**Cyber Security Windows 10 Workstation and Server 2019 Hardening Guide**

Me when I open an image:

****

**README HAS EVERYTHING YOU WILL EVER NEED**

**MAKE A BACKUP ADMIN ACCOUNT (i've never done this lmao)(same)**

**BENCHMARKS IF ALL ELSE FAILS:** [**CIS Downloads (cisecurity.org)**](https://downloads.cisecurity.org/#/)

* **Windows Server 2019 Benchmark v2.0.0**
  + **Windows Server 2022 Benchmark v2.0.0**
* **Enterprise Benchmark v2.0 for workstation**
* **USE THIS FOR WORKSTATION (please)** [Benchmarks](https://docs.google.com/document/d/1Y845AGeSDppsmIWXk2swsoBGCjsIVHG1MjwLfZcah9E/edit#)
* **Gpsearch.azurewebsites.net**

**DO FORENSICS QUESTIONS FIRST PLEASE**

**EMPTY THE RECYCLE BIN**

**UPDATE ALL APPS THROUGH THE APP WEBSITE NOT THROUGH THE APP**

# secpol.msc

* **Passwords**
  + Password history: 5
  + Max age: 30 days
  + Min age: 7 days
  + 14 character password minimum length
  + Our password: **jhkbestCTL1234!**
  + Enable complexity
  + Disable reverse encryption
  + Account lockout:
    - 30 minutes
    - 5 invalid attempts
    - 30 again for the one under
* **Misc**
  + Local policies
    - Security Options
      * Ctrl+alt+delete: disable
      * Do not display last sign in: enable
      * Accounts: limit local account use of blank passwords: enabled
      * The rest of this shit is benchmarks, see the top for link
* **Audit policy**
  + Every option should be checked for audits
  + Everything should be **off** in the **advanced audit policy config**
    - Advanced audit policy config should not be touched unless it has been edited and you need to reset it (I just generally wouldn't touch this)
* **Windows defender firewall with Advanced Security**
  + For Domain, Private, and Public Profile
    - Firewall state: On
    - Inbound connections: Block
    - Outbound connections: Allow
    - Settings
      * Display a notification: no
      * Allow unicast response: yes
      * Size limit: 16,384 KB (bizarre)
      * Log dropped packets: yes
      * Log successful connections: yes
      * Logging name should just be the default after you uncheck the box

# Computer Management (compmgmt.msc)

* Come here to edit users (disable or add) and groups
* Password never expire should not be checked!
* Guest, admin, and defaultaccount should be disabled

# 

# Group policy

* gpedit.msc

- Weird ass remote desktop setting

-Computer Configuration

- Admin templates

- Windows components

- Remote desktop services

- Remote desktop session host

- Device and resource redirection

- Plug and play device redirection: enabled

- Computer config

- Windows settings

- Scripts

- Startup and shutdown should both be empty

- Security settings (same as secpol)

- Anything in here **WILL OVERRIDE ANYTHING IN SECPOL**

# Browsers

* **Firefox**
  + Go to privacy and security
  + Strict protection
  + Enable pop-up blocker
  + Automatic updates
  + All the way down
    - “Enable HTTPS-Only Mode in all windows” - **ON**
    - That new DNS over https setting should also be on
  + Under Cookies and Site Data
    - Manage exceptions
      * Any exceptions should be deleted
  + Check to make sure it is the latest version
    - Help
      * About firefox
        + What's new
  + **Thunderbird** (not a browser)
    - General
      * Updates
        + Allow thunderbird to automatically install updates
      * Privacy and Security
        + Don't allow remote content

No exceptions

* + - * + Don't remember websites and links
        + Don't accept cookies
        + Send a “Do Not Track” signal
        + No saved passwords
        + Don't allow thunderbird to send technical data or backlogged crash reports
        + Turn on scam detection
        + Turn on antivirus
        + Ask me every time for certificates
        + Turn on “Query OCSP responder…”

