NECCDC 2019
Champlain College

Operating System Hardening

Windows 10

Note: Don't forget about Windows Defender Firewall.

Initial Steps -

- Change your account password and update your security questions
- Remove unnecessary user accounts
- Ensure only one account has administrator access (Create a new Admin)
- Update Windows
- Change User Access Control (UAC) to highest level
- Install NXLog, Sysinternals Suite, and Microsoft Security Compliance Toolkit (SCT)
- Check for running and startup processes using Sysinternal Suite's Autoruns tool

Quick Commands -

Accounts -

Passwords Do Not Expire: `Get-ADUser -Filter 'useraccountcontrol -band 65536' -Properties useraccountcontrol`

No Password Requirement: `Get-ADUser -Filter 'useraccountcontrol -band 32' -Properties useraccountcontrol`

Passwords Stored in Reversibly Encrypted Format: `Get-ADUser -Filter 'useraccountcontrol -band 128' -Properties useraccountcontrol`

No Pre-Authentication: `Get-ADUser -Filter 'useraccountcontrol -band 4194304' -Properties useraccountcontrol`

DES Encrypted Credentials: `Get-ADUser -Filter 'useraccountcontrol -band 2097152' -Properties useraccountcontrol`

Disable Features -

Disable Task Scheduler: `Set-ItemProperty HKLM:\SYSTEM\CurrentControlSet\Services\Schedule -Name Start -Value 4`

Disable remote PowerShell: `Disable-PSRemoting -Force`

Miscellaneous -

List All Users in Admin Group: `net localgroup administrators`

Network -

Check for Listening Services: `netstat -naob`

Check for Open Ports: `netstat -plntu`

Outside Connections -

Show Shared Folders: `net view \\127.0.0.1\` OR `net view /all`

List Open Sessions: `net use`

Persistence -

List AutoRuns: **`net start`**
List Scheduled Tasks: **`schtasks`**
List Services: **`sc query`** OR **`Get-Service | Where-Object {$_.status -eq “running”}`**
List Startup Tasks: **`wmic startup list full`**
Kill & List Tasks: **`tasklist & taskkill /P <PID> /F`**

Sysinternals Suite -

Autoruns: AutoRuns

- GatherNetworkInfo.vbs is OKAY (part of Autoruns)
- Right-Click → Search Online
- Right-Click → Check VirusTotal
- Check last modified date of files in System32 (very recent times = bad file)
- Colors:
    - Pink: No publisher information was found
    - Green: New item
    - Yellow: Startup entry is there but the file/job is not

Portmon: Monitor Port Activity

Process Explorer: View Running Processes

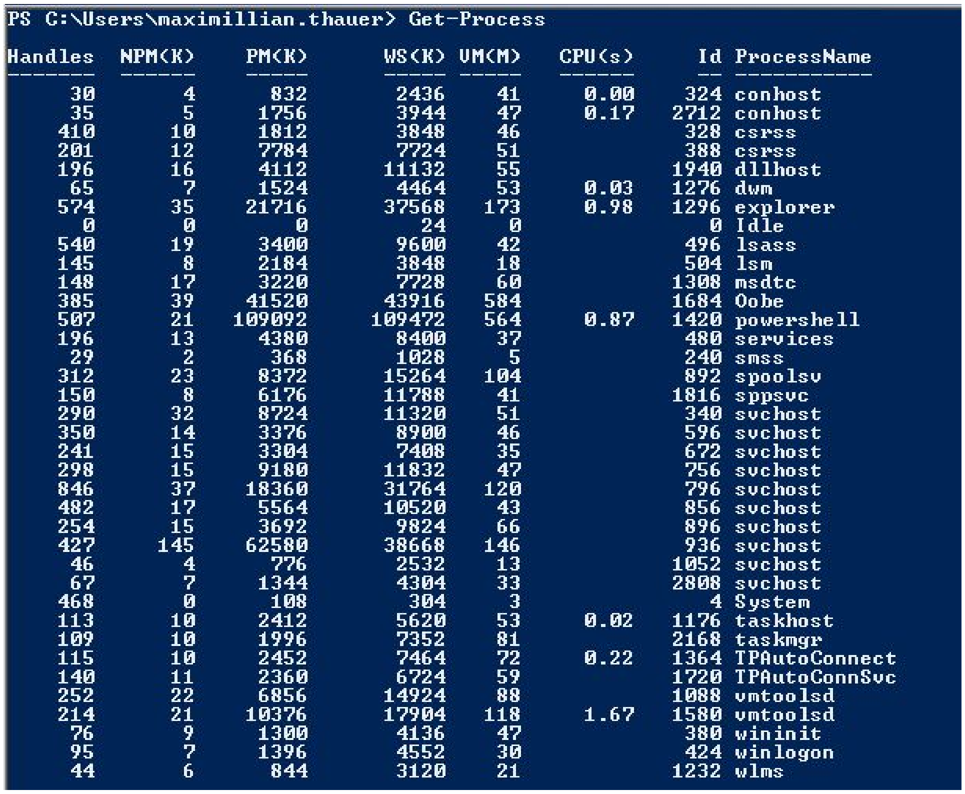
- Add the following columns: Autostart location, Virus Total, Users
- Options: Verify file signatures, replace task manager

