Checklist

1. Change Password
2. Setup Firewall **(see Firewall config sheet)**
3. Disable unknown users, guest account.
    a. Admin Tools
    b. Users and computers
    c. Users
    d. Look for users OUTSIIDE of the scoring users group, disable.
4. Set UAC to the highest setting
5. Check windows updates
6. Check Task scheduler, follow path for more clues before removing
    a. Start
    b. Administrative tools
    c. Task Scheduler
7. Disable services RDP in services
    a. Server Manager
    b. Local Server
    c. Remote Desktop disabled (Don't allow connections)
8. Sheck for startup files
    a. Open RUN
    b. Shell:startup
    c. Msconfig
    d. Follow to home directory for clues
9. Check event logs
10. Password Policy **(See Policy config sheet)**
11. Set Banners **(See policy config sheet)**
12. System hardening **(see hardening sheet)**
13. Splunk **(see splunk config sheet**

Firewall Config

(already in PS1 script)

1. Disable all firewall rules

netsh advfirewall firewall delete rule name= “all”

2. Enable Firewall

Netsh advfirewall set currentprofile state on

3. Turn on all profiles

Netsh advfirewall set all profiles state on

4. Set default policy to block all traffic

Netsh advfirewall set allprofiles firewallpolicy "blockinbound,blockoutbound"

Rules (do in PowerShell, or make rules in firewall gui:

TCP IN

Netsh advfirewall firewall add rule name="Allow Inbound TCP" protocol=TCP dir=in localport="25,53,80,110,143,389,443,587,636,993,995,9997" action=allow

TCP OUT

Netsh advfirewall firewall add rule name="Allow Outbound TCP" protocol=TCP dir=out localport="53,80,443,8080" action=allow

UDP IN

Netsh advfirewall firewall add rule name="Allow Inbound UCP" protocol=UDP dir=in localport="53,80,123,443" action=allow

UDP OUT

Netsh advfirewall firewall add rule name="Allow Outbound UDP" protocol=UDP dir=out localport="25,53,80,123,138,389,443" action=allow

ICMP (PING) IN

Netsh advfirewall firewall add rule name="icmp in" protocol=”icmpv4:8,any” dir=in action=allow

ICMP (PING) OUT

Netsh advfirewall firewall add rule name="icmp out" protocol=”icmpv4:8,any” dir=out action=allow

UPSTREAM DNS – may not be needed

Netsh advfirewall firewall add rule profile=any name="Upstream DNS" protocol=UDP dir=out action=allow

Firewall Logging:

Netsh advfirewall set allprofiles logging allowedconnections enable

Netsh advfirewall set allprofiles logging filename "C:\Usefilenamers\Administrator\Desktop\pfirewall.log"

policy config sheet

How to access?

- **Group policy management**
- **Default domain policy, right click, edit**
- **Computer Configuration**
- **Policies**

Change password Policy

- **Security Settings**
- **Account policies**
- 24 passwords remembered
- Max password age: 42 Days
- Min password age: 1 Day
- Min password length: 12 Chars
- Password must meet complexity: Enabled
- Store Password Using Reversible: Disable

Lockout policy

- Duration 99999
- Threshold 5

Banner Messages

- **Local policy**
- **Security Options**
- Interactive Logon: Message text for users attempting to log on
- Interactive logon: Message Title for users attempting to log on

UAC

- User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode
- User Account Control: Behavior of the elevation prompt for standard users
- **Set both to “prompt for credentials”**
- User Account Control: Use Admin Approval Mode for the built-in Administrator account **↑Set to enable ↑**

Security hardening sheet

PowerShell Commands:

