TCP adapter functionality | Disabled |
| Net.Pipe Listener Adapter | Pipe adapter functionality | Disabled |
| Net.Tcp Listener Adapter | TCP adapter functionality | Disabled |
| Net.Tcp Port Sharing Service | Port sharing functionality | Disabled |
| Netlogon | Manages domain logins for Workstation scv. | Disabled unless needed on image |
| Offline Files | Offline filesharing functionality | Disabled |
| Remote Access Auto Connection Manager | RDP dependency | Disabled unless needed on image |
| Remote Access Connection Manager | RDP dependency | Disabled unless needed on image |
| Remote Desktop Configuration | RDP dependency | Disabled unless needed on image |
| Remote Desktop Services | RDP host service | Disabled unless needed on image |
| Remote Desktop Service Usermode Port Redirector | RDP networking functionality | Disabled unless needed on image |
| Print Spooler | Printing | Disabled |
| Remote Access Management connection manager | Consolidation for remote desktop functionality | Disabled unless needed on image |
| Remote Registry | Remote Access to registry | Disabled |
| RIP Listener | Distance vector routing functionality | Disabled |
| Routing and Remote Access | Routing for remote access protocols | Disabled |
| RPC Locator | RPC network discovery | Disabled |
| Server | File and Printer sharing on LAN | Disabled unless needed on image |
| Secondary Logon | Allows concurrent logons | Disabled |
| Simple TCP/IP services | Legacy internet functionality | Disabled |
| SNMP service | Mailing | Disabled |
| SNMP trap | Mailing infrastructure/backbone functionality | Disabled |
| SSDP Discovery |  | Disabled |
| Web Management Service | IIS management | Disabled unless needed on image |
| Windows Media Player Network Sharing | Limited media server functionality | Disabled unless needed on image |
| Windows Update |  | Enabled |
| Telephony |  | Disabled |
| Telnet | Remote console functionality | Disabled unless needed on image |
| TFTP | File Transfer Protocol | Disabled unless needed on image |
| Windows Remote Management | Remote Desktop | Disabled unless needed on image |
| XBOX services | X-Box dependencies | Disabled |
| Xbox Live Game Save |  | Disabled |
| Application Layer Gateway Service | Legacy and unneeded | Disabled |
| Client for NFS | Network file system client | Disabled unless needed on image |
| Interactive Services Detection | Compatibility | Disabled |
| Natural Authentication | Biometric authentication | Disabled |
| Microsoft Keyboard Filter | iSCSI compatibility | Disabled |
| Multipoint repair service | Distributed LAN server functionality | Disabled |
| Multipoint Service | Distributed LAN server functionality | Disabled |
| Peer Name Resolution Protocol | DNS discovery for peer-to-peer functionality | Disabled |
| Peer Networking grouping | Peer-to-peer networking functionality | Disabled |
| Peer networking identity manager | Peer-to-peer networking functionality | Disabled |
| Printer extensions and notifications | Printing | Disabled |
| Retail demo service | Retail demo functionality | Disabled |
| Shared PC Account manager | Laptop/Tablet functionality | Disabled |
| Spatial Data Service | Bing APIs | Disabled |
| User Profile Service | Active directory logon | Disabled |
| UPnP Device Host |  | Disabled |
| World Wide Web Publishing |  | Disable unless needed |
| Windows Event Log |  | Enabled |
| Windows Defender Firewall |  | Enabled |

# Local Security Policy

## Account Policy

* Windows+R, type **secpol.msc,** and click **Account Policies**
* Verify that is matches this

| Setting Title | Desired Setting |
| --- | --- |
| **Password Policy tab** |  |
| Enforce Password History | 5 |
| Max Password Age | 60 |
| Minimum password Age | 30 |
| Minimum Password Length | 8 |
| Store passwords using reversible encryption | Disabled |
| Complexity Requirements | Enabled |
| **Account Lockout Policy** |  |
| Account Lockout threshold | 5 |
| Other two items | 30 mins |

## 

## Audit Policy

* Audits everything important on the computer.
* Very important that everything is enabled.

| Setting Title | Desired Setting |
| --- | --- |
| Audit account logon events | Success, Failure |
| Audit account management | Success, Failure |
| Audit directory service access | Success, Failure |
| Audit logon events | Success, Failure |
| Audit object access | Success, Failure |
| Audit policy change | Success, Failure |
| Audit privilege use | Success, Failure |
| Audit process tracking | Success, Failure |
| Audit system events | Success, Failure |

