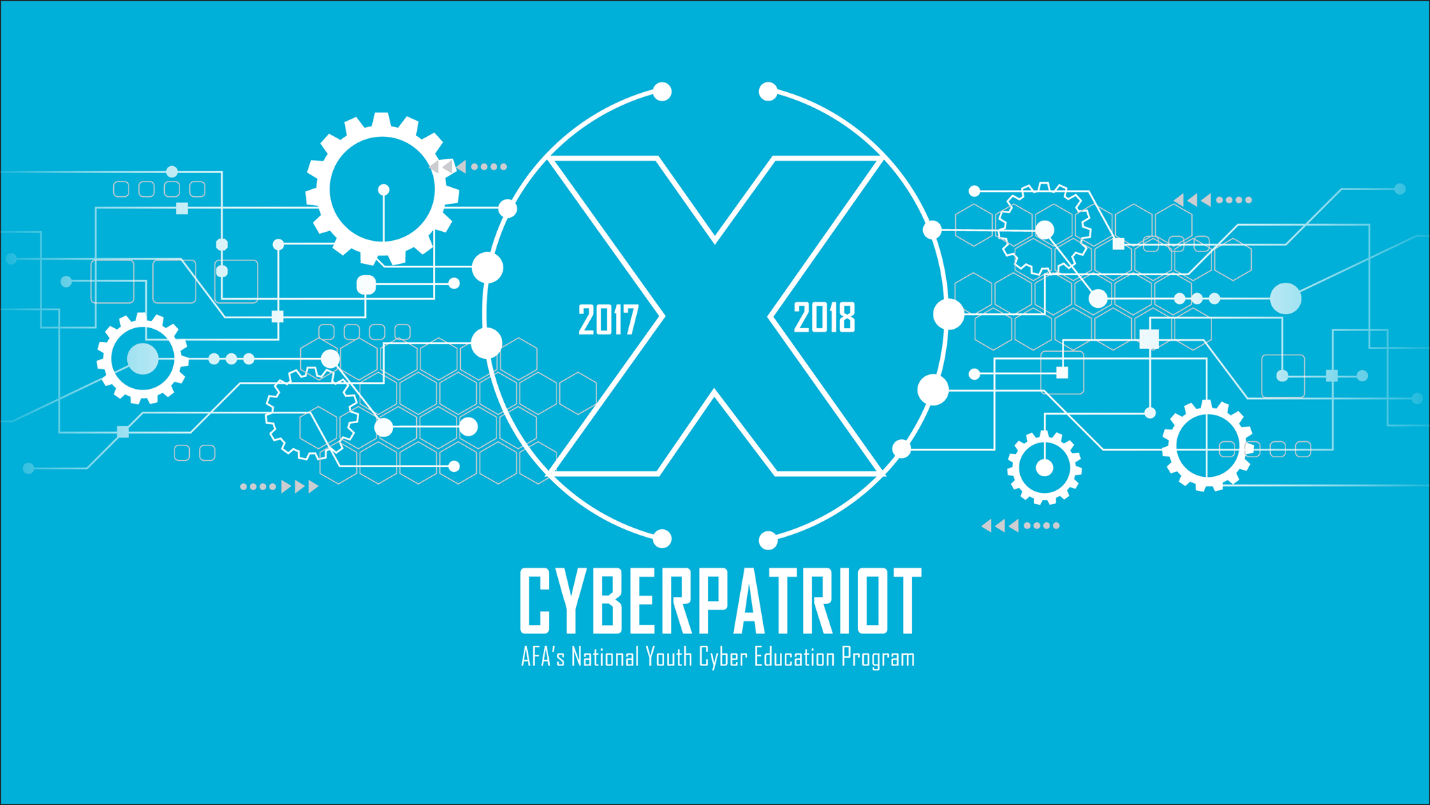
CyberPatriot Windows Playbook

LC CyberPatriot Team

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Comments** |
| 1.0 | 2/2017 | Thorne Garvin | Original Version –team comments, revamped for 2017-2018 |
| 1.4 | 2/6/2018 | Thorne Garvin | Updates incl. more tools and server roles |
| 1.5 | 2/7/2018 | Jason Popp | Updates to tools sections, draft IIS/FTP/FileZilla notes, Checklist table added |
| 1.5.1 | 2/8/2017 | Thorne Garvin | Minor clerical edits, added FileZilla user management section, moved FileZilla to Server Roles section  Added section on CyberPatriot-spawned groups  Deleted “Media Files and Hacking tools” as it was out of date |
| 1.5.2 | 2/8/2017 | Thorne Garvin | Expanded User Rights Assignment Section |
|  |  |  |  |



