**The Supreme Checklist**

By Michael Litrenta

This is the supreme checklist. I don’t know why it is called a checklist even though most of the time it is just a collection of notes. So in reality this is a collection of notes from various sources. Have fun reading.

My Achievements: 2nd States Platinum Junior Year. Being kicked off of LT right before Senior Year. Having my mentee be cracked (Counselman).

My Mission: To collect as many people’s checklists/Notes I can to amass here. I will create an amazing and supreme checklist that will have as much information as possible. Enjoy 🙃

People whose Note sheets I’ve used/have had access to: Ben Scholtes, Val Runge, Ben Fredrick/Connor Lockett, Aidan Sachs, Dimitri Kokkinakos, Spencer Davis

# **Checklist**

* ReadMe
  + Users
  + Critical Services
  + Applications
  + Anything else the scenario might want (ex. Make a user)
* Forensics
* dCode
* CyberChef
* Rumpkin
* Make a backup admin (Litrenta)
* File Explorer (view everything)
* Computer Management
  + Shares
  + Users
  + Services
* Browsers
* Applications
* Group Policy
  + Password Policy
  + Lockout Policy
  + Audit Policy
  + Security Options
  + User Rights Assignment
  + Administrator Templates - Computer
  + Administrator Templates - User
* Control Panel
  + Programs & Features
    - Programs
    - Features
  + Autoplay
  + Internet Options
  + User Access Control
  + Firewall
* Threat Hunting

# **Notes**

* ReadMe
  + Everything below is good, but ReadMe takes priority over everything. If the ReadMe says to do something, do it.

## File Explorer (view everything)

* + View
    - Option
      * View
        + Uncheck anything that hides
        + Check anything that shows
        + Check anything that show

## Computer Management

#### Users

* + - Groups
      * Administrators from ReadMe
      * Remove anyone that may be in a group unless told so by ReadMe
    - Users
      * Disable authorized user (anyone not in ReadMe)
      * Change password - This1s@G00dPass!
      * Check “User must change password at next logon”
        + Do after password
      * Uncheck everything else
      * Disable default administrator, guest, and any other default account.

#### Shares

* + - Default Shares
      * ADMIN$
      * C$
      * IPC$
    - Remove all other shares unless told so by ReadMe

#### Services

* + - Enable - Start and Automate
      * BITS
      * CCS Client (CyberPatriot Scoring Bot)
      * Diagnostic Policy Service
      * DNS Client
      * DHCP Client
      * IPsec Policy agent
      * Network list service
      * Network location awareness
      * Windows Defender Advanced Threat Protection
      * Windows Event Collector
      * Windows Firewall
      * Windows Installer
      * Windows Search
      * Windows Time
      * Windows Update
      * WMI
    - Disable - Stop and Disable
      * Fax
      * FTP
      * Geolocation
      * IP Helper
      * LDP Service
      * Microsoft FTP service
      * Net.TCP Port Sharing
      * Netlogon
      * Phone Service
      * Plug and Play
      * Print Spooler
      * Remote Access Connection Manager (RPC)
      * Remote Desktop Services (RPC)
      * Remote Registry (RPC)
      * Secondary Logon
      * SNMP Trap
      * SSDP Discovery
      * Smart Card
      * TCP/IP Net Bios Helper
      * Telephony
      * Telnet
      * Threat Vector
      * Web Client
      * WinHTTP Web Proxy Auto-Discovery Service
      * World Wide Web Publishing Service

## Group Policy

### Computer Configuration -> Windows Settings

* + - Startup/Shutdown Script - Delete All (find location and delete malicious file)

#### Security Policy

##### Password Policy

* + - * + Enforce password history - 5 passwords remembered
        + Maximum password age - 30 days
        + Minimum password age - 7 days
        + Password must meet complexity requirements - enabled
        + Store passwords using reversible encryption - disabled

##### Lockout Policy

* + - * + Account lockout duration - 30 minutes
        + Account lockout threshold - 5 invalid logon attempts
        + Reset account lockout counter after - 30 minute