## User Rights Assignment

* Direct extreme scrutiny at the **Everyone** object
* Check to make sure that CyberPatriot groups don't have any permissions.
* Don’t screw with CyberPatriot settings
* Set everything to the following:

| Setting Title | Function | Default Setting | Desired Setting |
| --- | --- | --- | --- |
| Access Credential Manager as a trusted caller | VERY dangerous. Allows access to plaintext passwords | <blank> | <blank> |
| Access this computer from the network | Allows console and RDP sessions from the network with broad permissions | Administrators, Users, Backup Operators | Blank unless specified by readme |
| Act as part of the operating system | Act with system permissions (godmode) | <blank> | <blank> |
| Add workstations to the domain | Establish trust relationship between computer and DC | <blank> | <blank> |
| Adjust memory quotas for a process | Allocate more memory to an extant process | Administrators, LOCAL SERVICE, NETWORK SERVICE | Administrators, LOCAL SERVICE, NETWORK SERVICE |
| Allow log on locally | Allows local logon | Guest, Administrator, Backup Operators, Users | Users |
| Allow log on through remote desktop services | Allows initiation of RDP sessions | Administrators, Remote Desktop Users | Blank unless specified by readme |
| Back up files and directories | Backup functionality | Administrators, Backup Operators | Administrators |
| Bypass traverse checking | Allows directory browsing without appropriate permissions | LOCAL SERVICE, NETWORK SERVICE, Administrators, Backup Operators | LOCAL SERVICE, NETWORK SERVICE, Administrators |
| Change the system time | Change the system time for the local computer | LOCAL SERVICE, Administrators | LOCAL SERVICE, Administrators |
| Change the time zone | Change the time zone for the local computer | LOCAL SERVICE, Administrators | LOCAL SERVICE, Administrators |
| Create a pagefile | RAM to HDD functionality | Administrators | Administrators |
| Create a token object | Used for tokening permissions, should be blank | <blank> | <blank> |
| Create global objects | Create system wide objects | LOCAL SERVICE, NETWORK SERVICE, SERVICE, Administrators | LOCAL SERVICE, NETWORK SERVICE, SERVICE, Administrators |
| Create permanent shared objects | Create directory-wide shared objects | <blank> | <blank> |
| Create symbolic links | Create links between files | Administrators | Administrators |
| Debug programs | Debugging functionality | Administrators | Administrators |
| Deny access to this computer from the network | Deny network logon | Guest | Guest |
| Deny log on as a batch job | Deny some remote session initiation functionality | <blank> | <blank> |
| Deny log on as a service | Deny accounts service initiation | <blank> | <blank> |
| Deny log on locally | Prevent local log on | Guest | Guest |
| Deny log on through remote desktop services | Deny remote desktop log in | <blank> | <blank> |
| Enable computer and user accounts to be trusted for delegation | Complex network functionality related to peer to peer stuff | <blank> | <blank> |
| Force shutdown from a remote system | Shutdown system remotely | Administrators | Administrators |
| Generate security audits | Log security in event log | LOCAL SERVICE, NETWORK SERVICE | LOCAL SERVICE, NETWORK SERVICE |
| Impersonate a client after authentication | Allows acting on behalf of another user | Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE | Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE |
| Increase a process working set | Allocate additional RAM to a process | Users | Users |
| Increase scheduling priority | Allows users to increase a process’s resource distribution priority | Administrators | Administrators |
| Load and unload device drivers | Load new drivers into the system. Dangerous as drivers run as system | Administrators and (possibly) Print Operators | Administrators |
| Lock pages in memory | Prevent paging for a section of physical memory | <blank> | <blank> |
| Log on as a batch job | Allows log on as batch job for task scheduler and other purposes | Administrators, Backup Operators, Performance Log Users | Administrators, Backup Operators, Performance Log Users |
| Log on as a service | Allows service accounts to register a process as a service | <blank> - OR - NETWORK SERVICE only | Identical to default |
| Manage auditing and security log | Allows users to create SACLS on arbitrary objects for logging purposes | Administrators | Administrators |
| Modify an object label | Allows arbitrary increase of security label for unowned objects | <blank> | <blank> |
| Modify firmware environment values | Allows modifying which firmware is considered “Last Trusted” by Windows | Administrators | Administrators |
| Perform volume maintenance tasks | Allows high-level disk management | Administrators | Administrators |
| Profile single process | Allows profiling program performance | Administrators | Administrators |
| Profile system performance | Allows profiling system-wide performance | Administrators | Administrators |
| Remove computer from docking station | Allows removal of portable device from locking dock | Administrators | Administrators |
| Replace a process level token | Spawn a process using a passed credential token | LOCAL SERVICE, NETWORK SERVICE | LOCAL SERVICE, NETWORK SERVICE |
| Restore files and directories | Rollback files to previous restore points | Administrators, Backup Operators | Administrators, Backup Operators |
| Shut down the system | Shut down the system | Administrators, Backup Operators, Print Operators, Server Operators | Administrators, Server Operators |
| Synchronize directory service data | Grants ability to synch GPOs between domain controllers | <blank> | <blank> |
| Take ownership of files or other objects | Allows taking ownership of any object in the system | Administrators | Administrators |