General Progress Checklist

* [Competition Preparation 3](#_30j0zll)
* [General Competition Tips 3](#_1fob9te)
* [Readme File –Forensics, Functions, Accounts 3](#_3znysh7)
* [Application and OS Patching Process 4](#_2et92p0)
* [Windows Updates 4](#_tyjcwt)
* [Software Updates 5](#_3dy6vkm)
* [Addressing Forensics Questions 5](#_1t3h5sf)
* [Secure Browser Configuration 6](#_4d34og8)
* [CyberPatriot-Installed Software 8](#_2s8eyo1)
* [Windows Client Programs and Features (7/8/10) 8](#_17dp8vu)
* [Software Management 8](#_3rdcrjn)
* [FileZilla 9](#_26in1rg)
* [Windows Firewall 10](#_lnxbz9)
* [AV –Malwarebytes, Windows Defender, Windows Security Essentials 10](#_35nkun2)
* [Users and Groups 11](#_1ksv4uv)
* [User Account Control 12](#_44sinio)
* [Windows Services (7/8/10) 12](#_2jxsxqh)
* [Local Security Policy 15](#_z337ya)
* [Processes and Malware 18](#_3j2qqm3)
* [Rootkits and Backdoors 19](#_1y810tw)
* [Media Files and Hacking Tools 19](#_4i7ojhp)
* [File sharing (Win7/8/10) 20](#_2xcytpi)
* [File Ownership 21](#_1ci93xb)
* [Auditing 21](#_3whwml4)
* [Scheduled Tasks 23](#_2bn6wsx)
* [Server Roles: IIS, FTP 24](#_qsh70q)
* [Remote Access and RDP 25](#_3as4poj)
* [Microsoft Tools: MBSA, Policy Analyzer 26](#_1pxezwc)
* [SYSINTERNALS Tools 26](#_49x2ik5)
* [Event Viewer 27](#_2p2csry)
* [Miscellaneous 28](#_147n2zr)

# Competition Preparation

* Increase RAM to 4 GB
* Increase CPU cores to 2 (assuming quad-core cpu)
* Ensure internet connectivity is working
* Have a standby flash drive with Windows updates and tools
* Tools/Downloads should be organized by OS
  + Win7, Win8.1, Win10, Win Server 2016, Ubuntu 14/16
* Download content to USB:
  + Service Packs
  + Browsers
  + Tools
    - Malwarebytes
    - Avast or other AV of choice. MUST register with Windows Defender as 3rd-party AV
      * MSFT Security Essentials is also a good option for Windows
    - Sysinternals (ALL)
    - MBSA
    - Policy Analyzer
    - DROID
* Verify tools USB is accessible from image

# General Competition Tips

* Take a PICTURE of the Readme before you start (has admin account passwords and hints)
* Use the ReadMe to look for clues and set the first phases of the remediation plan
* Run assessment tools like MBSA/Policy Analyzer first to record the base issues” to be corrected
* Take notes while executing each step of the workbook
  + It will help with time management and ensure no areas are forgotten (lost points!)
* Set an alarm and check in with the team on progress every 30 minutes
* At each 30 minute milestone, evaluate progress with the full team for < 5 minutes.
* Re-run assessment tools if there are questions

# Readme File –Forensics, Functions, Accounts

This file will contain:

1. The tips/hints for how the system should be used (to help guide what to enable/disable in the image)
2. Passwords for admin accounts in case you lock yourself out
3. Open the ReadMe and take notes to the answers to the questions below to guide remediation focus areas
   * Get as much data out of the readme as you can.
     + What is the problem the readme states?
     + What are the main goals?
     + Are there any details that could affect your methodology?
   * Look for words/phrases that could lead to specific vulnerabilities.
     + E.G. “Employees MUST have access to the latest, most up-to-date version of Libreoffice. Is Libreoffice installed? Is it patched? Does it run?
   * Software
     + List out critical software with three checkboxes: Installed, Updated, Secure
     + Don’t forget about internet explorer and java!
     + If any software mentioned in the readme is NOT installed on the system, install it right now.
   * Critical Services
     + List out critical services with three checkboxes: Installed, Updated, Secure
   * Users
     + Who can access the system remotely?
       - How do I configure this through groups and server roles?
     + Who is a valid administrator?
     + Who is a valid user?
     + What service users are required?
     + What access should the ‘everyone’ (All users on the system) object have?

# Application and OS Patching Process

* Make sure all relevant service packs are installed first, then run any key application or browser upgrades
* This will reduce the number of individual hotfixes that need to be installed and should speed up the update process
* Don’t forget to look for updates to installed software as well (FileZilla, Wordpress etc.)

## Recommended Patching Order

1. Service Packs
2. Browser Updates/Version Upgrades
3. Software Updates
4. Windows Updates

# Windows Updates

1. Run MBSA first to verify the status of the system and key software updates
2. This will help you plan the time needed for updates
3. If an OS is missing service packs or convenience rollups, install them manually from USB to save time

### Desktop (7/8/10)

* + Search: ‘Windows Update’
  + Change settings
    - CP will usually want automatic download/install even if it means that your computer will be down without your control.
  + Check for updates.
  + Install service packs (Up to SP1 for 7)
  + You may have to install updates multiple times before they work.
  + Don’t install language packs!
  + Restart

### Server (2008/2016)

* Control Panel
* Search: “Windows update”
* Change settings
* Check for updates
* Install any service packs (Up to SP2) (or launch manually if downloaded to the USB drive)
* Restart

# Software Updates

## Web Browsers

* + Firefox
    - Top right -> Help -> About Firefox
    - Keep running until Firefox registers as up to date
    - Alternatively, download the Quantum installer from Mozilla
  + Internet Explorer
    - Most up to date version possible varies based on operating system
    - Win7+: Internet Explorer 11
    - Win2k8 R2: IE 11
    - Win2k8 SP2: IE 9
    - Windows Vista: IE 9
    - Download and install the appropriate 32-bit version from Microsoft
* Other software in readme
  + Refer to the checklist produced during readme notetaking
  + If CP references a specific version, make sure to download it even if it’s not the latest version
  + Otherwise, download the most up-to-date version from the appropriate website.
  + Do this for EVERY piece of software from the readme and otherwise (anything left in the programs and features menu)
    - Java