##### Security Options

* + - * + [Benchmarks](https://docs.google.com/document/u/0/d/1gcf_8BFq3n2MkScxQdaSUoZ1eO9Ns8_eSGDVPzFxAmI/edit)

##### User Rights Assignment

* + - * + [Benchmarks](https://docs.google.com/document/u/0/d/1gcf_8BFq3n2MkScxQdaSUoZ1eO9Ns8_eSGDVPzFxAmI/edit)
        + No user should be named in anything
        + Use common sense/your brain
    - Administrator Templates
      * [Benchmarks](https://docs.google.com/document/u/0/d/1gcf_8BFq3n2MkScxQdaSUoZ1eO9Ns8_eSGDVPzFxAmI/edit)
      * Search by state makes things easier/shows you edited things

### User Configuration -> Windows Settings

* + - Logon/Logoff Script - Delete All (find location and delete malicious file)
    - Administrator Templates
      * [Benchmarks](https://docs.google.com/document/u/0/d/1gcf_8BFq3n2MkScxQdaSUoZ1eO9Ns8_eSGDVPzFxAmI/edit)
      * Search by state makes things easier/shows you edited things

## Control Panel

* + Programs & Features

#### Programs

* + - * Don’t Remove:
        + VMware
        + C++ Microsoft stuff
        + Java
        + ReadMe Application
        + ReadMe Browser
      * Remove all programs that are not on ReadMe (look them up first to see what they are)

#### Features

* + - * Remove all except
        + .Net 4.8 Framework
        + Work Folders Client

### Autoplay

* + - Ask me every time for all for everything

### Devices and Printers

* + - Remove all printers

### Internet Options

* + - Security
      * Set all to high
      * Enable Protected Mode
      * Remove all trusted sites
      * Local intranet & Trusted sites
        + Require server verification (https:) for all sites in this zone
    - Privacy
      * Settings
        + Remove all sites
        + Advanced

Cookies

Block both

No not allow session cookies

* + - * Location
        + Never allow websites to request your physical location
        + Clear sites
      * Pop-up Blocker
        + Turn on Pop-up Blocker
        + Settings

Remove all allowed sites

Blocking level: High

* + - Connections
      * LAN Settings
        + Uncheck “Automatically detect settings” (disabled WPAD)
    - Advanced
      * HTTP settings
        + Use HTTP2
        + Uncheck any others
      * Multimedia
        + Disable all but top 2
      * Security
        + Uncheck anything that has: allow
        + Check anything that has: check, block, enable

Enable Enhanced Protected Mode

If this is not enabled then the protected mode in the zones does not take effect.

* + - * + Send Do Not Track requests
        + Use TLS 1.2 (latest non-experimental version)
        + Use SSL 3.0
        + Check bottom 3 warns

### Firewall

* + - Turn on
    - Advanced
      * Domain
        + State

State: On

Inbound Connections: Block (default)

Outbound Connections: Allow (default)

* + - * + Settings

Display a notification: No

* + - * + Logging

Name: %SystemRoot%\System32\logfiles\firewall\privatefw.log

Size Limit: 16384

Log dropped packets: Yes

Log successful connections: Yes

* + - * Private
        + State

State: On

Inbound Connections: Block (default)

Outbound Connections: Allow (default)

* + - * + Settings

Display a notification: No

* + - * + Logging

Name: %SystemRoot%\System32\logfiles\firewall\privatefw.log

Size Limit: 16384

Log dropped packets: Yes

Log successful connections: Yes

* + - * Public
        + State

State: On

Inbound Connections: Block (default)

Outbound Connections: Allow (default)

* + - * + Settings

Display a notification: No

Apply local firewall rules: No

Apply local connection security rules: No

* + - * + Logging

Name: %SystemRoot%\System32\logfiles\firewall\publicfw.log

Size Limit: 16384

Log dropped packets: Yes

Log successful connections: Yes

### User Access Control

* + - Set to max/highest

### Network Sharing Center

* + - Change adapter settings -> the WIFI you are using properties
      * Uncheck:
        + Microsoft LLDP Protocol Driver
        + TCP/IPv6
        + Link-Layer Responder
        + Link-Layer Mapper I/O Driver
      * Check:
        + Top things with cool icons
        + TCP/IPv4

