Scroll According to Scholtes

Ben Scholtes

# Checklist

Read Scenario

* Authorized Users
* Critical Services
  + RDP
  + Browsers

Baseline

* Check Ports
  + Netstat -aon
  + Task Manager

Forensics Questions

* Google if stuck

Firefox (and other browsers)

* Update
* Secure

Control Panel

* Firewall
  + On or Off
  + Rules
* RDP
  + Critical Services (Read Me)
  + Remote Assistance disabled
* Windows Defender
  + Quick Scan
  + MalwareBytes also works
* Programs
  + Unistall
  + Look up all programs
* Turn Windows features on or off
  + All but .Net 4.8 need to be off
* Smart Screen
* UAC
* Lockout
  + Screen Saver

Computer Management

* Users and Groups
  + Scenario
  + Disable Guest accounts
* Passwords
* Services
* Shared Folders
  + C$
  + IPC$
  + ADMIN$

Secpol

* Account Policies
  + Password
  + Lockout
* Local
  + Audit
  + URA
  + Security Options
* Firewall
* Advanced Audits

Settings

* Updates
* Security
* AutoPlay

File Explorer

* Search for hidden files
* Search for .mp3 etc.
* Properties

Group Policy

* Sort by configured
* Read what they mean

Applications

* Update
* Security

Registry

* Run/Run Once
* DisableAntiSpyware
* Permissions

# Details

### Baseline

* Command Prompt
  + Use “netstat -aon” to check listening ports
    - Or “netstat -aonb”
* Task Manager
  + Check for unwanted processes
  + Match PIDs with command line

### Forensics

* Use:
  + [Rumkin](https://rumkin.com/tools/cipher/)
  + [dCode Tools List](https://www.dcode.fr/tools-list)
  + [CyberChef](https://gchq.github.io/CyberChef/)
  + [Hash Analyzer](https://www.tunnelsup.com/hash-analyzer/)
  + [CVE](https://cve.mitre.org/)
  + [Cryptii](https://cryptii.com/)
* For MD5 and SHA256:
  + certutil -hashfile <file name> <encryption>

### Firefox

* Update
  + Help->About->Update
* Secure
  + Enhanced Tracking Protection
    - Strict
  + Send websites a “Do Not Track”
    - Always
  + Cookies and Site Data
    - Check box
  + Logins and Password
    - Ask to save logins
      * Uncheck box
    - Autofill logins and passwords
      * Uncheck box
    - Suggest and generate strong passwords
      * Uncheck box
    - Show Alerts about passwords
      * Check box
    - Use a Primary Password
      * Uncheck box
    - Allow Windows single sign-on
      * Uncheck box
  + Forms and Autofill
    - Autofill addresses
      * Uncheck box
    - Autofill credit cards
      * Uncheck box
  + Permissions
    - Location
      * Remove all from settings
    - Camera
      * Remove all from settings
    - Microphone
      * Remove all from settings
    - Notifications
      * Remove all from settings
      * Uncheck pause notification
    - Autoplay
      * Remove all from settings
    - Virtual Reality
      * Remove all from settings
    - Block pop-up windows
      * Check box
      * Remove all from exceptions
    - Warn when websites try to install
      * Check box
      * Remove all from exceptions
  + Firefox Data and Collection
    - Uncheck all boxes
  + Deceptive Content and Dangerous Software
    - Check all boxes
  + Certificates
    - Check box
  + HTTPS-Only Mode
    - Enable HTTPS-Only Mode in All Windows

### Chrome

* Autofill
  + Password Manager
    - Offer to save passwords
      * Off
    - Auto Sign-in
      * Off
    - Saved Passwords
      * Remove all passwords
  + Payment Methods
    - Save and fill payment methods
      * Off
    - Allow sites to check if you have payment methods saved
      * Off
    - Payment methods
      * Remove all payment methods
  + Addresses and more
    - Save and fill addresses
      * Off
    - Addresses
      * Remove all addresses
  + Privacy and Security
    - * Cookies and other site data
        + Block all cookies

On

* + - * + Clear cookies and site data when you close all windows

On

* + - * + Send a “Do Not Track” request with your browsing traffic

On

* + - * + See all site data and permissions

Clear all data

* + - * + Customized behviors

Remove all

* + - * Security
        + Enhanced protection

On

* + - * + Always use secure connections

On

* + - * + Use secure DNS

On

* + - * Site Settings
        + View permissions and data stored across sites

Clear all data

* + - * + Location

Don’t allow sites to see your location

* + - * + Camera

Don’t allow sites to use your camera

* + - * + Microphone

Don’t allow sites to use your microphone

* + - * + Notifications

Don’t allow sites to send notifications

* + - * + Background sync

Don’t allow closed sites to finish sending or receiving data

* + - * + Additional permissions

Don’t allow for all

* + - * + Content

Don’t allow for all

* + - System
      * Continue running background apps when Chrome is closed
        + Off