* **Chrome**
  + Update:
    - Help
      * About Google chrome
  + Settings
    - Privacy: use enhanced protection
    - Always use secure connections

# Control panel

* **System and Security**
  + **Security and Maintenance**
    - Turn on **all** under each tab
    - User account control settings:
      * Slider all the way up
  + **Windows Defender Firewall**
    - Both private and public/guest networks should have a green check
  + **Power options**
    - Change when the computer sleeps
      * Turn off the display
        + control15 minutes
      * Put the computer to sleep
        + 15 minutes
  + **System**
    - Allow remote access - don't allow **AND** unchecked top box
    - **IF** remote access should be on, make sure the box is checked at the **bottom**
* **Programs**
  + Uninstall any programs that **are not** listed in the **README**
    - Nmap, ccleaner, anything that claims to be “anti-virus” are things to look out for
  + ALWAYS CHECK IN FOLDERS AND RECYCLE BIN FOR FILES YOU HAVE “DELETED”
    - If something comes back, check task scheduler for a task that reinstalls it
  + **Turn windows features on or off**
    - **Turn off everything except:**
      * **.NET Framework 4.5 Advanced Series**
      * **Work folders client**
    - **EVEN POWERSHELL 2.0, TURN IT OFF (depends)**
* **Hardware and Sound**
  + Autoplay
    - Uncheck “use autoplay for all media and devices”
* **Network and Internet**
  + Internet options
    - Security
      * Turn the slider all the way up and check the box for all 4 settings
    - Advanced
      * Scroll down and enable “enhanced protection mode”
  + Network and Sharing Center
    - Click on the the thing next to “connections”, it should be blue and say ethernet0 or ethernet1
      * Properties
        + Turn off

"Microsoft Network Adapter Multiplexor Protocol"

* + - * + Turn off “Link-Layer Topology Discovery Mapper I/O Driver”
        + Turn off “Internet Protocol Version 6 (TCP/IPv6)” **UNLESS THE README SAYS TO KEEP IPv6 ON (should not happen but always check)**
        + Turn off “Link-Layer Topology Discovery Responder”
        + Turn off “Microsoft LLDP Protocol Driver”
      * Turn off NetBIOS over TCP/IP for IPv4
        + Click on IPv4 (make sure u dont turn it off)

Properties

Under general (first tab), “advanced…”

WINS (third tab)

Disable NetBIOS over TCP/IP

* + - Change advanced sharing settings
      * Guest or Public (current profile)
        + Both network discovery and file and printer sharing should be off

# Normal Computer Settings

* **System**
  + About
    - System info
      * Advanced settings
        + Performance advanced settings
        + Data execution prevention should be on **for all services**
        + Restart after doing this
* **Devices**
  + Auto-play
    - Turn it off
    - Set removable drive and memory card as “ask me every time”

# Windows Security Settings

* Can be found by typing it into the search bar
* **Virus and threat protection settings**
  + Manage Settings
    - Exclusions
      * Add or Remove Exclusions
        + Harmful file blockers, typically .exe, are located here
  + Ransomware protection
    - Turn on controlled folder access
* **App and browser control**
  + Turn on “reputation-based protection”
  + Exploit protection`
    - Validate heap integrity should be on, and everything else should have its default setting