Properties

Set everything to automatic

General -> Advanced

WINS

Disable NetBIOS over TCP/IP

Enable LMHOSTS lookup

## Settings

### Power & Sleep

* + - When plugged in, turn off after: 15 minutes
    - When plugged in, PC goes to sleep after

### About

* + - System Info
      * Advanced System Settings
        + Performance

Settings

Data Execution Protocol

Turn on DEP for all

Remove all exceptions

Remote

Remote Assistance: disabled

Don’t allow remote desktop

ReadMe

### Devices

* + - Printers & Scanners
      * Remove all printers & disable everything that allow printers
    - Bluetooth
      * More bluetooth options
        + Allow Bluetooth devices to find this PC: disabled
        + Check hardware for connected bluetooth: disable
    - Autoplay
      * Use Autoplay for all media devices: disabled
      * “Ask me every time” for everything

### Network & Internet

* + - VPN
      * Disable all

### Update & Security

* + - Windows Update
      * Install Updates
      * Advanced Options
        + Automatic
        + Defender upgrades: enabled
    - Windows Defender
      * Real-Time Protection: enabled
      * Cloud-based Protection: enabled
      * Exclusions
        + Add an exclusion

Remove all exclusions

* + - Windows Security
      * App & Browser Control
        + System Settings

Force randomization for images: enabled

* + - * Memory Integrity: Enabled
      * Controlled folder access: enabled

## Firefox

* + Settings
    - General
      * Firefox Update
        + Automatically install updates

Update by downloading again (what I use)

* + - Privacy & Security
      * Browser Policy
        + Enhanced Tracking Protection: Strict
        + Send Websites a “Do Not Track” signal: Always
        + Login and Passwords: disabled all

Show alerts about passwords for breached websites: enabled

* + - * + Autofill addresses: disabled
        + Autofill credit card: disabled
      * Permissions
        + Block new requests for everything and remove all exceptions
        + Block pop-up windows: enabled
        + Warn you when websites try to install add-ons: enabled
      * Security
        + Deceptive Content and Dangerous Software Protection

Enabled all

* + - * + Certificates

Enabled

* + - * + HTTPS-Only Mode

enabled HTTPS-Only Mode in all windows

Remove exceptions

* + - * DNS over HTTPS
        + Max Protection

Cloudflare (default)

Remove all exceptions

## Threat hunting

* + Unauthorized Programs
    - Possible bad extensions
      * .mp3 | .mp4 | .jpg or jpeg | .png | .mov | .gif | .exe | .html or .htm | .mpeg | .pdf | .txt | .rtf | .vbs | .aspx | .bat | .cda | .avi | .rip | .rip | .ps1 | .wav | .psm1 | .car | .ntf | .c | .bmp | .py | .xlsx | .p12 | .pfx
    - Common Unauthorized applications
      * iTunes, TeamViewer, CCleaner, ophcrack, uTorrent, qBitTorrent, Npcap, Adware WebCompanion, Firefox addon Video DownloadHelper, NetBios Pro, Angry IP Scanner, Epic Games Launcher, K-Lite Codec Pack, Progress Telerik Fiddler Web Debugger, Teamspeak, Avernum, Abyss Web Server, Wireshark
  + Backdoors
    - Common Backdoors
      * Tini
      * Netcat
      * Perl owl-shell
    - How to find active open backdoors
      * Open command prompt as administrator
      * netstat -ano
      * Open task manager -> details
      * Compare PIDs
      * Look up any suspicious programs and IP addresses

# **Server Configurations**

* This is up to Server 2022

## IIS

* + How to get
    - Install IIS through features
  + How to make a self-signed HTTPS certificate
    - <Computer Name>
      * Server Certificate
        + Make a self-signed certificate

Name it whatever you want (I like HPPS - 1)