## Security Options

| Setting Title | Desired Setting |
| --- | --- |
| **Accounts** |  |
| Administrator account status | Disabled |
| Block Microsoft Accounts | Enabled |
| Guest account status | Disabled |
| Rename Administrator account | Shrek |
| Rename Guest account | Donkey |
| Limit local account use of blank passwords to console logon only | Enabled |
| **Audit** |  |
| Audit the access of global system objects | Enabled |
| Audit the use of Backup and Restore privilege | Enabled |
| Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings. | Enabled |
| Shut down system immediately if unable to log security audits | Enabled |
| **DCOM** |  |
| DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax | Not Defined |
| DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax | Not Defined |
| **Devices** |  |
| Allow undock without having to log on | Disabled |
| Allowed to format and eject removable media | Administrators |
| Prevent users from installing printer drivers | Enabled |
| Restrict CDROM access to locally logged-on users only | Enabled |
| Restrict Floppy access to locally logged-on users only | Enabled |
| **Domain controller** |  |
| Allow server operators to schedule tasks |  |
| LDAP server signing requirements | Require signing |
| Refuse machine account password changes |  |
| **Domain controller** |  |
| 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 | 60 |
| Require strong (Windows 2000 or later) session key | Enabled |
| **Interactive** **Logon** |  |
| Display user information when the session is locked | Disabled |
| Do not require CTRL-ALT-DEL | Disabled |
| Do not display user last name | Enabled |
| Don’t display username at sign-in | Enabled |
| Machine account threshold | 5 |
| Machine Inactivity Limit | 600 seconds |
| Number of Previous logons to cache | 4 |
| Prompt user to change password before expiration | 5 days |
| Require Domain Controller authentication to unlock | Enabled |
| **Network Client** |  |
| Digitally sign communications (if server agrees) | Enabled |
| Digitally sign communications (Always) | Enabled |
| Send unencrypted password to third-party SMB servers | Disabled |
| **Microsoft Network Server** |  |
| Amount of idle time required before suspending session | 15 minutes |
| Send unencrypted password to clients | Disabled |
| Attempt S4U2Self to obtain claim information | Enabled |
| Digitally sign communications (Always) | Enabled |
| Digitally sign communications (if client agrees) | Enabled |
| Disconnect Clients when logon hours expire | Enabled |
| Server SPN Target name validation | Accept if provided by client |
| **Network Access** |  |
| Allow anonymous SID/Name translation | Disabled |
| Do not allow anonymous enumeration of SAM accounts | Enabled |
| Do not allow anonymous enumeration of SAM accounts and shares | Enabled |
| 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 | <blank> |
| Remotely accessible registry paths | <blank> |
| Remotely accessible registry paths and subpaths | <blank> |
| Restrict anonymous access to named pipes and shares | Enabled |
| Restrict Clients allowed to make remote calls to SAM | Enabled |
| Shares that can be accessed anonymously | <blank> |
| Sharing and security model for local accounts | Classic |
| Force logoff when logon hours expire | Enabled |
| **Network Security** |  |
| Allow local system to use computer identity for NTLM | Enabled |
| Allow Local system NULL session fallback | Disabled |
| Configure encryption types allowed for Kerberos win7 only | RC4, both AES, future encryption types |
| Do not store LAN manager hash value on next password change | Enabled |
| Force Logoff when logon hours expire | Enabled |
| LAN manager authentication level | Send NTLMv2 response only, refuse LM and NTLM |
| LDAP client signing requirements | Require Signing |
| Minimum session security for NTML SSP based (including secure RPC) clients | Require 128 bit encryption, Require NTLMv2 |
| Minimum session security for NTML SSP based (including secure RPC) server | Require 128 bit encryption, Require NTLMv2 |
| Restrict NTLM: Audit Incoming NTLM Traffic | Enable auditing for all accounts |
| Restrict NTLM: Audit NTLM authentication in this domain | Enable all |
| Restrict NTLM: Incoming NTLM traffic | Deny all |
| Restrict NTLM: NTLM authentication in this domain | Deny all |
| Restrict NTLM: Outgoing NTLM traffic to remote servers | Deny all |
| **Recovery Console** |  |
| Allow automatic administrative logon | Disabled |
| Allow floppy copy and access to all drives and all folders | Disabled |
| **Shutdown** |  |
| Allow system to be shut down without having to log on | Disabled |
| Clear virtual memory pagefile | Enabled |
| **System cryptography** |  |
| Force strong key protection for user keys stored on the computer | User must enter a password each time they use a key |
| Use FIPS 140 compliant cryptographic algorithms, including encryption, hashing and signing algorithms | Enabled |
| **System Objects** |  |
| Strengthen default permissions of internal system objects (e.g., Symbolic Links) | Enabled |
| **System Settings** |  |
| Optional subsystems | <Blank> |
| Use Certificate Rules on Windows Executables for Software Restriction Policies | Enabled |
| **User Account Control** |  |
| Admin Approval Mode for the built-in Administrator account | Enabled |
| Allow UIAccess applications to prompt for elevation without using the secure desktop | Disabled |
| Behavior of the elevation prompt for administrators in Admin Approval mode | Prompt for Credentials on the Secure Desktop |
| Behavior of the elevation prompt for standard users | Prompt for credentials |
| Detect application installation and prompt for elevation | Enabled |
| Only elevate executable files that are signed and validated | Enabled |
| Only elevate UIAccess applications that are installed in secure locations | Enabled |
| Run all administrators in Admin Approval Mode | Enabled |
| Switch to the secure desktop when prompting for elevation | Enabled |
| Virtualize file and registry write failures to per-user locations | Enabled |