### Control Panel

* System and Security
  + Security and Maintenance
    - Change User Account Control settings
      * Always Notify
    - Maintenance
      * Start Maintenance
  + Windows Defender Firewall
    - Advanced Settings
      * Domain Profile
        + Firewall State

On (recommended)

* + - * + Inbound Connections

Block (default)

* + - * + Outbound Connections

Allow (default)

* + - * Private Profile
        + Firewall State

On (recommended)

* + - * + Inbound Connections

Block (default)

* + - * + Outbound Connections

Allow (default)

* + - * Public Profile
        + Firewall State

On (recommended)

* + - * + Inbound Connections

Block (default)

* + - * + Outbound Connections

Allow (default)

* + - * IPsec Settings
        + Exempt ICMP from IPsec

No (default)

* + System
    - Remote Settings
      * Remote Assistance
        + Allow Remote Assistance connections to this computer

Uncheck box

* + - * Remote Desktop
        + Don’t allow remote connections to this computer

Select unless the ReadMe needs RDP

* + - * + Allow remote connections to this computer

Don’t select unless the ReadMe needs RDP

* + - * + Allow connections from authorized computer

Check, especially if RDP is required

* + Power Options
    - Change when the computer sleeps
      * Turn off the display
        + 15 minutes
      * Put the computer to sleep
        + 15 minutes
* Network and Internet
  + Internet Options
    - Security
      * Internet
        + Security level for this zone

High

Enable Protected Mode

Check box

* + - * Local Intranet
        + Security level for this zone

High

Enable Protected Mode

Check Box

* + - * Trusted Sites
        + Security level for this zone

High

Enable Protected Mode

Check box

* + - * Restricted Site s
        + Security level for this zone

High

Enable Protected mode

Check box

* Hardware and Sound
  + AutoPlay
    - Use AutoPlay for all media and devices
      * Uncheck box
    - Set all to Ask me every time
* Programs
  + Programs and Features
    - Google all programs and remove if
      * Suspicious
      * Not required by ReadMe
  + Turn Windows Features On or Off
    - Turn all off except:
      * .NET Framework 4.8
      * Work Folder Client
      * IIS can be on if required by ReadMe

### Computer Management

* Shared Folders
  + Shares
    - Remove all except the default shares:
      * ADMIN$
      * C$
      * IPC$
      * Any required by the ReadMe
* Local Users and Groups
  + Users
    - Disable all guest and unauthorized accounts
    - Create any authorized accounts that are missing
    - Set 14 character (or higher) password for all accounts
    - Set all to change password at next logon
  + Groups
    - Check Administrator Group
      * Remove unauthorized users
      * Add authorized users
    - Create any group that needs is required by ReadMe
  + Services
    - Started and Automatic:
      * BITS
      * CCS Client
      * DNS Client
      * DHCP Client
      * Diagnostic Service Host
      * IPsec Policy Agent
      * Windows Defender Advanced Threat Protection
      * Windows Defender Firewall
      * Windows Event Collector
      * Windows Event Log
      * Windows Installer
      * Windows Search
      * Windows Time
      * Windows Update
      * WMI Performance Adapter
    - Stopped and Disabled:
      * Fax
      * Geolocation
      * Infrared Monitor Service
      * IP Helper
      * Net TCP Port Sharing
      * Netlogon
      * Phone Service
      * Plug and Play
      * Print Spooler
      * Remote Desktop Services (README)
      * Remote Registry
      * Secondary Logon
      * Simple TCP/IP Services
      * Smart Card
      * SNMP Trap
      * SSDP Discovery
      * TCP/IP NetBios Helper
      * Telephoney
      * Telnet
      * WebClient
      * World Wide Web Publishing Service