# File explorer

* **Readme will have all info on what needs to be kept, everything else should go**
* Check for files inside all folders (downloads, documents, photos, videos)
  + Also check inside each individual user’s folders (see below on searching for files)
    - **The size of the user’s folder can indicate the presence of something**
  + **CHECK PROGRAM FILES**
* Under the “view” tab at the top
  + Check the “hidden items” box
  + Options
    - View
      * Hide empty drives, hide extensions for known file types, hide folder merge conflicts, and hide protected operating system files should all be **unchecked**
      * Everything that says “show….” should be checked
      * Do this before searching for files
    - Search
      * Include compressed files: checked
      * Always search file names and contents: don't check this unless you are desperate for points
* **User permissions for files**
* File explorer
  + Right click on the file
    - microsoft properties
      * Security tab
        + “Edit” button
* FTP folder properties
  + Whatever the folder is called will be in the readme, along with who should have what permissions
    - It's usually the “ftp users” group or something like that are the only people who should read + write privileges
* **File extensions**
* **Search “\*.extension”**
  + .aspx - ASP.NET Active Server Page
  + .bat - PC batch file
  + .cda - CD audio track
  + .exe - Executable program
  + .gif - GIF file
  + .htm or .html - Hypertext markup language page
  + .jpg or .jpeg - Joint Photographic Experts GRoup photo file
  + .mp3 - MPEG layer 3 audio
  + .mp4 - MPEG layer 4 video
  + .mpeg - Moving Pictures Experts Group movie file
  + .pdf - Portable Document Format file
  + .png - Portable Network Graphics file
  + .rtf - Rich Text Format file
  + .txt - Unformatted text file
  + .vbs - VBScript
  + .bmp - Windows bitmap file
  + .ini - config files
  + .msi - windows installer
* **File attributes**
  + The powershell command “attrib” will list all files and their attributes in whatever directory you are in
  + The attrib command can also be used to add and remove
* **Good websites to use for ciphers and decoding**
  + Cyber Chef
  + **dCode**
  + VirusTotal

# Services

* Services.msc
* **Started and automatic startup type**
  + Windows defender advanced threat protection (Windows Defender ATP)
  + Start BITS (Background Intelligent Transfer Service)
    - Updates will not work if this is off
  + DNS Client: No web-browser will work if this is not on
    - Check “hosts” file if web-browsers are redirecting to somewhere else
      * Hosts file is in C:\Windows\System32\drivers\etc
      * Port 53
  + CCS Client: cyber patriot score bot **THIS CANNOT BE TURNED OFF**
  + Windows Event Collector
  + Windows Event Log
  + Windows Installer
  + Windows Time
    - Port 123
  + Windows Update
  + Windows Installer
  + Windows Search
  + DHCP Client
    - Port 68 (client) and port 67 is DHCP server
  + Windows Management Installer
  + Diagnostic service host and policy host
  + IP sec Policy agent (“PolicyAgent”)
    - Builds tunnels with the internet (encrypted traffic)
  + WMI Performance Adapter (“wmiApSrv”)
* **Misc services to stop and disable**
  + **Kill command in powershell: stop-service -name “servicename”**
  + Remote Registry
  + Plug and play
  + Print Spooler (readme)
  + Telnet
    - Port 23 or 3389 (RDP)
    - Two way communication between two computers on a local network
  + Remote desktop services (check readme)
  + WebClient
    - Allows windows apps to access the internet
  + World Wide Web Publishing Service
    - Needed for iis (readme)
  + Smart Card
  + IP Helper (“iphlpsvc”)
  + Telephony (“TapiSrv”)
    - Allows networks onto your local
  + TCP/IP netBios Helper
    - Allows users to share files and log onto the network and print
  + Simple TCP/IP Services (“simptcp”)
    - Port 7 is Echo
    - Port 13 is Daytime
    - Port 17 is QOTD (quote of the day)
    - Port 19 Character Generator
    - Port 9 is Discardfs.msc
  + Geolocation (“lfsvc”)
  + Phone service
  + SMNP trap (“SNMPTRAP”)
    - Can transport events on the computer on an outward connection
  + Fax (“fax”)
  + Net TCP Port Sharing
  + Netlogon
  + Secondary logon
    - Admins can log onto the computer on a non-admin account
  + Infrared monitor service
  + SSDP Discovery (“SSDPSRV”)
    - Outgoing and incoming connections that look for networks with plug and play
    - Port 1900
  + Windows remote management

# Shared folders

* **Fsmgmt.msc**
* **Can also be accessed through computer management**
  + Shares
    - Unshare everything **without a $ sign UNLESS readme says so**
    - **ADMIN$, IPC$, C$** are the default shares and **should not be unshared**
* <http://woshub.com/enable-remote-access-to-admin-shares-in-workgroup/> has good information about shares, use if stuck