# Addressing Forensics Questions

* Open explorer.
  + Hidden files/folders: Folder Options > View
  + Uncheck “Hide extensions for known file types.”
* Attempt to answer the question for ~5 minutes.
  + If you can’t, have someone else research the topic and move on.
* If the forensics question specifically mentions a vulnerability, make sure to fix it.
* Windows key R -> eventvwr.msc -> Security -> Right Click -> Properties -> Max log size: 60000
  + Increase logs to usable size

# Secure Browser Configuration

## Web Browsers

## Firefox

* Pre-Quantum (rounded tabs)
  + Top Right -> Options -> Security Tab
    - All three in General section
    - Also make sure there are no exceptions on “Warn me when sites try to install add-ons”
    - None in Logins section
  + General Tab
    - Always check if Firefox is your default browser -> Check
    - Set homepage to google.com
    - Always ask me to save files -> Check
  + Search Tab
    - Default search engine -> Google
  + Content
    - Block pop-up windows -> Check
  + Privacy
    - Request that sites not block you -> Check
    - Use tracking protection in private windows –> Check
    - Firefox will slider -> Never remember history
  + Advanced Tab
    - Network Tab
      * Configure how Firefox connects to the internet -> Make sure no proxy is configured
  + Updates Tab
    - Firefox Updates -> Automatically install updates
    - Check “Use a background service to install updates”
  + Extensions
    - Type in about:addons in the search bar
    - Disable anything but what CP explicitly says to keep. (Except adobe and other baseline stuff)
* Quantum (square tabs, modern UI)
  + Top Right -> Options
  + General Tab
    - Always check if Firefox is your default browser -> Check
    - When Firefox Starts -> Show a blank page
    - Home Page -> Default
    - Updates subsection
      * Allow Firefox to:
        + Automatically install updates
        + Use a background service to install updates
        + Automatically update search engines
  + Privacy and Security Tab
    - Forms & Passwords -> Uncheck “Remember logins…”
    - Forms & Passwords -> Uncheck “Use a master password”
    - History -> Firefox will “Never Remember history”
    - Address Bar -> Uncheck all three
    - Tracking Protection -> Use Tracking Protection… -> Always
    - Tracking Protection -> Send websites do not track… -> Always
    - Permissions -> Check “Block pop-up windows…”
    - Permissions -> Check “Warn you when Websites try to install…”
    - Security -> Deceptive Content -> Check All 3
    - Certificates -> Personal Certificate -> Every time
    - Certificates -> Check “Query OCSP responder servers…”
  + Type “about: addons” in the search bar
    - Disable anything under “Add-ons” except what CP explicitly says to keep. (Except baseline stuff)
    - Do the same for the plugins section

## Internet Explorer

* Search for “Internet Options”
* General Tab
  + Check “Delete browsing history on exit”
* Security Tab
  + Max out the security bar for all of the zones
  + Make sure “Enable Protected Mode” is checked for each zone
* Privacy Tab
  + Check “Never allow websites to request your physical location”
  + Check “Turn on pop-up blocker”
  + Check “Disable toolbars and extensions…”
* Advanced Tab
  + Accelerated Graphics -> Nothing Checked
  + Accessibility -> Nothing Checked
  + Browsing Section
    - 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 -> Always
  + HTTP settings -> All checked
  + 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…”
    - 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”
* Windows key R -> iexplore.exe -> Top Right -> Tools(Gear) -> Manage Add-Ons
  + Disable everything not mentioned in the readme exceptbaseline stuff

# Windows Client Programs and Features (7/8/10)

* Control Panel > Programs > Uninstall a Program > Turn Windows Features On or Off
  + Uncheck:
    - Games
    - Media Features
    - IIS (Internet Information Services)
      * Microsoft’s web server
      * Disable unless required
    - IIS Services Hostable Web Core
    - Active directory lightweight directory services
    - Hyper-V
    - RIP Listener
    - Telnet
    - SMB
    - File and Printer sharing
    - Filesharing (might exist on certain systems)
    - Disable unless required
    - TFTP Client

# Software Management

* Programs and Features (Control Panel -> Programs -> Programs and Features)
  + Look to purge all software not mentioned by the readme.
  + Sort by size, sort by publisher (look for blanks.)
  + Don’t remove “base level” stuff (Java, C++ libraries, Perl, etc.)
    - Write it down to update later (Esp. Java)
* Program Files (x86), Program Files, and Program Data
  + Look for suspiciously named folders
    - Gibberish names
    - “Keylogger”
    - “-crack”, “password”, “ninja”, “logger”, etc.
    - Hidden folders except for the “Default” one
    - Anything you’ve never recognized or heard of before
  + CHECK README FIRST
    - Just delete the folder if it’s suspicious
    - If you get readlocked, find and kill the source process via process explorer.
  + Write down folders where you find suspicious things- other stuff can be there as well.
    - Especially note names of files and folders to look for more references in autoruns, the registry or process explorer
  + Make sure to check against processes, autoruns
  + “kind:program” can be useful here
* Software Installation
  + If any software mentioned in the readme is NOT installed on the system, install it right now.
  + Refer to software you wrote down during your readme process: check first that everything is installed and install it if it isn’t. This includes internet explorer.