### Secpol

* Account Policies
  + Password Policies
    - Enforce password history
      * 7 passwords
    - Maximum password age
      * 30 days
    - Minimum password age
      * 15 days
    - Minimum password length
      * 14 characters
    - Password must meet complexity requirements
      * Enabled
    - Store passwords using reversible encryption
      * Disabled
  + Account Lockout Policy
    - Account lockout duration
      * 30 minutes
    - Account lockout threshold
      * 5 invalid logon attempts
    - Reset account lockout counter after
      * 30 minutes
* Local Policies
  + Audit Policy
    - Audit account logon events
      * Success and Failure
    - Audit account management
      * Success and Failure
    - Audit directory service access
      * Success and Failure
    - Audit logon events
      * Success and Failure
    - Audit object access
      * Success and Failure
    - Audit policy change
      * Success and Failure
    - Audit privilege use
      * Success and Failure
    - Audit process tracking
      * Success and Failure
    - Audit system events
      * Success and Failure
  + User Rights Assignment
    - Access Credential Manager as a trusted caller
      * No One
    - Access this computer from the network
      * Administrators, Remote Desktop Users
    - Act as part of the operating system
      * No One
    - Adjust memory quotas for a process
      * Administrator, LOCAL SERVICE, NETWORK SERVICE
    - Allow log on locally
      * Administrators, Users
    - Allow log on through Remote Desktop Services
      * Administrators, Remote Desktop Users
    - Back up files and directories
      * Administrators
    - Change the system time
      * Administrators
    - Change the time zone
      * Administrators, LOCAL SERVICE, Users
    - Create a token object
      * No One
    - Create global objects
      * Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE
    - Create permanent shared objects
      * No One
    - Debug programs
      * Administrators
    - Deny access to this computer from the network
      * Guest, Local account
    - Deny log on as a batch job
      * Guests
    - Deny log on as a service
      * Guests
    - Deny log on locally
      * Guests
    - Deny log on through Remote Desktop Services
      * Guests, Local account
    - Enable computer and user accounts to be trusted for delegation
      * No One
    - Force shutdown from a remote system
      * Administrators
    - Generate security audits
      * LOCAL SERVICE, NETWORK SERVICE
    - Impersonate a client after authentication
      * Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE
    - Increase scheduling priority
      * Administrators
    - Load and unload device drivers
      * Administrators
    - Lock pages in memory
      * No One
    - Log on as a batch job
      * Administrators
    - Manage auditing and security log
      * Administrators
    - Modify an object label
      * No One
    - Modify firmware environment values
      * Administrators
    - Perform volume maintenance tasks
      * Administrators
    - Profile single process
      * Administrators
    - Profile system performance
      * Administrators
    - Replace process level token
      * LOCAL SERVICE, NETWORK SERVICE
    - Restore files and directories
      * Administrators
    - Shut down the system
      * Administrators, Users
    - Take ownership of file or other objects
      * Administrators
  + Security Options
    - Accounts
      * Administrator account status
        + Disabled
      * Block Microsoft accounts
        + Users can’t add or log on with Microsoft accounts
      * Guest account status
        + Disabled
      * Limit local account use of blank password to console logon only
        + Enabled
    - Audit
      * Force audit policy subcategory settings to override audit policy category settings
        + Enabled
      * Shut down system immediately if unable to log security audits
        + Disabled
    - Devices
      * Allowed to format and eject removable media
        + Administrators and Interactive Users
      * Prevent users from installing printer drivers
        + Enabled
    - Domain Member
      * Digitally encrypt or sign secure channel data (always)
        + Enabled
      * Digitally encrypt secure channel data (when possible)
        + Enabled
      * Digitally sign secure channel data (when possible)
        + Enabled
      * Disable machine account password changes
        + Disabled
      * Maximum machine account password age
        + 30 days or fewer
      * Require strong session key
        + Enabled
    - Interactive logon
      * Do not require CTRL+ALT+DEL
        + Disabled
      * Don’t display last signed-in
        + Enabled
      * Machine account lockout threshold
        + 5-7 invalid logon attempts
      * Machine inactivity limit
        + 900 (or fewer) seconds
      * Number of previous logons to cache
        + 4 or fewer logon(s)
      * Prompt user to change password before expiration
        + 7 days
      * Smart card removal behavior
        + No Action
    - Microsoft network client
      * Digitally sign communications (always)
        + Enabled
      * Digitally sign communications (if server agrees)
        + Enabled
      * Send unencrypted password to third-party SMB servers
        + Disabled
    - Microsoft network server
      * Amount of idle time required before suspending session
        + 15 minutes
      * Digitally sign communications (always)
        + Enabled
      * Digitally sign communications (if possible)
        + Enabled
      * Disconnect clients when logon hours expire
        + Enabled
      * Server SPN target name validation level
        + 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 password and credentials for network authentication
        + Enabled
      * Let Everyone permissions apply to anonymous users
        + Disabled
      * Named Pipes that can be accessed anonymously
        + None
      * Restrict anonymous access to Named Pipes and Shares
        + Enabled
      * Restrict clients allowed to make remote calls to SAM
        + Administrators: Remote Access: Allow
      * Shares that can be accessed anonymously
        + None
      * Sharing and security model for local accounts
        + Classic - local users authenticate as themselves
    - Network Security
      * Allow Local System to use computer identity for NTLM
        + Enabled
      * Allow LocalSystem NULL session fallback
        + Disabled
      * Allow PKU2U authentication requests to this computer to use online identities
        + Disabled
      * Configure encryption types allowed for Kerberos
        + AES128\_HMAC\_SHA1, AES256\_HMAC\_SHA1, 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 & NTLM
      * LDAP Client signing requirements
        + Negotiate signing
      * Minimum session security for NTLM SSP based clients
        + Require NTLMv2 session security, Require 128-bit encryption
      * Minimum session security for NTLM SSP based servers
        + Require NTLMv2 session security, Require 128-bit encryption
    - System cryptography
      * Force strong key protection for user keys stored on the computer
        + User is prompted when the key is first used
    - System objects
      * Require case insensitivity for non-Windows subsystems
        + Enabled
      * Strengthen default permissions of internal system objects
        + Enabled
    - User Account Control
      * Admin Approval Mode for the Built-in Administrator account
        + Enabled
      * Behavior of the elevation prompt for administrators in Admin Approval Mode
        + Prompt for consent on the secure desktop
      * Behavior of the elevation prompt for standard users
        + Automatically deny elevation requests
      * Detect application installations and prompt for elevation
        + Enabled
      * Only elevate UIAccess applications hat 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
* Windows Firewall with Advanced Security
  + Same as [control panel](#_2u3vtsz1j8nc)

