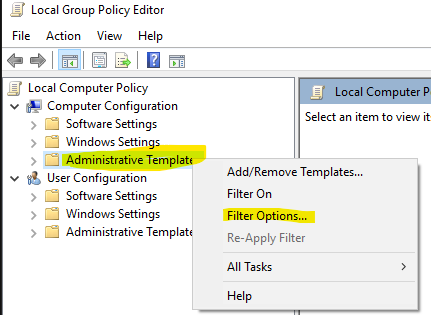
****

# **Wildcard CCDC Windows Checklist**

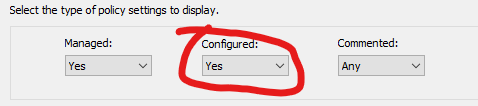
|  |
| --- |
| Key  * Anything in text like this is a command to be typed in cmd   + ping 8.8.8.8 * Anything in single quotes is a file or directory path   + ‘C:\Users\nmap.exe’ * Anything in double quotes is a line to be added to a file   + “securesetting = 1” * Anything in brackets is a run command(Windows Key + R)   + [lusrmgr.msc] * Anything in double quotes with pipe(s) and ends with a colon is a group policy path. The key is after the colon   + “Computer Configuration|Administrative Templates|Windows Components|Windows Update:Configure Automatic Updates” * If group policy [gpedit.msc] is mentioned anytime and Active Directory is a critical service, then do group policy settings inside of Domain Group Policy, NOT Local group policy |

**Pre-CCS**

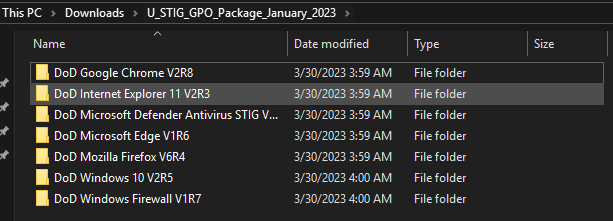
* Read the ReadMe
  + Please for the love of whatever you believe in just do it
  + Critical Services
  + Software
* Download necessary software
  + Everything
  + Sysinternals
  + Security compliance toolkit
    - LGPO
    - Current OS’s GPO Files (use [winver])
  + Malwarebytes
  + Shellbagsviewer
* Do forensics
* Check current policy configurations
  + Open [gpedit.msc], right click on “Administrative Templates” and select “Filter Options”.



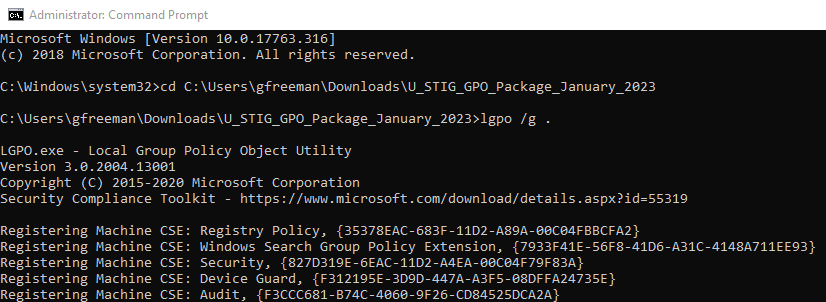
* + Set “Configured” to “Yes” and select “OK”



* + Search the configured Group policy settings and change any insecure ones
  + Do the same for “User Configuration”
* Apply DISA STIG LGPO’s
  + Download LGPO <https://www.microsoft.com/en-us/download/details.aspx?id=55319>
  + Download the DISA STIG Group Policy Objects <https://public.cyber.mil/stigs/gpo/>
  + Place LGPO.exe in C:\Windows\System32
  + Extract the STIGS
  + Delete all folders except:
    - Your OS (Windows 10, Server 2016, etc)
    - Windows Firewall
    - Firefox
    - Edge
    - Defender AV
    - IE 11
    - Google Chrome



* + then in an administrative command prompt, cd to the location of the folders
  + lgpo /g .