# 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 damn 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.

# AV – Malwarebytes, Windows Defender, Windows Security Essentials

### Malwarebytes

* Install + Run
* Setup automated scans
* Write down the path names of any returns- can help to find further malware.
* Manually look in all1 of the directories/registry keys.
* Uninstall after full scan finishes

### Windows Defender (Win7/8)

* Make sure Defender is on.
* Control Panel > Windows Defender
* Launch Tools –Options
  + Enable “Automatically scan my computer”
  + Use Default “Recommended Actions”
  + Ensure Real Time protection is enabled
  + Under Advanced, enable “Use Heuristics” and “Scan Archive Files”
  + Update definitions
  + Run a Quick Scan (at minimum)

### Windows Defender (Win10)

* Needs to be Enabled
* Windows Defender has several versions –the Desktop app, the Security Settings, and in Creators Build Windows 10, version 1703 there is a new Windows Defender Security Center app
* Control Panel > Windows Defender (this will open the “Desktop” version)
  + You can also access the Win10 by typing Settings from the Run line to launch the Windows Store App
    - Then access “Updates and Security” where you can launch the Desktop app (above) and set the base options for Real Time Protection, Cloud-based protection, Enhanced Notifications
    - Also has an option for Windows Defender Offline” which is 15+ min process to update and then scan after a reboot to find embedded malware
* Launch Tools –Options
  + Enable “Automatically scan my computer”
  + Use Default “Recommended Actions”
  + Ensure Real Time protection is enabled
  + Under Advanced, enable “Use Heuristics” and “Scan Archive Files”
  + Update definitions
  + Run a Quick Scan (at minimum)

### Avast or other AV of your choice

* MUST register with defender as third-party AV, which MBAM does not
* Install and run as standard. Might catch something but that’s bonus points

# Users and Groups

* Accessed through Computer > Manage > Users and Groups
* Alternatively, use MMC and add the computer management snap-in.

## Users

* Make sure allowed users are not disabled.
* Default Guest/Administrator
  + Rename unless specified in readme
  + Disable unless specified in readme
* Delete malicious or unused users
  + If a user is not mentioned in the readme, there is no reason to keep it around.
* For EVERY user account
  + Set secure password for all users
    - At least 8 characters in length
    - Number and symbol
    - “LCt1gers!” or “TacoCat123!”
  + Make sure “Password never expires” is NOT set unless specified by readme
  + Make sure “Password must be changed on next logon” is set

## Groups

* Administrator Group
  + Most important group on system.
  + Add authorized users to group.
  + Remove unauthorized users
* Users Group
  + Also very important; make sure to purge malicious users
  + Add authorized users to group.
  + Remove unauthorized users.
* Remote Users Group
  + Remote desktop users, etc.
  + Target ‘everyone’ object
  + Adding users – better to do this here than in user privilege specification in sec. pol.
    - If a GROUP needs to log in, add it here and in user privilege specification.
    - Otherwise, add only the users that are mentioned in the readme and no others.
    - NEVER add the ‘Everyone’ object unless it’s absolutely necessary – the ‘User’ group is vastly preferred.
* Don’t delete any groups that CyberPatriot has added to the system.
  + Remove permissions from the groups unless specified by the readme
  + Remove uses whose presence in the group would result in inappropriate permissions
* No one should be in ANY other group unless specified by readme (Power users, Recovery Users etc.)
* 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

# User Account Control

* Accessed through Windows Action Center
* Set to ‘Always Notify”
* Double check against Local Security Policy settings to enforce behaviors for Users + Admins

# Windows Services (7/8/10)

1. Windows-Key R -> services.msc. Also accessible through MMC snap-in
   1. Use tskmgr.exe to verify what services are actually running on your system
   2. Verify key services
      * Windows Firewall
      * Security Center
      * Windows Update
      * Event Logger
      * If any of these are not started, ENABLE them in services.msc
2. Be careful with these. If you disable the wrong one, it can easily lose you points in addition to screwing up your image. Be conscious of the required services that the readme wants and are dependencies for server roles. (E.G. Microsoft web server is dependent on IIS.)
3. If you don’t know what a service does, blackviper.com is a great resource.
   1. http://www.blackviper.com/windows-services/
4. Key services to disable:

|  |  |  |  |
| --- | --- | --- | --- |
| ✔ | Service Name | Function | State |
|  |  |  |  |
|  | 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. Cannot be disabled on win10 (maybe?) | 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 |
|  | 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 |
|  | Web Management Service | IIS management | Disabled unless needed on image |
|  | Windows Media Player Network Sharing | Limited media server functionality | Disabled unless needed on image |
|  | 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 |
|  | (win10 only) XBOX services | X-Box dependencies | Disabled |
|  | (win10 only) Application Layer Gateway Service | Legacy and unneeded | Disabled |
|  | (win10 only) Client for NFS | Network filesystem client | Disabled unless needed on image |
|  | (win10 only) Interactive Services Detection | Compatibility | Disabled |
|  | (win10 only) Natural Authentication | Biometric authentication | Disabled |
|  | (win10 only) Microsoft Keyboard Filter | iSCSI compatibility | Disabled |
|  | (win10 only) Multipoint repair service | Distributed LAN server functionality | Disabled |
|  | (win10 only) Multipoint Service | Distributed LAN server functionality | Disabled |
|  | (win10 only) Peer Name Resolution Protocol | DNS discovery for peer-to-peer functionality | Disabled |
|  | (win10 only) Peer Networking grouping | Peer-to-peer networking functionality | Disabled |
|  | (win10 only) Peer networking identity manager | Peer-to-peer networking functionality | Disabled |
|  | (win10 only) Printer extensions and notifications | Printing | Disabled |
|  | (win10 only) Retail demo service | Retail demo functionality | Disabled |
|  | (win10 only) Shared PC Account manager | Laptop/Tablet functionality (portable computers) | Disabled |
|  | (win10 only) Spatial Data Service | Bing APIs | Disabled |
|  | (win10 only) User Profile Service | Active directory logon | Disabled |