Personal

* + <Computer Name>
    - FTP
      * FTP Authentication
        + Anonymous Authentication: Disabled
        + Basic Authentication: Enabled
      * FTP Logging
        + One log file per: Site
        + Log file directory: C:\inetpup\logs\LogFiles
        + Encoding: UTF-8
        + Max file size (in bytes): 100000000
      * File Logon Attempt Restrictions
        + Enabled
        + Max number of failed logon attempts: 4-5
        + Time period: 21600
        + Deny IP addresses based on the number of failed logon attempts
      * FTP SSL Settings
        + SSL Certificate: Choose
    - IIS
      * Authentication
        + Anonymous Authentication: disabled
        + ASP.Net Impersonation: disabled
      * Default Document
        + Disable
      * Directory Browsing
        + Disable
      * Feature Delegation
      * 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

* + - * + Maximum file size (in bytes): 100000000
      * Request Filtering
        + Do not allow

.exe | .py | .java | .php | .psl | .js | .bat | .json

* + Application Pools
    - DefaultAppPool
      * Advanced Settings
        + Process Model

Identity

ApplicationPoolIdentity

* + Sites
    - Default Web Site
      * Change to 443
        + Create new Site Binding

Type: HTTPS

IP Address: All Unassigned

Host Name: whatever (HTTPS - 1)

SSL Certificate: self-signed (HTTPS - 1)

* + - * + Remove Port 80 bindings
      * SSL Settings
        + Require SSL
        + Client Certificates

Require

## FileZilla

* + Download FileZilla Server
  + Server Listeners
    - Addresses: 0.0.0.0 | :: | 127.0.0.1
    - Port: 21 | 1 (for 127.0.0.1)
    - Protocol: Require explicit FTP over TLS
  + Protocol Settings
    - Autoban
      * Ban IP addresses after: 5 failed login attempts
      * If they happen within: 3600 seconds
      * The ban will last: 21600 seconds
    - Timeout
      * Login timeout: 20 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 certifications
      * Use a self-signed X.509 certificate
      * Generate New
        + Distinguished name: *nothing*
        + Hostnames: localhost
  + 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
        + 14148
      * Password
        + Check box
        + Enter secure password
      * Connection Security
        + Minimum allowed TLS version: v1.3
  + 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 reach
      * Maximum file size
        + 100MB

## DNS

## AD DS

# **Miscellaneous Notes**

## Registry Keys

* + - Mostly every registry key has an HKLM & HKCU key with the same path
    - Can find pretty much any registry key on [Group Policy Search](https://gpsearch.azurewebsites.net/)
  + Run & RunOnce
    - HKLM:\Software\Microsoft\Windows\CurrentVersion\Run
    - HKLM:\Software\Microsoft\Windows\CurrentVersion\RunOnce
  + Right Click
    - HKLM:\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoViewContextMenu
    - HKLM:\ Local\_Machine\System\CurrentControlSet\Services
  + Services
    - HKLM\System\CurrentControlSet\Services

## Powershell/CMD

* + add/remove registry keys
    - New-Itemproperty -path -name -property -value -force
    - Remove-Itemproperty -path -name -property -value -force
  + Change attributes
    - Attrib [attribute wanted to add or remove (1 only at a time)] *filepath*

## Common Broken Items

* + Hosts file/Internet
  + netstat
    - How to see if it is broken: if a PID in netstat -ano is not in task manager details.
    - Go to netstat file location
  + Pretty much every other application
    - Regedit
      * Where? - Idk just look it up

## Ports

* + Simple TCP/IP
    - 7 - Echo
    - 9 - Discord
    - 13 - Daytime
    - 17 - Quote of the Day
    - 19 - Character Generator
  + 20/21 - FTP
  + 22 - SSH
  + 23 - Telnet
  + 25 - SMTP
  + 53 - DNS
  + 67/68 - DHCP
  + 69 - TFTP
  + 80 - HTTP
  + 81 – Apache
  + 88 – Kerberos
  + 110 – PoP3
  + 123 – NTP
  + 135 – RPC
  + 139 - NetBIOS
  + 443 – HTTPS
  + 445 – SMB/File Share
  + 990 - FTPS
  + 3306 - MySQL
  + 3389 – RPC
  + 5900 – VNC
  + 6667 – IRC
  + 8080 - Apache
  + 14148 - FileZilla
  + 25565 - Minecraft Java