* Enable viewing of hidden and critical OS files by opening File Explorer, clicking View, selecting Options, Change Folder and Search Options, click View again, and enabling Hidden and protected file viewing
* Copy forensics and related files to desktop
* View Powershell**/**CMD history by opening said window and pressing up key to see past inputs
* Run shellbagsviewer and log any entries
  + https://privazer.com/en/download-shellbag-analyzer-shellbag-cleaner.php

**OS Updates**

* Start updates manually
  + If updates fail to start, check the following
    - Windows Update service might be disabled
    - Group policy
      * Computer Configuration|Administrative Templates|Windows Components|Windows Update might have automatic updates disabled or disallow automatic updates immediate installation
    - Registry
      * HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\wuauserv or HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\WindowsUpdate might have a key disabling updates or automatic updates
* Turn on automatic updates
  + Set service to auto
  + Change group policy to “Auto download and notify for install” with the option “install updates for other microsoft products”

**User auditing**

* Open [lusrmgr.msc] (or [dsa.msc] if a domain controller) and do the following:
  + Disable default Administrator and Guest accounts
  + Set all users to “Change password at next logon” and manually change passwords if no point gain occurs
  + Uncheck all user options boxes except for “must change password at next logon” ***but do not check this option on your account***
  + Disable all users not mentioned in the ReadMe
  + Check groups and ensure only users authorized to be in said groups are present, also add any necessary users who aren’t already in them, such as adding Administrators to DnsAdmins or removing a non-admin user from Enterprise Admins group
  + Re-enable any disabled authorized users
  + Add new account(s) or group(s) if mentioned in ReadMe
  + Ensure specific users are not members of other groups by themselves if not specifically mentioned in the ReadMe
  + If RDP is a critical service and permissions are not to be restricted to specific user groups, ensure all authorized users are included in the Remote Desktop Users group

**Local Policy**

* Open [secpol.msc] (or domain group policy in server manager for domain controllers) and do the following:
  + In Account Policy, do the following:
    - Enforce a password history of 5 passwords remembered
    - Set max password age to 90
    - Set min password age to 30
    - Set min password length to 10
    - Set password meets complexity requirements to enabled
    - Set store passwords using reversible encryption to disabled
    - Set an account lockout threshold of 5 invalid logons and allow the other two account lockout policies to default to 30 minutes
  + In Local Policy, set these permissions:

|  |  |
| --- | --- |
| Access Credential Manager as a trusted caller | Blank |
| Access this computer from the network | Administrators and Remote Desktop Users |
| Act as part of the operating system | Blank |
| Add workstations to domain | Blank or Administrators(DC only) |
| Adjust memory quotas for a process | Administrators, LOCAL SERVICE and NETWORK SERVICE |
| Allow log on locally | Administrators and Users |
| Allow log on through Remote Desktop Services | Administrators and Remote Desktop Users |
| Back up files and directories | Administrators |
| Bypass traverse checking | Everyone, Administrators, Users, LOCAL SERVICE, NETWORK SERVICE, Window Manager |
| Change the system time | Administrators and LOCAL SERVICE |
| Change the time zone | Administrators, Users and LOCAL SERVICE |
| Create a pagefile | Administrators |
| Create a token object | Blank |
| Create global objects | Administrators, SERVICE, LOCAL SERVICE and NETWORK SERVICE |
| Create permanent shared objects | Blank |
| Create symbolic links | Administrators |
| Debug programs | Blank |
| Deny access to this computer from the network | Guests group and Guest |
| Deny log on as a batch job | Blank (maybe Enterprise Admins group and Domain Admins group) |
| Deny log on as a service | Blank (maybe Enterprise Admins group and Domain Admins group) |
| Deny log on locally | Guests group and Guest(maybe Enterprise Admins group and Domain Admins group as well) |
| Deny log on through Remote Desktop Services | Everyone (Guests if Remote Desktop is being used) |
| Enable computer and user accounts to be trusted for delegation | Blank |
| Force shutdown from a remote system | Administrators |
| Generate security audits | LOCAL SERVICE and NETWORK SERVICE |
| Impersonate a client after authentication | Administrators, SERVICE, LOCAL SERVICE and NETWORK SERVICE |
| Increase a process working set | Administrators and LOCAL SERVICE |
| Increase scheduling priority | Administrators |
| Load and unload device drivers | Administrators |
| Lock pages in memory | Blank |
| Log on as a batch job | Administrators (maybe Blank) |
| Log on as a service | Blank |
| Manage auditing and security log | Administrators |
| Modify an object label | Blank |
| Modify firmware environment values | Administrators |
| Perform volume maintenance tasks | Administrators |
| Profile single process | Administrators |
| Profile system performance | Administrators and “NT Service\WdiServiceHost” |
| Remove computer from docking station | Administrators and Users |
| Replace a process level token | LOCAL SERVICE and NETWORK SERVICE |
| Restore files and directories | Administrators |
| Shut down the system | Administrators and Users |
| Synchronize directory service data | Blank |
| Take ownership of files or other objects | Administrators |