### Settings

* System
  + About
    - Advanced Settings
      * Turn on DEP for all
* Devices
  + AutoPlay
    - AutoPlay
      * Use AutoPlay for all media and devices
        + Off
    - Choose AutoPlay defaults
      * Removable drive
        + Ask me everytime
      * Memory card
        + Ask me everytime
* Apps
  + Default apps
    - Check ReadMe for any that need to be changed
  + Startup
    - Check Startup Apps to see if any are bad
* Search
  + Permissions & History
    - Safe Search
      * Strict-Filter out adult text, images, and videos from my web results
* Update & Security
  + Windows Update
    - Run updates while eating and at a convenient time
  + Windows Security
    - Open Windows Security
      * Virus & threat protection
        + Quick scan (unless you use Malwarebytes)
        + Allowed threats

Check for anything there

* + - * + Virus & threat protection settings

Real-time protection

On

Cloud-delivered protection

On

Automatic sample submission

On

Tamper Protection

On

Exclusions

Check for any exclusions (there should be none)

Notifications

Virus & threat protection notifications

Get informational notifications

On

Recent activity and scan results

Check box

Threats found, but no immediate action is needed

Check box

Files or activities are blocked

Check box

Firewall & network protection notifications

Notify me when Microsoft Defender Firewall blocks a new app

On

Domain firewall

Check box

Private firewall

Check box

Public firewall

Check box

* + - * + Ransomware Protection

Controlled folder access

On

Allow an app through Controlled folder access

Check for any unauthorized apps

* + - * App & Browser control
        + Reputation based protection settings (formerly smart screen)