# Local Security Policy

Running Policy Analyzer here will give you a simple table to check settings (before and after you work through the configs)

## Account Policy

Windows Key + R > secpol.msc > Account Policies

|  |  |  |
| --- | --- | --- |
| ✔ | Setting Title | Desired Setting |
|  | Password Policy tab |  |
|  | Enforce Password History | 10 |
|  | Max Password Age | 60 |
|  | Minimum password Age | 1 |
|  | 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 |

## User Right Assignment

* Direct EXTREME scrutiny towards the “Everyone” object
* Be careful with DENY permissions, don’t add anything to them, instead revoke ALLOW permissions
* Check to make sure that CyberPatriot-created groups can’t do things that they’re not supposed to be able to. Delete permissions that they’re not supposed to have.
* As always, don’t interfere with any CyberPatriot-related settings

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ✔ | 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 | Identical to default |
|  | Allow log on locally | Allows local logon | Guest, Administrator, Backup Operators, Users | Authorized Users for the system |
|  | 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 | Identical to default |
|  | Bypass traverse checking | Allows directory browsing without appropriate permissions | LOCAL SERVICE,  NETWORK SERVICE,  Administrators,  Backup Operators | Identical to default |
|  | Change the system time | Change the system time for the local computer | LOCAL SERVICE,  Administrators | Identical to default |
|  | Change the time zone | Change the time zone for the local computer | LOCAL SERVICE,  Administrators | As above |
|  | 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 systemwide objects | LOCAL SERVICE,  NETWORK SERVICE,  SERVICE,  Administrators | Identical to default |
|  | Create permeant 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 - OR -  HomeGroupUser$ | Identical to default |
|  | 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 | Identical to default |
|  | Impersonate a client after authentication | Allows acting on behalf of another user | Administrators,  LOCAL SERVICE,  NETWORK SERVICE,  SERVICE | Identical to default |
|  | Increase a process working set | Allocate additional RAM to a process | Users | Identical to default |
|  | Increase scheduling priority | Allows users to increase a process’s resource distribution priority | Administrators | Identical to default |
|  | Load and unload device drivers | Load new drivers into the system. Dangerous as drivers run as system | Administrators and (possibly) Print Operators | Identical to default |
|  | 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 | Identical to default |
|  | 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 | Identical to default |
|  | 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 | Identical to default |
|  | Perform volume maintenance tasks | Allows high-level disk management | Administrators | Identical to default |
|  | Profile single process | Allows profiling program performance | Administrators | Identical to default |
|  | Profile system performance | Allows profiling system-wide performance | Administrators | Identical to default |
|  | Remove computer from docking station | Allows removal of portable device from locking dock | Administrators | Identical to default |
|  | Replace a process level token | Spawn a process using a passed credential token | LOCAL SERVICE,  NETWORK SERVICE | Identical to default |
|  | Restore files and directories | Rollback files to previous restore points | Administrators,  Backup Operators | Identical to default |
|  | Shut down the system | Shut down the system | Administrators,  Backup Operators,  Print Operators,  Server Operators | Identical to default |
|  | 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 | Identical to default |

## Security Options

|  |  |  |
| --- | --- | --- |
| ✔ | Setting Title | Desired Setting |
|  | **Accounts** |  |
|  | Administrator account status | Disabled |
|  | 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** |  |
|  | Shut down system immediately if unable to log security audits | Enabled |
|  | **Devices** |  |
|  | Restrict CDROM access to locally logged-on users only | Enabled |
|  | Restrict Floppy access to locally logged-on users only | Enabled |
|  | Prevent users from installing printer drivers | Enabled |
|  | **Interactive** **Logon** |  |
|  | Display user information when the session is locked | Disabled |
|  | Do not display user last name | Enabled |
|  | Do not require CTRL-ALT-DEL | Disabled |
|  | Machine Inactivity Limit | 1800 seconds |
|  | Prompt user to change password before expiration | 5 days |
|  | Number of Previous logons to cache | 4 |
|  | **Network Client** |  |
|  | Digitally sign communications (if server agrees) | Enabled |
|  | Digitally sign communications (Always) | Enabled |
|  | Send unencrypted password to third-party SMB servers | Disabled |
|  | **Network Server** |  |
|  | Digitally sign communications (if client agrees) | Enabled |
|  | Digitally sign communications (Always) | Enabled |
|  | Disconnect Clients when logon hours expire | Enabled |
|  | Send unencrypted password to clients | Disabled |
|  | Server SPN Target name validation | Accept if provided by client |
|  | Amount of idle time required before suspending session | 15 minutes |
|  | **Network Access** |  |
|  | Do not allow anonymous enumeration of SAM accounts | Enabled |
|  | Allow anonymous SID/Name translation | Disabled |
|  | Do not allow anonymous enumeration of SAM accounts and shares | Enabled |
|  | 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 Clients allowed to make remote calls to SAM | Enabled |
|  | Shares that can be accessed anonymously | Not defined |
|  | Restrict anonymous access to named pipes and shares | Enabled |
|  | 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 |
|  | Do not store LAN manager hash value on next password change | Enabled |
|  | Configure encryption types allowed for Kerberos win7 only | RC4, both AES, future encryption types |
|  | Force Logoff when logon hours expire | Enabled |
|  | LAN manager authentication level | Send NTLMv2 response only, refuse LM and NTLM |
|  | 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 |
|  | **Recovery Console** |  |
|  | Allow automatic administrative logon | Disabled |
|  | Allow floppy copy | Disabled |
|  | **Shutdown** |  |
|  | Allow system to be shut down without having to log on | Disabled |
|  | Clear virtual memory pagefile | Enabled |
|  | **User Account Control** |  |
|  | Admin Approval Mode for the built-in Administrator account | Enabled |
|  | Detect application installation and prompt for elevation | Enabled |
|  | Only elevate UIAccess applications that are installed in secure locations | Disabled |
|  | 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 consent |
|  | Behavior of the elevation prompt for standard users | Prompt for credentials |
|  | Run all administrators in admin approval mode | Enabled |
|  | Switch to the secure desktop when prompting for elevation | Enabled |
|  | Run all administrators in Admin Approval Mode | Enabled |
|  | Virtualize file and registry write failures to per-user locations | Enabled |