* + In Security options, set the following:

|  |  |
| --- | --- |
| Accounts: Administrator account status | Disabled |
| Accounts: Block Microsoft accounts | Users can’t add or log on with Microsoft accounts |
| Accounts: Guest account status | Disabled |
| Accounts: Limit local account use of blank passwords to console logon only | Enabled |
| Accounts: Rename administrator account | CoolDude |
| Accounts: Rename guest account | Dude |
| Audit: Audit the access of global system objects | Disabled |
| Audit: Audit the use of Backup and Restore privilege | Disabled |
| Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings | Disabled |
| Audit: Shut down system immediately if unable to log security audits | Enabled |
| DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax | (DO NOT MESS WITH) |
| DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax | (DO NOT MESS WITH) |
| Devices: Allow undock without having to log on | Disabled |
| Devices: Allowed to format and eject removable media | Administrators |
| Devices: Prevent users from installing printer drivers | Enabled |
| Devices: Restrict CD-ROM access to locally logged-on user only | Enabled |
| Devices: Restrict floppy access to locally logged-on user only | Enabled |
| Domain controller: Allow server operators to schedule tasks | Disabled |
| Domain controller: LDAP server signing requirements | Require signature |
| Domain controller: Refuse machine account password changes | Disabled |
| Domain member: Digitally encrypt or sign secure channel data (always) | Enabled |
| Domain member: Digitally encrypt secure channel data (when possible) | Enabled |
| Domain member: Digitally sign secure channel data (when possible) | Enabled |
| Domain member: Disable machine account password changes | Disabled |
| Domain member: Maximum machine account password age | 30 |
| Domain member: Require strong (Windows 2000 or later) session key | Enabled |
| Interactive logon: Display user information when the session is locked | User display name only |
| Interactive logon: Don't display last signed-in | Enabled |
| Interactive logon: Don't display username at sign-in | Disabled |
| Interactive logon: Do not require CTRL+ALT+DEL | Disabled |
| Interactive logon: Machine account lockout threshold | 5 |
| Interactive logon: Machine inactivity limit | 300 |
| Interactive logon: Message text for users attempting to log on | This computer is for authorized use only! |
| Interactive logon: Message title for users attempting to log on | WARNING! |
| Interactive logon: Number of previous logons to cache (in case domain controller is not available) | 2 |
| Interactive logon: Prompt user to change password before expiration | 14 |
| Interactive logon: Require Domain Controller authentication to unlock workstation | Enabled |
| Interactive logon: Require smart card | Disabled |
| Interactive logon: Smart card removal behaviour | No action |
| Microsoft network client: Digitally sign communications (always) | Enabled |
| Microsoft network client: Digitally sign communications (if server agrees) | Enabled |
| Microsoft network client: Send unencrypted password to third-party SMB servers | Disabled |
| Microsoft network server: Amount of idle time required before suspending session | 15 |
| Microsoft network server: Attempt S4U2Self to obtain claim information | Default |
| Microsoft network server: Disconnect clients when logon hours expire | Enabled |
| Microsoft network server: Server SPN target name validation level | Accept if provided by client |
| Network access: Allow anonymous SID/Name translation | Disabled |
| Network access: Do not allow anonymous enumeration of SAM accounts | Enabled |
| Network access: Do not allow anonymous enumeration of SAM accounts and shares | Enabled |
| Network access: Do not allow storage of passwords and credentials for network authentication | Enabled |
| Network access: Let Everyone permissions apply to anonymous users | Disabled |
| Network access: Named Pipes that can be accessed anonymously | Blank |
| Network access: Remotely accessible registry paths | Blank |
| Network access: Remotely accessible registry paths and subpaths | Blank |
| Network access: Restrict anonymous access to Named Pipes and Shares | Enabled |
| Network access: Restrict clients allowed to make remote calls to SAM | Allow Remote Access Administrators |
| Network access: Shares that can be accessed anonymously | Blank |
| Network access: 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 |
| Network security: Allow Local System NULL session fallback | Disabled |
| Network security: Allow PKU2U authentication requests to this computer to use online identities | Disabled |
| Network security: Configure encryption types allowed for Kerberos | AES128\_HMAC\_SHA1, AES256\_HMAC\_SHA1 and Future Encryption Types |
| Network security: Do not store LAN Manager hash value on next password change | Enabled |
| Network security: Force logoff when logon hours expire | Enabled |
| Network security: LAN Manager authentication level | Send NTLMv2 response only. Refuse LM & NTLM |
| Network security: LDAP client signing requirements | Require Signing |
| Network security: Minimum session security for NTLM SSP based (including secure RPC) clients | Both |
| Network security: Minimum session security for NTLM SSP based (including secure RPC) servers | Both |
| Network security: Restrict NTLM: Add remote server exceptions for NTLM authentication | Blank |
| Network security: Restrict NTLM: Add server exceptions in this domain | Blank |
| Network security: Restrict NTLM: Audit incoming NTLM traffic | Enable auditing for all accounts |
| Network security: Restrict NTLM: Audit NTLM authentication in this domain | Enable all |
| Network security: Restrict NTLM: Incoming NTLM traffic | Deny all accounts |
| Network security: Restrict NTLM: NTLM authentication in this domain | Deny All |
| Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers | Audit All |
| Recovery console: Allow automatic administrative logon | Disabled |
| Recovery console: Allow floppy copy and access to all drives and folders | Disabled |
| Shutdown: Allow system to be shut down without having to log on | Disabled |
| Shutdown: Clear virtual memory pagefile | Enabled |
| System cryptography: Force strong key protection for user keys stored on the computer | User must enter a password each time they use a key |
| System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing | Enabled |
| System objects: Require case insensitivity for non-Windows subsystems | Enabled |
| System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links) | Enabled |
| System settings: Optional subsystems | Blank |
| System settings: Use certificate rules on Windows executables for Software Restriction Policies | Enabled |
| User Account Control: Admin Approval Mode for the Built-in Administrator account | Enabled |
| User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop | Disabled |
| User Account Control: Behaviour of the elevation prompt for administrators in Admin Approval Mode | Prompt for credentials on the secure desktop |
| User Account Control: Behaviour of the elevation prompt for standard users | Prompt for credentials on the secure desktop |
| User Account Control: Detect application installations and prompt for elevation | Enabled |
| User Account Control: Only elevate executables that are signed and validated | Enabled |
| User Account Control: Only elevate UIAccess applications that are installed in secure locations | Enabled |
| User Account Control: Run all administrators in Admin Approval Mode | Enabled |
| User Account Control: Switch to the secure desktop when prompting for elevation | Enabled |
| User Account Control: Virtualize file and registry write failures to per-user locations | Enabled |