Check apps and files

On

SmartScreen for Microsoft Edge

On

Potentially unwanted app blocking

On

Block apps

Check box

Block downloads

Check box

SmartScreen for Microsoft Store apps

* + - * + Exploit protection

System settings

Change everything to default

* + - * Device security
        + Core isolation

Memory integrity

On

### Registry

* HKEY\_Local\_Machine\SOFTWARE\Microsoft\Windows\CurrentVersion
  + Run
    - (Default) REG\_SZ (value not set)
    - VMware User Process REG\_SZ “C:\Program Files\VMware\VMware Tools\vmtoolsd.exe” -n vmusr
  + RunOnce
    - (Default) REG\_SZ (value not set)
* HKEY\_Local\_Machine\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon
  + AutoAdminLogon
    - AutoAdminLogon 0
* HKEY\_Local\_Machine\SOFTWARE\Microsoft\Windows\CurrentVersion\Explore
  + Shell Folders
    - (Default) (value not set)
    - Common Administrative Tools C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Administrative Tools
    - Common AppData C:\ProgramData
    - Common Desktop C:\Users\Public\Desktop
    - Common Documents C:\Users\Public\Documents
    - Common Programs C:\ProgramData\Microsoft\Windows\Start Menu\Programs
    - Common Start Menu C:\ProgramData\Microsoft\Windows\Start Menu
    - Common Startup C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
    - Common Templates C:\ProgramData\Microsoft\Windows\Templates
    - CommonMusic C:\Users\Public\Music
    - CommonPictures C:\Users\Public\Pictures
    - CommonVideo C:\Users\Public\Videos
    - OEM Links C:\ProgramData\OEM\Links
    - PSPath Microsoft.PowerShell.Core\Registry::HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\
    - PSParentPath Microsoft.PowerShell.Core\Registry::HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer
    - PSChildName Shell Folders
    - PSDrive HKLM
    - PSProvider Microsoft.PowerShell.Core\Registry
  + User Shell Folders
    - (Default) (value not set)
    - Common AppData C:\ProgramData
    - Common Desktop C:\Users\Public\Desktop
    - Common Documents C:\Users\Public\Documents
    - Common Programs C:\ProgramData\Microsoft\Windows\Start Menu\Programs
    - Common Start Menu C:\ProgramData\Microsoft\Windows\Start Menu
    - Common Startup C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
    - Common Templates C:\ProgramData\Microsoft\Windows\Templates
    - CommonMusic C:\Users\Public\Music
    - CommonPictures C:\Users\Public\Pictures
    - CommonVideo C:\Users\Public\Videos
    - {3D644C9B-1FB8-4f30-9B45-F670235F79C0} C:\Users\Public\Downloads
    - PSPath Microsoft.PowerShell.Core\Registry::HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\
    - PSParentPath Microsoft.PowerShell.Core\Registry::HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer
    - PSChildName User Shell Folders
    - PSDrive HKLM
    - PSProvider Microsoft.PowerShell.Core\Registry
* HKEY\_Current\_User\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer
  + Shell Folders
    - (Default) (value not set)
    - !Do not use this registry key Use the SHGetFolderPath or SHGetKnownFolderPath function instead
    - AppData C:\Users\cyber\AppData\Roaming
    - Local AppData C:\Users\cyber\AppData\Local
    - {1B3EA5DC-B587-4786-B4EF-BD1DC332AEAE} C:\Users\cyber\AppData\Roaming\Microsoft\Windows\Libraries
    - My Video C:\Users\cyber\Videos
    - My Pictures C:\Users\cyber\Pictures
    - Desktop C:\Users\cyber\Desktop
    - History C:\Users\cyber\AppData\Local\Microsoft\Windows\History
    - NetHood : C:\Users\cyber\AppData\Roaming\Microsoft\Windows\Network Shortcuts
    - {56784854-C6CB-462B-8169-88E350ACB882} C:\Users\cyber\Contacts
    - {00BCFC5A-ED94-4E48-96A1-3F6217F21990} C:\Users\cyber\AppData\Local\Microsoft\Windows\RoamingTiles
    - Cookies C:\Users\cyber\AppData\Local\Microsoft\Windows\INetCookies
    - Favorites C:\Users\cyber\Favorites
    - SendTo C:\Users\cyber\AppData\Roaming\Microsoft\Windows\SendTo
    - Start Menu C:\Users\cyber\AppData\Roaming\Microsoft\Windows\Start Menu
    - My Music C:\Users\cyber\Music
    - Programs C:\Users\cyber\AppData\Roaming\Microsoft\Windows\Start Menu\Programs
    - Recent C:\Users\cyber\AppData\Roaming\Microsoft\Windows\Recent
    - CD Burning C:\Users\cyber\AppData\Local\Microsoft\Windows\Burn\Burn
    - PrintHood C:\Users\cyber\AppData\Roaming\Microsoft\Windows\Printer Shortcuts
    - {7D1D3A04-DEBB-4115-95CF-2F29DA2920DA} C:\Users\cyber\Searches
    - {374DE290-123F-4565-9164-39C4925E467B} C:\Users\cyber\Downloads
    - {A520A1A4-1780-4FF6-BD18-167343C5AF16} C:\Users\cyber\AppData\LocalLow
    - Startup C:\Users\cyber\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
    - Administrative Tools C:\Users\cyber\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Administrative Tools
    - Personal C:\Users\cyber\Documents
    - {BFB9D5E0-C6A9-404C-B2B2-AE6DB6AF4968} C:\Users\cyber\Links
    - Cache C:\Users\cyber\AppData\Local\Microsoft\Windows\INetCache
    - Templates C:\Users\cyber\AppData\Roaming\Microsoft\Windows\Templates
    - {4C5C32FF-BB9D-43B0-B5B4-2D72E54EAAA4} C:\Users\cyber\Saved Games
    - Fonts C:\Windows\Fonts
    - PSPath Microsoft.PowerShell.Core\Registry::HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\
    - PSParentPath Microsoft.PowerShell.Core\Registry::HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer
    - PSChildName Shell Folders
    - PSDrive HKCU
    - PSProvider Microsoft.PowerShell.Core\Registry
  + User Shell Folders
    - (Default) (value not set)
    - {374DE290-123F-4565-9164-39C4925E467B} C:\Users\cyber\Downloads
    - AppData C:\Users\cyber\AppData\Roaming
    - Cache C:\Users\cyber\AppData\Local\Microsoft\Windows\INetCache
    - Cookies C:\Users\cyber\AppData\Local\Microsoft\Windows\INetCookies
    - Desktop C:\Users\cyber\Desktop
    - Favorites C:\Users\cyber\Favorites
    - History C:\Users\cyber\AppData\Local\Microsoft\Windows\History
    - Local AppData C:\Users\cyber\AppData\Local
    - My Music C:\Users\cyber\Music
    - My Pictures C:\Users\cyber\Pictures
    - My Video C:\Users\cyber\Videos
    - NetHood C:\Users\cyber\AppData\Roaming\Microsoft\Windows\Network Shortcuts
    - Personal C:\Users\cyber\Documents
    - PrintHood C:\Users\cyber\AppData\Roaming\Microsoft\Windows\Printer Shortcuts
    - Programs C:\Users\cyber\AppData\Roaming\Microsoft\Windows\Start Menu\Programs
    - Recent C:\Users\cyber\AppData\Roaming\Microsoft\Windows\Recent
    - SendTo C:\Users\cyber\AppData\Roaming\Microsoft\Windows\SendTo
    - Start Menu C:\Users\cyber\AppData\Roaming\Microsoft\Windows\Start Menu
    - Startup C:\Users\cyber\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
    - Templates C:\Users\cyber\AppData\Roaming\Microsoft\Windows\Templates
    - {374DE290-123F-4565-9164-39C4925E467B} C:\Users\cyber\Downloads
    - PSPath Microsoft.PowerShell.Core\Registry::HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders\
    - PSParentPath Microsoft.PowerShell.Core\Registry::HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer
    - PSChildName User Shell Folders
    - PSDrive HKCU
    - PSProvider Microsoft.PowerShell.Core\Registry