Rootkit Revealer: Check for Rootkit(s)

TCPView: View TCP/UDP Endpoints

Expectations -

Processes running on a fresh install of Windows Server 2008 R2:



```
PS C:\Users\maximillian.thauer> Get-Process

Handles  NPM(K)    PM(K)      WS(K) VM(M)   CPU(s)     Id ProcessName
-------  ------    -----      ----- -----   ------     -- -----------
     30       4      832       2436    41     0.00    324 conhost
     35       5     1756       3944    47     0.17   2712 conhost
    410      10     1812       3848    46             328 csrss
    201      12     7784       7724    51             388 csrss
    196      16     4112      11132    55            1940 dllhost
     65       7     1524       4464    53     0.03   1276 dwm
    574      35    21716      37568   173     0.98   1296 explorer
      0       0        0         24     0               0 Idle
    540      19     3400       9600    42             496 lsass
    145       8     2184       3848    18             504 lsm
    148      17     3220       7728    60            1308 msdtc
    385      39    41520      43916   584            1684 Oobe
    507      21   109092     109472   564     0.87   1420 powershell
    196      13     4380       8400    37             480 services
     29       2      368       1028     5             240 smss
    312      23     8372      15264   104             892 spoolsv
    150       8     6176      11788    41            1816 sppsvc
    290      32     8724      11320    51             340 svchost
    350      14     3376       8900    46             596 svchost
    241      15     3304       7408    35             672 svchost
    298      15     9180      11832    47             756 svchost
    846      37    18360      31764   120             796 svchost
    482      17     5564      10520    43             856 svchost
    254      15     3692       9824    66             896 svchost
    427     145    62580      38668   146             936 svchost
     46       4      776       2532    13            1052 svchost
     67       7     1344       4304    33            2808 svchost
    468       0      108        304     3               4 System
    113      10     2412       5620    53     0.02   1176 taskhost
    109      10     1996       7352    81            2168 taskmgr
    115      10     2452       7464    72     0.22   1364 TPAutoConnect
    140      11     2360       6724    59            1720 TPAutoConnSvc
    252      22     6856      14924    88            1088 vmtoolsd
    214      21    10376      17904   118     1.67   1580 vmtoolsd
     76       9     1300       4136    47             380 wininit
     95       7     1396       4552    30             424 winlogon
     44       6      844       3120    21            1232 wlms
```

Adapter Settings -

- Disable Client for Microsoft Networks
- Disable File and Printer Sharing for Microsoft
- Disable Inter Protocol Version 6
- Disable Link Layer Topology Discovery Mapper IO Driver
- Disable Link Layer Topology Discovery Responder
- Disable QoS Packet Scheduler

Boot Processes -

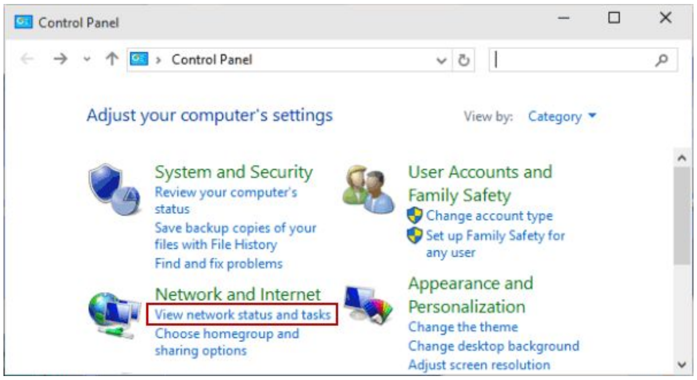
1. Enter System Configuration: `msconfig.exe`
2. Services Tab: Hide all Microsoft services; Disable unnecessary features
3. Startup Tab: Disable non-critical services