* + For audit policies, do the following
    - Select the “advanced audit policies” area and click + drag one category at a time to select all policies inside that section. Right-click on the selected policies, click properties, and check “define this policy setting”, “success”, and “failure” on, off, and on again so there is a check mark and not a box.
      * If you have not already, set the security option of “Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings” to “enabled”
    - Open [cmd.exe] and issue the command auditpol /set /category:\* /success:enable /failure:enable

**Group Policy**

* All of these **should** be done by LGPO, but incase not
* Open Group Policy [gpedit.msc] and do the following:
  + AutoPlay
    - To disable AutoPlay, go to Computer Configuration|Administrative Templates|Windows Components|AutoPlay Policies, and switch “turn off autoplay” to enabled
    - To disable AutoRun commands, stay in that portion and switch “Set the default behavior for AutoRun” to Enabled and change the dropdown panel to “Do not execute any AutoRun commands”
  + Screensaver
    - To enable screensaver, go to User Configuration|Administrative Templates|Control Panel|Personalization, and turn on “Enable Screen Saver”
    - To force password protection on screen saver, stay in that portion and switch “Password protect the screen saver” to enabled
  + Remote Desktop (if not critical service)
    - To require secure RPC connections, go to Computer Configuration|Administrative Templates|Windows Components|Remote Desktop Services|Remote Desktop Session Host|Security, and change “Require secure RPC communication” to enabled
    - To enable RDP TLS Connections, stay in that portion and change “Require use of specific…” to SSL
    - To enable RDP Network Level Authentication, stay in that portion and change “Require user authentication for remote connections by using Network Level Authentication” to enabled
    - To force a high level of encryption, stay in that portion and change “Set client connection encryption level” to High Level
    - To disable drive redirection, go to Computer Configuration|Administrative Templates|Windows Components|Remote Desktop Services|Remote Desktop Session Host|Device and Resource Redirection and turn “Do not allow drive redirection” to enabled
    - To disable PnP redirection, stay in that portion and change “Do not allow supported Plug and Play device redirection” to enabled
  + Admin Enumeration
    - To disable Administrative enumeration on elevation, go to Computer Configuration|Administrative Templates|Windows Components|Credential User Interface and change “Enumerate administrator accounts on elevation” to disabled
  + Early Launch Anti-Malware
    - To stop ELAM from initializing bad drivers, go to Computer Configuration|Administrative Templates|System|Early Launch Antimalware, enable “Boot-start Driver Initialization Policy”, and change the dropdown menu to “Good and unknown”