# Processes and Malware

### Process Explorer

* Available under Sysinternals -> procecp.exe
* Each line in the program represents a process running on your system
* Colors
  + Green -> New process
  + Red -> Dying process
  + Salmon -> Service-Hosting process. Hover to see hosted services
  + Light Purple/Blue -> Own processes (Processes run by you or using your SID)
  + Acid Purple -> Packed (Encrypted) image in RAM. Exercise extreme scrutiny as packed images are often indicative of malware.
* Configuration
  + File -> Show details for all processes (run as admin)
  + Options -> Verify Image Signatures
    - Companies can sign – verify – programs when they release them. If you see something like “(Verified) Google Inc.” in process explorer you can be certain that Google actually created the software in question.
    - If you see an unsigned image - “No signature was present in the subject” – make sure to check that process out closely. Very likely malware or just shouldn’t be running unless given by readme
  + Options -> VirusTotal -> Check VirusTotal
    - VirusTotal is an online antivirus checker
    - The total in the VirusTotal represents the number of antiviruses that registered a process as malware. 30/64 -> 30 antiviruses thought that process was malware. IE that process is malware 100%.
    - Anything more than 1 or 2 should be CLOSELY looked at unless required by readme.
  + View -> Select Columns -> Username
    - Very useful to link processes to usernames (who is running this malware?)
    - Anything other than SYSTEM and your username should be closely inspected
* Use VirusTotal and Image Signatures to identify potentially suspicious processes.
  + Sort by description, sort by publisher
  + More than 1-2 VirusTotal signatures -> investigate/delete
* 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 in its source folder
* Purge
  + Once you’ve positively identified a process as malware
  + Open its source folder using Right Click -> Properties
  + Right click -> Stop Process
  + Delete its source files

# Rootkits and Backdoors

* First question: Are services clean?
  + Refer to the services section of the checklist
* The best way to do this is through network analysis
  + It’s a lot harder to hide an open/listening port or an active connection than a process
  + Run tcpview.exe from sysinternals for an interactive output with great visibility
  + Red flags
    - Local address of “0.0.0.0:[Port number] means that the process is listening on that port for any connection.
    - :[::] has the same meaning for IPv6
    - For any process that you find suspicious, investigate using either task manager, procmon, 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 kill the process.

# File sharing (7/8/10)

* Configuration is accessible under Computer Management (compmgmt.msc) –Shared Folders
* You can also get a quick view using “net share” from the CMD prompt
* The default ($) shares in Windows are created by default, C$, ADMIN$, IPC$, PRINT$, FAX$
* They are only accessible to administrative users and should not be removed
* If default Windows shares aren’t required
  + Control panel > Network and Sharing center > Advanced sharing settings
    - Turn off “network discovery”
    - Turn off “File and Printer sharing”
    - Turn off “Public Folder Sharing”
    - Leave “Password Protected Sharing” on.
  + Disable “Server” service in services.msc
  + Remove “File and Printer sharing” from the Windows features menu
  + Or block/Disable File and Print Sharing rules in Windows Firewall
* Stop sharing any other shares unless readme says otherwise.
  + Closely inspect the origin folders of each of the shares (is there bad stuff being shared?)
  + Write down for recheck later
* If file and print sharing is required for the scenario, you can lock down access to specific components of it (more secure) using the Windows Firewall
  + Windows key + 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

# Auditing

There are two locations for setting audit policy, for Win7+ it’s recommended to set the Advanced Audit Policy as it will generate less junk in the Security Event log (as a best practice)

For completeness, the legacy option is added here, but the Advanced Pol Config should be the preferred option

## Legacy Auditing Config

Windows Key + R > secpol.msc > Local Policies > Audit Policy

* Main audits
  + Enable success/failure for “Account Logon” events
  + Enable success/failure for “Account Management”
  + Enable success/failure for “Logon Events”
  + Enable success/failure for “Policy Change”
* When in doubt, enable it. This will be done much more granularly down below.