### Group Policy

* Computer Configuration
  + Windows Settings
    - Scripts
      * Startup
        + Make sure it is empty
      * Shutdown
        + Make sure it is empty
    - Security Settings
      * See [Secpol](#_3l2xxfkf5l1x)
  + Administrative Templates
    - See: [Benchmarks](https://loyolablakefield.myschoolapp.com/ftpimages/869/download/download_7106719.pdf)
    - All Settings
      * Sort by configured and see if any are important
* User Configuration
  + Windows Settings
    - Scripts
      * Logon
        + Make sure it is empty
      * Logoff
        + Make sure it is empty
  + Administrative Templates
    - See: [Benchmarks](https://loyolablakefield.myschoolapp.com/ftpimages/869/download/download_7106719.pdf)
    - All Settings
      * Sort by configured and see if any are important

### File Explorer

* View
  + File name extensions
    - Check box
  + Hidden items
    - Check box
* Search
  + Search using “\*.<extension>” for these extensions:
    - .aspx
    - .cda
    - .gif
    - .htm
    - .html
    - .jpg
    - .jpeg
    - .mp3
    - .mp4
    - .mpeg
    - .pdf
    - .png
    - .rtf
    - .txt
    - .vbs
* This PC
  + Local Disk (C:)
    - Check DNS Host file
      * C:\Windows\System32\drivers\etc
    - Search
      * Search using “\*.<extension>” for these extensions:
        + .aspx
        + .bat (only in users)
        + .cda
        + .exe (only in users)
        + .gif
        + .htm
        + .html
        + .jpg
        + .jpeg
        + .mp3
        + .mp4
        + .mpeg
        + .pdf
        + .png
        + .rtf
        + .txt
        + .vbs
    - Program Files
      * Look for any unwanted folders
    - Program Files (x86)
      * Look for any unwanted folders
    - Users
      * Check for any unwanted files in:
        + Desktop
        + Documents
        + Downloads
        + Pictures
        + Videos

### Antivirus Scan

* Use one of these
  + Windows Defender
    - Run a quick scan
    - If desperate run full
  + Malwarebytes
    - [Download](https://www.malwarebytes.com/mwb-download)
    - Set up
      * Who are you trying to protect
        + Select “Me or My Family”
    - Run a scan
    - Check report
      * Scorebot is considered malware now
    - Quarantine, don’t delete unless necessary

# Applications

### (IIS) Internet Information Services

#### Web Services

* DESKTOP
  + Authentication
    - Anonymous Authentication
      * Disable
    - ASP.NET Impersonation
      * Disable
  + Default Document
    - The document the website should open to should be moved up
  + Directory Browsing
    - Disable
  + Logging
    - One log file per
      * Site
    - Log File
      * Format
        + W3C
      * Directory
        + %SystemDrive%\inetpub\logs\LogFiles
      * Encoding
        + UTF-8
    - Log Event Destination
      * Both log file and ETW event
    - Log File Rollover
      * Maximum file size (in bytes)
        + 100000000
* Application Pools
  + Right-Click on DefaultAppPool
    - Advanced Settings
      * Click [...] next to Identity
        + Select Built-in account