**Countermeasures**

* Windows Firewall
  + Open [services.msc] and ensure the service is running and automatic
  + Open Windows Security and turn on the firewall with default configs
  + Open the Windows Firewall application and change the action to block and notify
  + Open the Action Center and turn UAC notification levels to the max
* Antivirus
  + Windows Defender
    - Open [services.msc] and ensure the service is running and automatic (some related services like Advanced Threat Protection cannot be made automatic or run manually)
    - Open Windows Security and enable Virus & Threat Protection
    - Turn “check apps and files” to Block
    - Turn “SmartScreen for Microsoft Edge” to Block
    - Turn “SmartScreen for Microsoft Store apps” to Warn
    - Exploit protection
      * Turn all System settings to “On by default”
      * Remove all Program settings overrides
  + Malwarebytes
    - Run a quick scan

**Services**

* Blackviper safe service configuration documentation
  + <https://www.blackviper.com/service-configurations/black-vipers-windows-10-service-configurations/>
* Bad services, stop and disable:
  + Bluetooth Support
  + DNS Server (if not required)
  + FTP (if not required)
  + Geolocation
  + Infrared
  + KpyM Telnet
  + LPD Service
  + Mercury
  + Message Queuing
  + Microsoft FTP (if not required)
  + Microsoft ISNS
  + MultiPoint Service
  + Net. TCP sharing
  + Payments and NFC/SE Manager
  + PNRP Machine Name Publication
  + RCP Locator
  + RIP Listener
  + Remote Access Connection Manager Service
  + Remote Registry
  + RIP
  + Routing and Remote Access
  + SNMP Service
  + SNMP Trap
  + SSDP Discovery
  + Simple Mail Transfer Protocol (SMTP)
  + Simple TCP/IP
  + Support
  + Telephony
  + Telnet
  + UPnP Device Host
  + WebClient
  + World Wide Web Publishing Service (if IIS not required)
  + Xbox Live Auth Manager
  + Xbox Live Game Save
* Good services, enable and set automatic:
  + Before Enabling these, remember that services can be impersonated, and malicious services can masquerade as helpful ones. Ensure you enable the correct service and that its process is signed by Microsoft or another trusted source
  + Windows Update
  + Event Log
  + Adobe Acrobat Update
  + Windows Firewall
  + Windows Defender

**Application Updates**

* If any of the following applications are installed and specified as necessary in the ReadMe, update them using ninite.com and other sources when ninite can’t be used:
  + Acrobat Reader DC
  + FileZilla
  + FileZilla Client
  + Firefox
  + Foxit Reader
  + Geany
  + Gimp
  + IrfanView
  + Java JRE 8
  + Krita
  + LibreOffice
  + MobaXterm
  + Notepad++
  + PeaZip
  + PHP
  + Powershell
  + PuTTY
  + Thunderbird
  + Visual Studio Code
  + TortoiseHG
  + VLC
  + MailEnable
  + OpenCPN
* Update any other required software specified in the ReadMe using the most recent compatible manufacturer distribution
* Enable all software to automatically update that can