Set-ExecutionPolicy Restricted

Disable-PSRemoting -Force

Set-Item WSMan:\localhost\Shell\MaxMemoryPerShellMB 0

Disable unused procedures with CMD: (already in PS1 script)

dism /online /disable-feature /featurename:Printing-Server-Role

dism /online /disable-feature /featurename:IIS-WebServer

dism /online /disable-feature /featurename:IIS-FTPServer

dism /online /disable-feature /featurename:IIS-WebServerManagementTools

dism /online /disable-feature /featurename:IIS-ManagementScriptingTools

dism /online /disable-feature /featurename:IIS-IIS6ManagementCompatibility

dism /online /disable-feature /featurename:IIS-Metabase

dism /online /disable-feature /featurename:IIS-ManagementConsole

Disable-NetAdapterBinding -Name "*Teredo*" -ComponentID ms_tcpip6

Malware / exploit detection

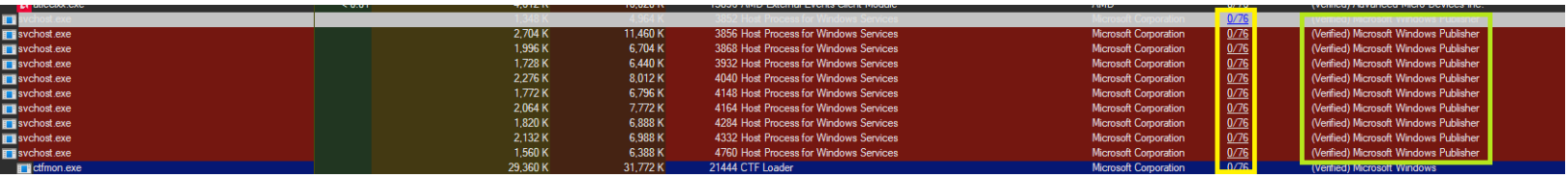
Software to install

- **Install process explorer** (from Microsoft, view processes in depth)
- **Install TCPView** (from Microsoft, lets you view listening ports / programs)
- **Install Autoruns** (from Microsoft, lets you view auto run tasks / programs)
- **↑Install all by going to Sysinternals.com ↑**
- **Install antimalware** (Malwarebytes etc..)
- All this software can be found via google

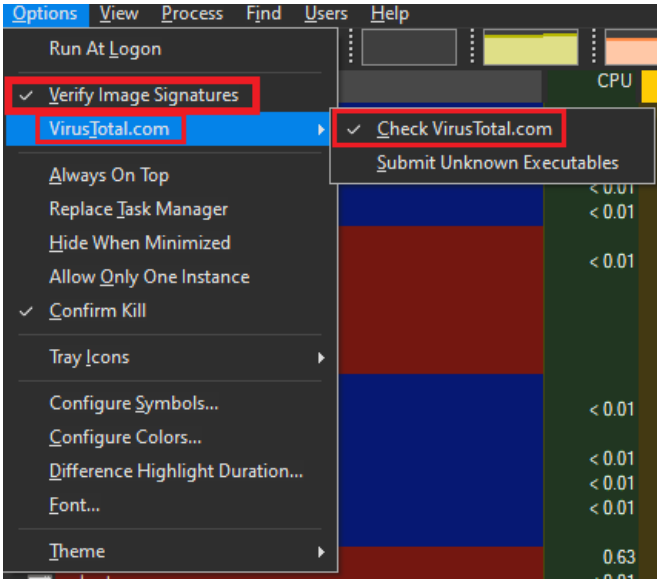
- Use CMD to run **netstat-anob** to look for listening services
- Look through server features, disable anything IIS and SMB1 related
- Look through services
- Check task scheduler again
- Look at event viewer
- Look for shared drives / folders
- Check common folders
    - C:\Windows\System32
    - C:\Users\<Username>\AppData
    - C:\ProgramData
    - C:\Windows\Temp or C:\Users\<Username>\AppData\Local\Temp
    - C:\Users\<Username>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
    - C:\Windows
    - C:\Users\Public
    - Downloads
    - C:\Program Files and C:\Program Files (x86)
    - Users folder

  Check cert of svchost

Useful information to look for in process explorer



- We can see that this svchost program is legitimate because it does not have any alerts in Viras Total (in yellow)
- The verified publisher is Microsoft (in green)



Go to options to enable this

Auto hotkey

Download auto hotkey, use the code bellow to paste to VM

Get from “tcc-ccdc/windows-scripts/sendClipboard.ah” OR use this code

; Alt + v

```
!v::
  SendRaw %clipboard%
```