# gpedit.msc

* First we are going to check if there are any preapplied GP’s
* Windows Key + r, **rsop.msc**
* After this is done, it will show you all of GPs modified by CP
* Windows Key + r, **gpedit.msc**
* Computer Configuration >> Administrative Templates >> Windows Components >> Credential User Interface
  + Do not display the password reveal button < Enabled
  + Require trusted path for credential entry < Enabled
  + Enumerate administrator accounts on elevation < Disabled
* Computer Configuration -> Administrative Templates -> Windows Components -> AutoPlay Policies
  + Turn off Autoplay < Enabled: All Drives
  + Prevent AutoPlay from remembering user choices < Enabled
  + Set the default behavior for AutoRun < Enabled:Do not execute any autorun commands

# BitLocker

* Windows Key+R, gpedit.msc
  + Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components > BitLocker Drive Encryption > Operating System Drives in the left pane.
  + Double click **Require additional authentication at startup**
  + Check **Enabled**
  + Check **Allow BitLocker without a compatible TPM (requires a password or a startup key on a USB flash drive)**
  + Click **OK**
* Windows Key+R, control
  + Go to Control Panel > System and Security > BitLocker Drive Encryption
  + Click **Turn on Bitlocker**
  + And select **Enter a password**
  + And do the password **IH@t3Pupp135**