**Prohibited Software**

* Check for recently modified files in the Program Files, Program Files (x86), and ProgramData folders by opening them and selecting the portion of the top bar titled “Date modified”. The most recent are likely files added for competition, check through them thoroughly
* If any of the following software is installed and not required in the ReadMe, delete them:
  + Abyss Web Server
  + Adaware WebCompanion
  + Advanced Port Scanner
  + Angry Ip scanner
  + AnyDesk
  + Arcade Lines
  + Avernum
  + Beware IRC server
  + BitComet
  + BitTornado
  + BoomBox Radio Player
  + ButtonBeats Virtual Piano Black
  + BZFlag
  + CCleaner
  + Chicken Invaders
  + CleanMyPC
  + Deluge
  + DOSBox
  + Driver Booster
  + Driver Support
  + Epic Games Launcher
  + Etherium cryptominer Geth
  + Fake an Error program
  + Firefox addon Video DownloadHelper
  + Garden Planner
  + HTTP Explorer
  + Hashcat
  + Hash Suite
  + Home Web Server
  + Itunes
  + John the Ripper
  + K-Lite Codec Pack
  + KNCTR
  + Kodi
  + Lazersoft
  + MyCleanPC PC Optimizer
  + MySQL-G0ld
  + Ncrack
  + Nmap
  + Open TFTP Server
  + Ophcrack
  + osquery
  + Plex Media Server
  + Progress Telerik Fiddler Web Debugger
  + Rainbowcrack
  + Radmin server
  + Reimage Repair
  + SDR tools
  + SuperScan
  + TeamViewer
  + Tetris
  + TightVNC Server
  + Tiny Web Server
  + Tonido Server
  + TV 3L PC
  + uTorrent
  + Vega
  + VirtualDJ8
  + Vistumbler
  + WebDiscover browser
  + Wireshark
  + Zed attack proxy
* Remove all addons from Firefox
* Install Microsoft baseline Security Analyzer 2
* Any non-work related software and other clutter programs must be removed, so check all unrecognized programs online to see their function

**Prohibited Files**

* Typically, prohibited files will appear in the following locations:
  + User directories
    - Desktop
    - Downloads
    - Music
    - Documents
    - Non-default folders (“my tunes”, “friends”, etc.)
  + Web Hosting Directories (inetpub)
  + Required file shares and readme-mentioned directories
* Use everything to look through the following extensions for suspicious or unnecessary files:
  + MP3
  + MP4
  + OGG
  + ZIP
  + TAR
  + GZ
  + PS1
  + EXE
  + CSV
  + TXT
  + GIF
  + JPG
  + JPEG
  + MSI
  + PNG
  + WAV
  + BAT
  + PHP
* Check for the following software archives:
  + Shodan
  + Brutus
  + Cain and Abel
  + Hashcat
  + Nikto
  + Mimikatz
* Remove suspicious files following these conventions:
  + Dumps
  + Plaintext files not used by programs
  + Phishing email templates
  + A file named “phpinfo”
* Check for common indicators of intrusion, such as “password”, “list”, “credit card”, “hash”, “archive”, and so on
* Remove all non-work related files, such as comic books, music, videos, and images

**Malware Scanning**

* Tasks
  + Use AutoRuns from Sysinternals to see all tasks that begin at startup
* Backdoors
  + Process-based, you must kill the process before being able to delete its file
    - NC
      * Runs as nc.exe w/ command line args of a port number
    - Tini
      * Typically runs on port 7777
    - TX
    - ntbindshell
  + Sticky keys (and similar)
    - Mostly found in registry, can test for it by pressing shift 5 times
    - Usually, these are found at the location ‘HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\’ with the location of the program being abused as the final portion of the path, primarily including sethc.exe, Maginfy.exe, Narrator.exe, DisaplaySwitch.exe, AtBroker.exe, utilman.exe, and osk.exe.
    - If the registry key is removed and the backdoor remains, check to see if ‘C:\Windows\System32\sethc.exe’ is actually a cmd instance
  + Remote access, usually found in program files directories
    - WindowsRAT
    - NetBus
    - WinUserProfileManager
* Keyloggers, don’t tend to show up as programs so search for names using Everything
  + Actual Keylogger
  + Rvlkl (Revealer Keylogger)
  + Spyrix
* Script files
  + Mimikatz invocation
  + NTDS dump
* Web shells, found as files in IIS Manager or ‘C:\inetpub\wwwroot’
  + Simple ASPX
  + LT ASPX
* Other
  + TCP DLL
    - Loaded onto DNS Server
  + Alternate Data Streams
    - Typically indicated by a running process in procexp.exe with a colon at the end of the process name
    - Check for using the sysinternals command Streams -d C:\