# Registry Editor

* **Regedit**
* Microsoft-Windows-Settings-System-Programs-(location if task manager is disabled)
* Path for security options keys:
* HKEY-LOCAL-MACHINE
  1. Software
     + Microsoft
       - Windows
         * Current version

Policies

System

* The “H” in HKEY means hive
* Run and RunOnce will run specified files, can be a common forensics questions in later rounds
  1. Location:HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
  2. HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
* AutoAdminLogon should be set to “0”
  + Location: HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
* If a service cannot start and is giving errors, check this path
* HKEY\_LOCAL\_MACHINE\System\Currentcontrolset\services
* XFNtservice.\msc should have full control to all service keys
* These keys are also where the call path of services can be edited, which will give errors when starting a service.

# Threat Hunting

* “netstat -ano” in command prompt or powershell
  + Lists things running on open ports
  + **IMPORTANT:** using “netstat -anob” will also list the .exe that is responsible for opening the ports
* Port is the number after the colon under the local address tab
  + Cross check the PIDs of any suspicious connections on unwanted ports with things running in task manager
  + For ports, see [services](#_sv3leoet44p2) and [ports stuff](#soz7y1r69leg)
* Open Task Manager
  + Click Details
  + Open the file location and delete it

# Performance monitor (mid)

* Network
  + Listening ports
    - Backdoor ports and other unwanted outgoing/incoming connections can usually be seen here
      * Cross check these ports with services and executables running in task manager

# Md5 and other hashes

* Extremely common for forensics questions
* Command prompt or powershell command: “**certutil -hashfile <file name and extension> MD5**”: can be used **AFTER** CD’ING INTO THE DIRECTORY OF THE DESIRED FILE
* The “certutil -hashfile” command can be used for multiple types of hashes (md5, md4, sha, etc) look up the exact command on google

# Task manager

* Check through the executables running for any suspicious services
* Google names of running services to see it they are official Microsoft services
* End the task of anything that is suspicious, and go to the file location and delete the .exe
* Check the **startup** tab

# FOR SERVER

* Turn on iis in server manager IF THE README CALLS FOR IT
* [**Scholtes notes**](#_bwro1ok2fp67) **have amazing iis stuff**
  + **ApplicationPoolIdentity thing under application pools**
* All of the settings that follow should only be applied **IF** the readme wants iis to be on
  + Manage
    - Add roles and features
      * Role based
      * Check off “iis hostable web core” in features
  + Tools
    - iis manager
      * Default document
        + Move index.html OR whatever file the readme calls for to be at the top of the list
        + File you want on the top MUST BE in C:\inetpub\wwwroot or it will not show up in the default document list
      * Double click on “directory browsing” and turn it off
      * Server certificates:
        + Right click and click “create self-signed certificate”
        + Name it whatever and its personal
      * Right click on site name
        + “Edit Bindings”

Can see what port the site is on

Click add and add the self-signed certificate you just created

Remove the port 80 one

* Webshell attacks always use .aspx file types
* You can force start windows defender using a powershell command: (**start-windowsdefender**)
* Normal users should not be able to take ownership of files(in user properties)
* Printers
  + Printers and Devices
  + Lpd services in server manager
* **Active Directory(AD)**
  + For install:
    - Add tools and features
      * Active Directory Domain Services
      * Add all the features with it
  + If need to promote
    - Click the flag and click promote
      * Add a new forest
        + Lockett.com or what it says in the README
* Add a password
* Turn off the thing in DNS Options
* Next to the end
* Deal with any Prereqs
* Install than restart
* Open AD Users and Computers  
   -Lockett.com or name of domain
  + - Computers
      * Right click and New
        + Group

Add name

Keep global

Choose other thing

* Users
  + Add any users and do that stuff
  + Add them to groups

Website name-> DNS converts to IP(sevice) -> Local PC(C:\windows\system32\drivers\etc Hosts) ->ipconfig /flushdns