# Processes and Malware

## Process Explorer (procexp.exe)

* Located in the Tools folder (inside the script folder)
* Each line represents a program running
* Color
  + Green > New Process
  + Red > Dying Process
  + Pink > Service-Hosting processes. (Hover over to see hosted services)
  + Light Purple/Blue > Own Processes (Program run by you or using your SSID)
  + Acid Purple > Packed (Encrypted) image in RAM. Exercise **extreme** scrutiny as packed images usually mean malware.
* Configurations
  + File > **Show Details for all processes (Run as admin)**
  + Options > **Verify Image Signatures**
    - Footnote: Companies sign their programs when they release them. If you see something like **(Verified) Google Inc.** in process explorer, you can be certain that Google released said program.
    - If you see an unsigned image make sure to check out the process carefully. Very likely malware or something that just shouldn’t be running. (Verify readme first)
  + Options > **VirusTotal** >  **Check VirusTotal**
    - If you are unaware, VirusTotal is an online anti-virus software composed of over 70 malware engines
    - Anything that gets more than 1 or 2 hits should be looked at CLOSELY (Unless specified by the readme)
  + View > **Select Columns** > **Username**
    - Useful to link processes to usernames (Who is running this program?)
    - Anything other than SYSTEM and your username should be looked at closely.
  + Use VirusTotal and Image Signatures to identify potentially suspicious processes.
    - More than 1-2 hits should be inspected/deleted
  + How to investigate a process.
    - Right Click > **Properties**
    - Find its file location
    - See if you can gain anything from its title, Google its .exe, look for info on its source folder.
  + Purging
    - THIS HAS TO BE DONE IN THIS ORDER
    - Once you identified it as malware
    - Open its source folder by using Right Click > **Properties**
    - Right Click > **Stop Process**
    - Delete its source files

# Rootkits & Backdoors

* Best way to find rootkits and backdoors is by doing it through a network analysis.
* Run tcpview.exe (as admin) found in the Tools folder (on desktop)
* Red Flags
  + Local address of **0.0.0.0[port]** means that a process is listening on that port for *any* connection
  + :[::] has the same meaning for IPv6
  + For any process that you find weird, investigate using task manager or process explorer
    - Is it obvious malware? Check signatures if it's a windows process.
    - Make sure to investigate the source folders of any malware you do find – what else could be hiding there? WRITE IT DOWN!
  + Make sure to eventually murder the process
* Common malware is Netcat, Tini, TX, NTBS, NTBindShell, Sticky Keys, and keyloggers. All of these will show up in process explorer and task manager

# File Sharing

* Shares can be accessed under Computer Management. Windows+R, type **compmgmt.msc**
* The default shares are C$,ADMIN$,IPC$,PRINT$, and FAX$
* If the default shares are not required
  + Control Panel > Network and Sharing > Advanced Sharing Settings
    - Turn off **Network Discovery**
    - Turn off **File and Printer sharing**
    - Turn off **Public Folder Sharing**
    - Leave **Password Protected Sharing** on
  + Disable the **Server** service in **services.msc**
  + Remove **File and Printer Sharing** from the Windows Feature menu
  + Or block/disable **File and Printer Sharing** rules in the Firewall
* Stop sharing any other shares (Unless specified by the readme)
  + Inspect each share folder (Is malware being shared?)
* If file and printer sharing are required
  + Windows+R, **wf.msc** > Inbound rules > File and Printer sharing group
    - All the **echo** and **smb** ones must be allowed
    - Everything else should be disabled
      * **LLMNR-UDP-IN**
      * **NB** Rules
      * **Spooler** rules

# Scheduled Tasks

* Open the **Tools** folder in the script folder and open **Autoruns.exe** (Autoruns64 if on 64bit)
  + This programs checks programs that run on startup
* Color meaning
  + Yellow - Don’t worry about this
  + Green - Indicated **new** items
  + Pink - No publisher or signature **BIG RED FLAG**
* Setup
  + File > Run as Administrator
  + Options
    - Check **Hide Empty Locations**
    - Check **Hide Microsoft Entries**
    - Scan Options
      * Check **Verify Code Signatures**
      * Check **Check VirusTotal.com**
    - Check **Hide VirusTotal** clean entries (Hides anything that hits a 0 out of ~70)
  + Everything Tab
    - Inspect anything with 2+ VirusTotal hits
    - Look closely at pink colored images
    - Otherwise inspect the source location and disable it if malicious
      * If there is anything else at the source location, delete it.
  + Logon Tab (Everything that runs on startup)
    - Liberally uncheck things that aren’t essential
    - Check against the readme.
  + Explorer Tab
    - Any VirusTotal hits are candidates for removal.
    - Ideally this should be black when VirusTotal clean is checked.
  + Internet Explorer Tab (Addons for IE)
    - Uncheck **everything** unless it is specified in the readme
  + Scheduled Tasks Tab
    - Uncheck **Hide VirusTotal clean entries** for this one
    - Inspect every service *closely*
    - Once done recheck **Hide VirusTotal clean entries**
  + Services (services autostarted by default
    - A bulk of this should already be done
    - Come-over it once with **Hide VirusTotal clean entries** off
  + Image Hijacks
    - Disable **EVERYTHING** unless specified by the readme.