**Application Security**

* Configure the following for Internet Explorer
  + To enable it, open Turn windows features on or off and select the checkbox next to Internet Explorer
  + Open Internet Explorer, press the gear in the top right and select “Internet options.”
    - Select the “Advanced” tab and scroll down to “Security” and check in the following settings if they are not already:
      * “Enable Windows Defender SmartScreen”
      * “Enable Enhanced Protection Mode”
      * Scroll down to the “Phishing Filter” and select the “Turn on automatic website checking” option.
    - Go back to the main “Internet options” tab and select the “security” tab.
      * Notice the “Enable Protected Mode” option and select it for the “security” tab and the three others.
      * Once that is completed, return to the “security” tab, select the internet and then the custom level.
      * Find the “Internet Zone: Initialize and script ActiveX controls not marked as safe for scripting” setting.
        + Make sure that it is disabled.
    - If you’re on server, open server manager and select “local server”. Move to “IE Enhanced Security Configuration” and click “on.”
* Firefox
  + Find Firefox’s install directory, tends to be either ‘C:/Program Files/Mozilla Firefox/’ or ‘C:/Program Files(x86)/Mozilla Firefox’
    - Create a file in the Mozilla Firefox folder called “mozilla.cfg” and add the following lines to it (including the comment at the top):

// mozilla.cfg

lockPref("browser.safebrosing.downloads.enabled", true);

lockPref("dom.disable\_open\_during\_load", true);

lockPref("xpinstall.whitelist.required", true);

lockPref("privacy.donottrackheader.enabled", true);

lockPref("browser.safebrowsing.downloads.remote.block\_potentially\_unwanted", true);

lockPref("browser.safebrowsing.downloads.remote.block\_uncommon", true);

lockPref("browser.safebrowsing.malware.enabled", true);

lockPref("browser.safebrowsing.phishing.enabled", true);

lockPref("browser.crashReports.unsubmittedCheck.autoSubmit2", false);

lockPref("browser.discovery.enabled", false);

lockPref("app.shield.optoutstudies.enabled", false);

lockPref("datareporting.healthreport.uploadEnabled", false);

lockPref(“dom.security.https\_only\_mode”, true);

* + - Move into the path “(current path)\defaults\pref” and create a file called “local-config.js” and add the following lines to it (including the comment at the top):

// local-settings.js

pref("general.config.filename", "mozilla.cfg");

pref("general.config.obscure\_value", 0);

* Chrome
  + Open “Google Chrome”, drop down the three dots and select settings.
  + Select “Security and Privacy” and open “Security.”
    - When there, select the “Enhanced protection” option.
    - After that, scroll down to the “Advanced” section and select the “Always use secure connections” option there.

* PHP
  + Download the following files and replace php.ini with it
    - https://github.com/danehrlich1/very-secure-php-ini
* SMB
  + To disable SMB 1.X, open “Turn Windows Features On or Off” and click the box next to SMB 1.0 until it’s off
  + To enable both Server Encryption and Digital signing, open an administrator powershell and issue the command Set-SmbServerConfiguration -RequireSecuritySignature $True -EnableSecuritySignature $True -EncryptData $True -Confirm:$false

**Critical Service Configuration**

(Only do these if the following services are critical)