## Advanced Audit Policy Configuration

|  |  |  |
| --- | --- | --- |
| ✔ | Setting Title | Desired Setting |
|  | Audit Credential Validation | Success and Failure |
|  | Audit Kerberos Authentication Service | Not Configured |
|  | Audit Kerberos Service Ticket Operations | Not Configured |
|  | Audit Other Account Logon Events | Success and Failure |
|  | Account Management |  |
|  |  |  |
|  | Audit Application Group management | Not Configured |
|  | Audit Computer Account Management | Not Configured |
|  | Audit Distribution Group Management | Not Configured |
|  | Audit Other Account Management Events | Success and Failure |
|  | Audit Security Group Management | Success and Failure |
|  | Audit User Account Management | Success and Failure |
|  | Detailed Tracking |  |
|  | NOTE: Use this for process forensics and RPC stuff. Don’t turn stuff on in here except for specific reasons or for last-gasp points |  |
|  | DS Access |  |
|  | Don’t configure here except for last-gasp points ; domain stuff |  |
|  | Logon/Logoff |  |
|  | Audit Account Lockout | Success and Failure |
|  | Audit IPsec Extended Mode | Not Configured |
|  | Audit IPsec Main Mode | Not Configured |
|  | Audit IPsec Quick Mode | Not Configured |
|  | Audit Logoff | Success and Failure |
|  | Audit Logon | Success and Failure |
|  | Audit Network Policy Server | Not Configured |
|  | Audit Other Logon/Logoff Events | Success and Failure |
|  | Audit Special Logon | Success and Failure |
|  | Object Access |  |
|  | Audit Application Generated | Not Configured |
|  | Audit Certification Services | Not Configured |
|  | Audit Detailed File Share | Success and Failure |
|  | Audit File Share | Success and Failure |
|  | Audit File System | Not Configured |
|  | Audit Filtering Platform Connection | Not Configured |
|  | Audit Filtering Platform Packet Drop | Not Configured |
|  | Note: Extremely valuable network level forensics ^^ |  |
|  | Audit Handle Manipulation | Not Configured |
|  | Audit Kernel Object | Not Configured |
|  | Audit Other Object Access Events | Success and Failure |
|  | Note: Used for task scheduler events |  |
|  | Audit Registry | Not Configured |
|  | Audit SAM | Success and Failure |
|  | Note: Can spawn a lot of junk |  |
|  | Policy Change |  |
|  | Audit Audit Policy Change | Success and Failure |
|  | Audit Authentication Policy Change | Success and Failure |
|  | Audit Authorization Policy Change | Not Configured |
|  | Audit Filtering Platform Module Change | Not Configured |
|  | Audit MPSSCV Rule-Level Policy Change | Not Configured |
|  | Audit Other Policy Change Events | Not Configured |
|  | Privilege Use |  |
|  | Audit Non Sensitive Privilege Use | Not Configured |
|  | Audit Other Privilege Use | Not Configured |
|  | Audit Sensitive Privilege Use | Success and Failure |
|  | Note: \*Might\* be useful and/or be points |  |
|  | System |  |
|  | Audit IPsec Driver | Not Configured |
|  | Audit Other System Events | Success and Failure |
|  | Note: Logs Firewall-related events |  |
|  | Audit Security State Change | Not Configured |
|  | Audit Security System Extension | Not Configured |
|  | Audit System Integrity | Success and Failure |
|  | Global Object Access Policy |  |
|  | File System | Not Configured |
|  | Registry | Not Configured |

# Scheduled Tasks

* Autoruns.exe (sysinternals)
  + Checks for programs that run on startup
* Colors
  + Yellow - No file where the entry points. (No worries.)
  + Green – Indicates NEW items.
  + Pink - No publisher info found or no signature (Red flag)
* Setup
  + File -> Run as Administrator
  + Options -> Hide Empty Locations
  + Options -> Hide Microsoft Entries
  + Options -> Scan Options -> Verify Code Signatures, Check VirusTotal
  + Options -> Hide VirusTotal clean entries
* Everything tab
  + Inspect anything with 3-4+ VirusTotal hits
  + Look closely at images without signatures (salmon or blank in the publisher tab)
  + Otherwise inspect source location and disable if malicious
    - Anything else in source location? Delete if so
  + Make sure to inspect exactly what the malicious entry is doing and reverse if necessary.
* Logon tab
  + Everything that runs on startup and user login
  + Liberally uncheck things that aren’t essential
  + Check against readme
* Explorer tab
  + Explorer addons
  + VirusTotal hits are good candidates for removal
  + Should typically be blank when VirusTotal clean is checked
  + NO unverified signers or unsigned images here. Likely to be malicious
* Internet Explorer tab
  + All add-ons to internet explorer
  + Uncheck everything not specifically mentioned in readme or baseline
* Scheduled Tasks tab
  + Tasks scheduled to run on system
  + Uncheck “Hide VirusTotal clean entries” for this one
  + Inspect closely for maliciousness (reverse shells, keyloggers, disabling stuff)
* Recheck “Hide VirusTotal clean entries”
* Services
  + Contains services that are autostarted by default
  + Once-over with “Hide VirusTotal clean on”
  + Bulk of configuration should have already been done
* Image Hijacks
  + Windows allows ‘Application substitution’ through the registry.
  + Disable anything here unless CP/Readme related

# CyberPatriot-Installed Software

* Typically googling “Securing x-software” will do this fairly well where x is the name of the software that is installed
* This includes things other than just
* The key goals in most scenarios are:
  + Ensure it is legitimate
  + Ensure it is patched
    - If an auto-update setting exists inside the software, turn it on
  + Ensure only the proper users have access
  + Ensure the application is not adding to the attack surface (risky ports/services etc.)
* Refer to section on securing server roles for more general guidance

# Server Roles: IIS, FTP

## 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

# FileZilla

Filezilla is an alternate, standalone FTP server that runs using a service called “FileZIlla Server FTP Service”

* Make sure the account that FileZilla server is running under is a standard user, not an Administrator or “LocalSystem”
  + Windows Key + R -> "lusrmgr.msc" and hit «ENTER»; "Local Users and Groups" MMC Console appears
  + Create a local Windows User called ‘filezilla’
* Then change the properties for the FileZilla service
  + Windows Key + R -> "services.msc" and hit «ENTER»; "Services" MMC Console appears
  + locate "FileZilla Server FTP server" service and double click; properties dialog appears
  + click "Stop" to stop service if running
  + switch to "Log On" tab and set following:
    - Username: filezilla
    - Password: LCt1gers

IF you change the account that FileZilla is running under, 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
  + Typically 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
* If you upload to some folders set "Full Control" to each topmost writable folder you want to use, the changes are propagated to children
* If you use SSL, double check if both the SSL certificate file and private key file are readable by "filezilla" account, to not break the SSL connection

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.