Choose ApplicationPoolIdentity

* Sites
  + Click on the required site (Default Web Site)
    - Basic Settings
      * Select…
        + DefaultAppPool (or desired App Pool)
  + Default Web Site
    - Change binding to HTTPS over port 443
    - SSL Settings
      * Require SSL
      * Client certificates
        + Require

#### FTP

* DESKTOP
  + FTP Authentication
    - Anonymous Authentication
      * Disabled
    - Basic Authentication
      * Enabled
  + FTP Logging
    - One log file per
      * Site
    - Log File
      * Directory
        + C:\inetpub\logs\LogFiles
      * Encoding
        + UTF8
    - Log File Rollover
      * Maximum file size (in bytes)
        + 100000000
  + FTP Logon Attempt Restrictions
    - Enable FTP logon Attempt Restrictions
      * Check Box
    - Maximum number of failed login attempts
      * 4-5 attempts
    - Time period (in seconds)
      * 21600
    - Deny IP addresses based on the number of failed login attempts
  + FTP SSL Settings
    - SSL Certificate
      * Select one or make one
    - SSL Policy
      * Require SSL connections
    - Use 128-bit encryption for SSL connections
      * Check box

### (AD DS) Active Directory Domain Services

For Installation:

* Add role
* Promote to Domain Controller
  + Add a new forest
    - Root Domain Name
      * *Something*.com
  + Password must be complex and 12+ characters
  + Make sure local admins have complex and 12+character passwords

Post-Installation:

Active Directory Users and Computers

* *Something*.com
  + Users
    - Sort by type and go to users
      * Disable all guest and unauthorized accounts
      * Create any authorized accounts that are missing
      * Set 14 character (or higher) password for all accounts
      * Set all to change password at next logon
    - Check all groups
      * Use ReadME
      * Principle of Least Privilege
  + Domain Controllers
    - ReadMe
    - Make sure all DCs are authorized
  + Computers
    - ReadMe
    - Make sure all computers are authorized

### (SMB) Server Message Block

(Chat GPT Response:

* Keep the Server Up to Date: Regularly install Windows updates, including security patches, to address any known vulnerabilities in SMB.
* Enable SMB Encryption: Enable encryption for SMB traffic to ensure data confidentiality. This can be done by enabling the "EncryptData" registry value for the SMB service.
* Disable SMBv1: SMBv1 is an outdated and vulnerable version of the protocol. Disable it entirely or limit its usage to legacy systems if necessary. This can be achieved by disabling the "SMB 1.0/CIFS File Sharing Support" feature in the Server Manager or by modifying the registry.
* Enable SMBv2 or SMBv3: Ensure that SMBv2 or SMBv3 is enabled on the server to leverage the improved security features and capabilities of these newer versions.
* Enable Secure Negotiate: Enable the "RequireSecureNegotiate" registry value to ensure that SMB connections require the highest level of security negotiation.
* Enable Opportunistic Locking (OpLock) Security: Opportunistic Locking can enhance performance but also introduces potential risks. Configure OpLocks to only be granted to trusted clients by enabling the "EnableOplocks" and "EnableSecuritySignature" registry values.
* Configure SMB Signing: Enable SMB signing to prevent tampering and unauthorized modification of SMB packets. Enable the "RequireSecuritySignature" and "EnableSecuritySignature" registry values to enforce SMB signing.
* Enable Access-Based Enumeration (ABE): ABE allows users to see only the files and folders they have permission to access. Enable ABE on shared folders to enhance security and prevent unauthorized browsing.
* Implement Strong Authentication: Require strong authentication for SMB connections by enabling Extended Protection for Authentication. This can be achieved by configuring Group Policy settings.
* Restrict SMB Access: Limit SMB access to trusted networks, subnets, or specific IP addresses through firewall rules or network access control mechanisms.
* Implement User Authentication and Authorization: Ensure that users accessing SMB shares have appropriate authentication and authorization. Use strong, complex passwords and implement proper user access controls.
* Regularly Monitor and Audit SMB Activity: Implement logging and monitoring for SMB traffic to detect any suspicious or unauthorized access attempts. Review logs regularly to identify potential security incidents.