# CyberPatriot Readme Software

* Typically googling **Securing <insert software name> software** works fairly well
* The key goals of most scenarios are:
  + Ensure the software is the legitimate version
  + Ensure it is updated and patched
    - If there is an auto-update feature within the software, turn it on
  + Ensure only proper users have access
  + Ensure the application is not adding to the attack surface (Risky ports/services)

# Microsoft Tools

## MBSA

* Microsoft Security Baseline Analyzer
* This is useful in case you missed something stupid.
* <https://www.microsoft.com/en-us/download/details.aspx?id=19892>
* Download and install it.
* Run it as Administrator
* Look for yellow and red in the report.

## Policy Analyzer

* Located in the Tools folder inside the script folder
* Run it as Administrator
* Check **Local Registry** and **Local Policy**
* Then click **View/Compare**
* This will simply list all of the configured local policy settings, make sure nothing looks off.

## Process Monitor (procmon.exe)

* Let it run for about 10 seconds and then hit the magnifying glass to stop it
* Filtering the output
  + The 4 icons at the top signify different actions
    - Registry, file access, etc.
* This is useful to figure out what a process is doing.

## Process Explorer (Procexp.exe)

* Configurations
  + Run as administrator
  + Options > Verify Image Signatures
  + Options > VirusTotal > Check VirusTotal
* Look for suspicious processes
* Right click > Properties
  + Investigate a process
  + Find its file location

## TCPView

* When you start TCPView it will enumerate all active TCP and UDP endpoints, resolving all IP addresses to their domain name versions.
  + This is a good visual tool to see what is connecting outbound or inbound (services, malware, backdoors etc.0
  + TCPView will show the
    - Name, Process IS (PID), local address/port, remote address/port and Status
      * Established -connected (inbound or outbound)
      * Listening -local service listening for traffic
      * SYN\_Sent -connect attempt initiated, not yet completed
      * Time\_Wait -connect attempt initiated, not yet completed
      * Close\_Wait -connection in process of being closed
    - You can close established TCP/IP connections (those labeled with a state of ESTABLISHED) by selecting **File|Close Connections**

# Event Viewer

* We are going to focus of the Security log
* Windows+R, type **eventvwr**

## Security Log

* Because auditing is enabled, many logs will show here
* Expand **Windows Logs**, right click on **Security**, and choose **Properties** 
  + Set the **Max Log Size** to 196608
  + Set the **Overwrite as needed**
* View event data (Might be useful for forensics!)
  + Right click on **Security** and **Select Filter Current Log**

## Event ID’s

* 4624 - Logon Event
* 4723 - User Account Management (attempt to change password)
* 4738 - User Account Management (account setting was changed)
* 4740 - User Account Management (account was locked out)
* 4767 - User Account Management (account was unlocked)
* 4688 - Process Creation

## Application Log

* Errors for apps (such as Filezilla)

## System Log

* Service issues (Startup failures)
* Firewall stability, DNS
* Anything red/yellow
  + Right click **System** > **Filter**
  + Critical and warning (Red and yellow)
* Checking for software installs
  + <http://eventlogs.blogspot.com/2007/11/tracking-software-installation-and.html>
* Yellows and Reds
  + Give you an idea for what you need to look at
    - What interface is this source tied too
  + Double-click > Descriptions
  + Look into that area

# Administrative Templates

* It is possible to disable a service through group policy
* Windows+R, **gpedit.msc**
* Computer Configuration > Administrative Templates > All settings

The following are critical services and are **NOT** needed unless specified.