# DNS over HTTPS(DoH)

Windows Settings>Network & Internet>Ethernet>Select Network>DNS settings>Edit>Manual>Preferred DNS>Encrypted only

On Port 443

# 

# SMB Encryption

Set-SmbServerConfiguration –EncryptData $true for entire file server

Set-SmbShare –Name <sharename> -EncryptData $true for individual file share

Run these in PS with elevated session

# Common Vulnerabilities and Exploits (CVE)

* <https://www.cve.org>
* A database of known vulnerabilities and exploits within applications and operating systems
* Possibly used for forensics questions

# THE SCRIPT (its ass) (not really)

<https://docs.google.com/document/d/1ZGgtR3wPH1VzKI-Eh-ZPNUfgsmgRwlTDX-RWlYVzzyk/edit>

Use the baseline tools at the bottom AT THE BEGINNING of the round to record initial netstat and processes running

# **Ports stuff**

**FTP**

Ports 20/21

Control panel

Network and internet

Internet options

Advance

**IIS**

Port 80 = http

Port 443 = https

**Telnet**

Can connect wirelessly and type commands

Uses transmission control protocol and internet protocol

Not encoded

Disable

-Rules(limits)

-Expectations

TCP. IP

-Transport. Address

Control Host

Protocol

**RDP**

Remote desktop protocol

Port 3389

In services

**SSDP**

Port 1900

Turn off

Prone to Ddos

**DNS**

Port 53

88: Kerberos (server)

25: SMTP

22: SSH

81: Apache Management

445: SMB

1306/3306: MySQL

67/68: DHCP

139: netBios

5800/5900: VNC

389: LDAP

636: LDAPS

**Scholtes Approved**

# FileZilla Server

* Follow all default settings when first installing
* After installing, go to server -> configure
  + **Server listeners**
    - Add 127.0.0.1 on port 21 with protocol “Explicit FTP over TLS and insecure plain FTP”
  + **Protocols settings**
    - Autoban
      * Ban IP address after **5 failed login attempts**
      * If they happen within **10 seconds**
      * The ban will last **300 seconds**
    - FTP and FTP over TLS (FTPS)
      * Minimum allowed TLS version should be **1.3**
      * TLS certificate
        + Use a **self signed X.509 certificate**
        + Click “generate new”
        + Use “**localhost**” as the hostnames and don't put a distinguished name
  + Administration
    - Connection
      * Should be password secured
      * Default local listening port is **14148**
    - Connection security:
      * Minimum allowed TLS version should be **1.3**
      * TLS certificate
        + Use a **self signed X.509 certificate**
        + Click “generate new”
        + Use “**localhost**” as the hostnames and don't put a distinguished name
* **Logging**
  + Logging level: **5**
  + Enable file rotation
  + Max size for log files
  + Default path for the log file is: C:\Program Files\FileZilla Server\Logs\filezilla-server.log

# XAMPP

* X: means its cross platform, can be used on windows, linux, macos, etc
* A: Apache, which is a open source version of IIS
* M: MySQL, contains SQL server and database, can also be MariaDB or Mercury
* PP: PHP and Perl, which are programming languages
* Apps that you can add:
  + [FileZilla](#_8njli6cv50s6)
  + Mercury- mail server
  + Tomcat- Java thing
  + Webalizer- web analytics
  + OpenSSL - HTTPS certificates

**SEARCHING**

* Search the website + "what you are looking for in the website"
  + This will control f for entire site, useful for STIG

# More notes

* [Scholtes scroll](https://docs.google.com/document/u/0/d/1Qhwc76qSXC_6OEHzhWtrpekgQjEWQcKyfZPW5b_GfA8/edit)
* [Dimitri](https://docs.google.com/document/d/16QJlF16AgeExsNIIxniSRAbI4mM4CtkdIvJX9jPH0nA/edit)
* [Litrenta](https://docs.google.com/document/d/1NK6v_rh6Dlq5yT60Kn6JisSyXNLCYWV6sq5weNmWeYQ/edit?usp=sharing)