* IIS
  + Open [inetmgr.exe]
  + Configure these in both the world configuration (clicking on the server on the top left) and the site (SERVER->Sites->YOURSITE)
    - Select Directory Browsing, and select “disable” on the right side
    - Select Error pages, “Edit Feature Settings” on the right side, and change it to “Detailed Errors for local requests and custom error pages for remote requests”
  + If you need to enable SSL with a self-signed certificate:
    - If they dont give you a self-signed certificate:
      * Navigate to the world configuration (your server) and select “Server Certificates”
      * Select “Create Self-Signed Certificate” on the right
      * Give it a name like “afa.com”
      * Select “Web Hosting” as the certificate store
    - Select your site and select “Bindings” on the right side
    - Add a binding with https
    - Select your Self signed certificate
  + Change App Pool Identity
    - Navigate to your application pools (SERVER-> Application Pools on the left side)
    - Select the app pool the site is running (probably “DefaultAppPool”)
    - Select on “Advanced Settings” on the right side
    - Ensure “Identity” is set to “ApplicationPoolIdentity” and not LocalSystem
* Windows Remote Desktop Group policy:
  + RDP connection encryption level - high
  + RDP network level authentication - enabled
  + Require secure RPC communication
  + RDP Security Layer - TLS/SSL
  + Do not allow COM port redirection - enabled
  + Do not allow drive redirection - enabled
  + Do not allow LPT port redirection - enabled
  + Do not allow supported Plug and Play device redirection - enabled
* DNS
  + Open [services.msc]
    - Set the DNS Server service to Automatic
    - Under recovery, make sure all failures are set to restart the service
  + Open [regedit]
    - HKEY\_LOCAL\_MACHINE\SYSTEM|CurrentControlSet|Services|DNS|Parameters|serverlevelplugindll
    - if there is a DLL file there. If there is, remove that registry key
  + Open [dnsmgmt.msc]
    - Right click on your server and select properties
      * In “Advanced”, check “Secure cache against pollution”
      * In event logging, select all events
    - Open Forward Lookup Zones
    - Right-click on the domain name (e.g. afa.com) and select Properties
      * under General change “Dynamic updates” to none
      * under Zone Transfers uncheck “Allow zone transfers”
    - Exit out of that menu again, right click on the domain name, and select DNSSEC-> sign the zone
      * sign using default settings
  + Open an admin powershell and type the command Set-ItemProperty -Path HKLM:\SYSTEM\CurrentControlSet\Services\DNS\Parameters -Name TcpReceivePacketSize -Type DWord -Value 0xFF00. This will create a workaround for the DNS vulnerability known as SIGRed
* Microsoft FTP
  + Open [inetmgr.exe]
    - Navigate to your site
    - Enable Logging
    - Check authentication, make sure its read-only
    - remove any unauthorized shares
* FileZilla
  + Remove unauthorized users
  + Enable Autoban
  + Enable SSL
  + Give admin interface a password
* Active Directory
  + Pain, suffering even
* MailEnable
  + Open mailEnable, right-click on “Messaging Manager”, select “Security”, click “Encrypt Passwords…”, create a key (AND write it down, the application is stupid and tells you not to).
  + If you already have a self-signed certificate from IIS, make a second one. If you don’t, then follow the IIS steps above to create an SSL certificate.
    - Open [certlm.msc] and move your unused certificate from “Web Hosting” to “Personal”
    - Open mailEnable’s application, click Servers, right-click your server, go to SSL, and select the certificate
    - Ensure the mailEnable accounts don’t have any unauthorized users. If there is one, delete it

**Other**

* Non-GPO Remote Desktop Config
  + Use [systempropertiesremote], select the “remote” tab, and do the following:
    - Uncheck “Allow Remote Assistance connections to this computer”
    - If RDP is not a critical service, click the radio button labeled “Don’t allow remote connections to this computer”
* Sharing (when not a critical service)
  + Deletion
    - The below options can also be done graphically with [fsmgmt.msc]
    - Open an administrator CMD window and run the command net share
      * If there is a share that is not mentioned in the ReadMe, SMB is not a critical service, AND Remote Desktop is not also a critical service, issue the command net share ExampleShareName /delete
      * If the C drive is shared, immediately delete the share for it
  + Permissions
    - For non-hidden shares, check the file permissions by right-clicking, selecting “properties”, “sharing”, and “share”. Ensure that only the proper users are allowed access and that those users are allowed only the permissions they need
    - For all shares, check the file permissions by opening an admin powershell and typing the command net share ExampleShareName. If there are users who shouldn’t have certain permissions use one of the following commands:
      * Change perms: Grant-SmbShareAccess -Name “ExShareName” -AccountName “UserToChangePermsFor” -AccessRight Read -Force
      * Remove perms: Revoke-SmbShareAccess -Name "ExShareName" -AccountName "UserToRemovePerms" -Force
      * If Active Directory is necessary, ensure the permissions on SYSVOL and NETLOGON are restricted to Users or Administrators, whichever is specified in the ReadMe
* DEP (if security center is not on current OS)
  + Open an administrator powershell and issue the command bcdedit.exe /set {current} nx alwayson
* IP Source Routing
  + To disable IP Source Routing, open [regedit] and go to HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters and change the value of DisableIPSourceRouting to 2
    - If the DisableIPSourceRouting key doesn’t exist, go to that path, right-click, select new, create a DWORD Value, rename it DisableIPSourceRouting, and change its value to 2