# Remote Access and RDP

* Remember that there are two “remote” options
  + Control Panel -> System Properties -> Remote
    - OR search “Remote Settings”
  + Remote Assistance is a different access than Remote Desktop Services
  + Disable Remote Assistance (typically) unless specifically mentioned in readme
* By readme – if RDP is allowed, then choose the “secure” option with “Network Level Authentication”
  + Otherwise, disable it altogether.
* 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

# Microsoft Tools: MBSA, Policy Analyzer

## MBSA

* Microsoft Security Baseline Analyzer
* Very useful for making sure you didn’t miss anything stupid
* <https://www.microsoft.com/en-us/download/details.aspx?id=7558>
* Download, install, and run as Administrator
* Look for yellow and red in report.

## Policy Analyzer

* Very useful for printing a simple table of applied local security policy (and some group policy settings)
* Download, install, and run as Administrator
* When the tool is launched, select the following
  + Compare Local Registry and “Local Policy” options
  + Then choose ‘View/Compare”
* The results will simply list all configured local policy settings, so you can check the list against the config and after you’ve made changes to make sure nothing has been missed

# SYSINTERNALS Tools

Sysinternals tools are the best diagnostic options. Have them downloaded on a USB key

* <https://technet.microsoft.com/en-us/sysinternals/bb842062.aspx>

## Process Monitor (procmon.exe)

1. Useful for process analysis
2. Shows all the events on a system at first
3. Let the capture run for ~10s, then stop capture (magnifying glass)
4. Filtering output
   1. 4 icons at the top signify different types of actions
      1. Registry, file access, etc.
      2. Preliminary
   2. Filter section -> Exclude if process name is NOT (process name)
      1. Can also use PID
5. Useful to figure out what exactly a process is doing.

## Process Explorer (procexp.exe)

1. Configuration
   1. Options > Verify Image Signatures : Makes sure processes are legit
   2. Options > VirusTotal > Check VirusTotal : Checks processes against malware database
   3. Run as administrator
2. Look for suspicious processes
3. Sort by description, sort by publisher
4. Right click > Properties
   1. Investigate a process
   2. 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

* Monitors all events on system. Used to just be 3 logs –Application, System, Security, but Windows now has dozens of different logs that you can see under ‘Applications and Services’
* For CyberPatriot, we’ll focus on the Security log.
* To access event viewer:
  + Computer Management -> System Tools -> Event Viewer
  + Or just eventvwr from the Run line

## Security Log

* As auditing is enabled, many events will be logged here.
* Expand ‘Windows Logs’ and Right click on Security and choose Properties
* Set the max log size to 196608
* Set the ‘Overwrite events as needed’

To view event data:

* Right click on “Security” and “Select Filter Current Log” then plug in Event ID’s into the field
* Or Select the event source of “Microsoft Windows Security Auditing”
  + Then select the Task Categories for events you want to review
    - These match to audit categories –Logon, Account management…

### Select Event ID’s

* 4624 –Logon Event
* 4723 –User Account Management (attempt to change a 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 (FileZilla etc.)

## System log

* 1. Service issues (startup failures..)
  2. firewall stability, DNS
  3. Anything red/yellow
     + filter
       - Right click system > Filter
       - critical & warning (red/yellow)
  4. [Checking for software installs](http://eventlogs.blogspot.com/2007/11/tracking-software-installation-and.html)

1. Yellows and Reds
   1. Source: Gives you an idea for what you need to look at
      * What interface is this source tied to?
   2. Double-click -> Descriptions
   3. Look into that area.

# Miscellaneous

## Secure Screensaver

* Control Panel > Screen saver settings > On resume, display logon screen

## Media Files

* + Organize -> Folder and Search options -> View hidden files, UNCHECK hide extensions for hidden file types
  + Navigate to the folder “C:\Users\”
  + Use the following search (upper right) syntax: “kind:=[filetype]”
    - Make sure to exclude the brackets
    - kind:=picture
    - kind:=program
    - kind:=music
    - kind:=video
    - kind:=document
  + If this doesn’t work, searching for “\*.jpg”, ”\*.txt” etc. might.
  + Also make sure to check all of the directories in your home directory by hand

## Hosts File

* Static DNS on local box.
* Can occur when you type in a website and go to a DIFFERENT website.
* Windows ALWAYS checks hosts file first. > Check for networking errors.
* All lines should be blank unless they have something to do with CyberPatriot.
  + If a line is there, # it instead of deleting it.
* NOTE: #s mean that the line is ignored by the operating system.
* How to edit
  + Run notepad as Administrator
  + File -> Open
  + Change “Text Documents (\*.txt)” to “All files”
  + Type in navbar: “C:\Windows\System32\drivers\etc\”
  + Select “hosts”
  + Make edits -> Save.

## Require a password when the computer wakes up

* Control Panel -> Hardware and Sound -> Power Options -> System settings
* Under ‘Password protection on wakeup’, select ‘Require a password.’

## Administrative Templates

* It is possible to disable a service through something called an ‘Administrative Template.’ (Group policy for local computer)
* Run ‘gpedit.msc’
* Computer Configuration -> Administrative Templates -> All settings
* Sort on the “State” field both ways – make sure nothing is doing anything