# RDP

* Windows+R, **gpedit.msc**
  + Go to Computer\Policies\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security
    - And enable **Require user authentication for remote connections by using Network Level Authentication**
    - Enable **Require secure RPC communication**
    - Enable and set to high **Set client connection encryption level**
* Windows+R, sysdm.cpl
  + Click the remote tab
    - Check **Allow remote connections to this computer**
    - Check **Allow connections only from computers running Remote Desktop with Network Level Authentication**
    - Click Apply
  + Click **Select Users**
    - Click **add**
    - Added users that need to be added (readme)
  + Two settings relevant to RDP, under System Properties –Remote tab
    - Windows Clients and Servers support RDP sessions by default for Administrators (max = 2 sessions)
    - Additional users can be granted permissions via the “Remote Desktop Users Group”
    - Set the option to “Allow connections ONLY from computers running network level authentication”

For Windows Server, there is a role for Remote Desktop Services

• This allow a server to host virtual desktops, virtual sessions etc. with limits only kept by amount of RAM/CPU

• There are deep security configs for this service, I will add some key best practices soon

# DNS

* [Here is a pretty decent article.](https://newhelptech.wordpress.com/2017/07/02/step-by-step-implementing-dns-security-in-windows-server-2016/) When in doubt just look it up.
* DNS zone transfers to any server is disabled
* Dynamic updated to the DNS server are disabled

# IIS

* Yeah so I don’t have time for this
* IIS detailed error messages disabled
* IIS default website directory browsing disabled
* Figure out how to do that and points for you

# SMB

Windows 8/10

* Run the following in Powershell as admin
  + Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol
  + Set-SmbServerConfiguration -EnableSMB1Protocol $false
  + Set-SmbServerConfiguration –EnableSMB2Protocol $true
  + Set-SmbServerConfiguration –EncryptData $true
  + Set-SmbServerConfiguration –RejectUnencryptedAccess $false

Windows Server

* Run the following in Powershell as admin
  + Disable-WindowsOptionalFeature -Online -FeatureName smb1protocol
  + Set-SmbServerConfiguration -EnableSMB1Protocol $false
  + Set-SmbServerConfiguration -EnableSMB2Protocol $true
  + Set-SmbServerConfiguration –EncryptData $true
  + Set-SmbServerConfiguration –RejectUnencryptedAccess $false
* Open File Server Manager
  + Go to **File and Storage Services**
  + Click on **Shares**
  + Select the share you want to turn encryption on for, and right-click
  + Select **Properties** from the context menu.
  + In the Share Properties window, select **Settings**, and enable **Encrypt data access**

# Filezilla

* This section applies to images that require Filezilla
* Filezilla is an alternate, standalone FTP client. It runs a service called **Filezilla Server FTP Service,** make sure this is on!
* This part is a bit difficult to understand, so buckle up!
* Make sure that FileZilla server is running under a standard user, not an Admin or **LocalSystem**
  + Windows + r, **lusrmgr.msc**
  + Click **Users**
  + Create a *new* user named **filezilla**
  + Make sure to password protect this user
* Change the properties of **Filezilla Server FTP Service**
  + Windows + r, **services.msc**
  + Find **Filezilla Server FTP Service**
  + Right click and open **Properties**
  + Click **stop** if the service is running
  + Switch to the **Log On** tab
    - Username: filezilla
    - Password: IH@t3Pupp135
* You must also set the Permissions on the folders that FileZilla is using (and any SSL certs that are being used) or the install will break.
* With Windows Explorer navigate to "FileZilla Server" installation directory
  + Found in Program Files or C:\
* Locate "FileZilla Server.xml" file, service requires write permissions to this file
  + Right click -> Properties
  + If you have "Simple File Sharing" enabled (no "Security" tab in file properties)
    - Click "Tools" in Explorer menu, select "Folder options"; "Folder Options" dialog appears
    - Select "View" tab
    - Uncheck "Use simple file sharing (Recommended)"
    - Click OK
* Right click "FileZilla Server.xml" select "Properties"; "Properties" dialog appears
  + Select "Security" tab, click "Add" button; "Select User or Group" dialog appears
  + Type "filezilla" into "Enter object names to select" textbox
  + Click "OK"; "filezilla" user is added to permissions list
  + Select "filezilla" user and check "Write" in "Allow" column
  + Click "OK"; permissions are now saved
  + If you use logging, set "Write" access to "Logs" folder too
* Filezilla maintains a set of users separate from that of windows; these need to be managed as well.
  + FileZilla Server Manager -> Connect to Server -> Edit -> Users
  + Remove “Anonymous” user if present and not necessary for image
  + Remove any other unauthorized users per readme.

# Overall, if you need to secure something look it up. “How to secure <insert name> on Windows X”