)

* Shares
  + *Active Share*
    - Properties
      * Permissions
        + Customize Permissions

Depends on ReadMe and apply principle of least privilege

Auditing

Add

Select a Principal

Everyone

Type

All

Applies to

This folder, subfolders and files

Basic Permissions

Full control

* + - * Settings
        + Enable access-based enumeration

Check box

* + - * + Allow caching of share

Check box

* + - * + Enable BranchCache on the file share

Check box

* + - * + Encrypt data access

Check box

### FileZilla

* Configure
  + Protocol Settings
    - Autoban
      * Ban IP address after: 5 failed login attempts
      * If they happen within: 3600 seconds
      * The ban will last: 21600 seconds
    - Timeout
      * Login timeout: 60 seconds
      * Activity timeout: 10 minutes
    - Performance
      * Depends on server stress
    - Filters
      * ReadMe
  + FTP and FTP over TLS(FTPS)
    - Minimum allowed TLS version
      * v1.3
    - TLS certificate
      * Use a self-signed X.509 certificate
      * Generate new if needed
  + Rights Management
    - Use system the server is running under
  + Users
    - Create Users as needed
    - User is enabled
      * Check box
    - Require a password to login
      * Assign a secure password
      * Could also switch to using system credentials
    - Assign to proper group
  + Groups
    - Create Groups as needed
  + Administration
    - Connection
      * Local Listening Port
        + 14147
      * Password
        + Check box
        + Enter secure password
    - Connection Security
      * Use same settings as FTP over TLS(FTPS)
  + Logging
    - Logging Level
      * 5 - Debug
    - Log Output
      * To file
      * File Path
        + C:\Program Files\FileZilla Server\Logs\filezilla-server.log
      * File Rotation
        + Enabled
    - Maximum number of Log files
      * 15
    - Log Rotation Policy
      * Rotate log file when its size reaches the maximum size
    - Maximum file size
      * 100MB

### XAAMP

Resources:

* [How to setup Apache web server using XAMPP on Windows](https://www.linglom.com/administration/how-to-setup-apache-web-server-using-xampp-on-windows/)
* [Create Valid SSL in XAMPP Apache](https://stackoverflow.com/questions/64800565/how-to-create-valid-ssl-in-localhost-for-xampp)

#### Apache

* F

#### MySQL

* F

#### FileZilla

* Ports:
  + 21 for FTP
  + 14147 for internal FileZilla
* Connect to Server
  + Server Address
    - 127.0.0.1
  + Port
    - 14147
  + Administrator Password
    - Create Secure Admin Password
* Settings
  + General Settings
    - Connection Settings
      * Listen on these ports
        + 21
      * Max. number of users
        + 0
    - Performance settings
      * Depends on machine and server stress
    - Timeout settings
      * Connections timeout
        + 120
      * No Transfer timeout
        + 120
      * Login timeout
        + 120
  + Security Settings
    - Block incoming server-to-server transfers
      * Check box
    - Strict IP filter
      * Check box
    - Block outgoing server-to-server transfers
      * Check box
  + Miscellaneous
    - Don’t show passwords in message log
      * Check box
    - Allow downloading of files…
      * Check box
    - Ignore unroutable IPs on PORT…
      * Check box
  + Admin Interface settings
    - Ports on which the admin interface should listen
      * 14147
    - Change admin password
      * Assign a secure password
  + Logging
    - Enable logging to file
      * Check box
    - Limit log file size
      * Uncheck box
    - Logfile
      * Log all to ‘FileZilla Server.log’
  + GSS Settings
    - Enable Kerberos GSS support
      * Check box
    - Prompt for password if necessary
      * Check box
  + SSL/TLS settings
    - Enable FTP over SSL/TLS support
      * Check box
    - Generate new certificate and use information for
      * Private key file
      * Certificate file
      * Key password
    - Allow explicit FTP over TLS
      * Check box
    - Disallow plain unencrypted FTP
      * Check box
  + Autoban
    - Enable automatic bans
      * Check box
    - Ban IP address after 10 failed attempts within one hour
    - Ban for 24 or more hours
* Users
  + General
    - Add any users that should be there
    - Account Settings
      * Enable accounts
      * Password
        + Check box
        + Assign secure password
      * Group membership
        + ReadMe
      * Bypass userlimit of server
        + Uncheck box
      * Force SSL for user login
        + Check box
  + Shared Folders
    - Manage any shared folders (ReadMe)
      * Manage privileges of each user on the shared folders
      * Use principle of least privilege
  + Speed Limits
    - Can leave on defaults
  + IP Filter
    - Clear all boxes unless ReadMe states otherwise
* Groups
  + Use the same settings as Users

#### Mercury

* [Most of the Notes](https://www.c-sharpcorner.com/UploadFile/c8aa13/send-mail-on-local-host-via-mercury-with-xampp/)

Steps for Configuring Mercury

* Configuration
  + Manage local users
    - Delete the test user
    - Add new user for yourself
  + Aliases
    - Add new alias
      * Alias
        + <user>@localhost.com
      * Real Address
        + <user>@localhost
  + Mercury core module
    - Local domains
      * Add new domain
        + Local host or server

Localhost.com

* + - * + Internet name

Localhost

* + - * Add new domain
        + Local host or server

Localhost.com

* + - * + Internet name

[127.0.0.1]