Credential Guard -

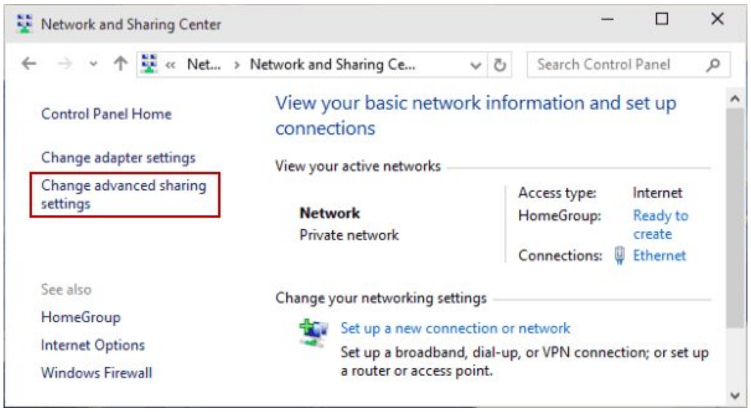
Device Guard -

File Sharing (Disable) -

1. Open Control Panel.
2. Choose “View network status and tasks” under “Network and Internet”.


Control Panel
Control Panel
Adjust your computer's settings
View by: Category
System and Security
Review your computer's status
Save backup copies of your files with File History
Find and fix problems
User Accounts and Family Safety
Change account type
Set up Family Safety for any user
Network and Internet
View network status and tasks
Choose homegroup and sharing options
Appearance and Personalization
Change the theme
Change desktop background
Adjust screen resolution

3. Select “Change advanced sharing settings” in Network and Sharing Center.


Network and Sharing Center
« Net... › Network and Sharing Ce...
Search Control Panel
Control Panel Home
Change adapter settings
Change advanced sharing settings
See also
HomeGroup
Internet Options
Windows Firewall
View your basic network information and set up connections
View your active networks
Change your networking settings
Set up a new connection or network

Network
Private network

Access type: Internet
HomeGroup: Ready to create
Connections: Ethernet

Set up a broadband, dial-up, or VPN connection; or set up a router or access point.

4. Choose “Turn off file and printer sharing” and Save changes.

Group Policy

Note: Please see Group Policy section (not me) for more.

- Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options
    - LAN Manager Authentication Level → Send NTLMv2 response only. Refuse LM & NTLM
    - 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 security: Do not store LAN Manager hash value on next password change → Enabled

Malicious Indicators

- Meterpreter Processes
    - metsrv.dll, metsvc-server.exe, metsvc.exe
- Prevent Mimikatz!!!
    - In **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Ls**a find **Security Packages** and remove “**wdigest**”

NECCDC 2019
Champlain College

MS08-67: Downadup/Conficker

Note: For server installations.

1. Disable Server and Computer Browser Services.
2. Block TCP ports 139 and 445.
3. Disable NetBIOS over TCP/IP.
    a. For EACH adapter (Network & Internet Settings → Change Adapter Options → <Ethernet/Wi-Fi> Adapter → Properties → Internet Protocol Version 4 (TCP/IPv4) → Advanced → WINS [tab] → Disable NetBIOS over TCP/IP)

Remote Connections/Access (Disable) -

1. Disable Remote Assistance & Remote Desktop (Control Panel → Advanced System Settings → Remote).
2. Disable Network Shares (Control Panel → Network and Sharing Center → Advanced Sharing Settings).
    a. Network Discovery → Turn off network discovery
    b. File and Printer Sharing → Turn off file and printer sharing
    c. Public Folder Sharing → Turn off Public folder sharing (people logged on to this computer can still access these folders)

Turn Windows Feature On or Off

1. Search for “Turn Windows Features On or Off”.
2. Uncheck:
    a. Print and Document Services
    b. SMB 1.0/CIFS File Sharing Support
    c. Telnet Server & Client
    d. XPS Services

UEFI Secure Boot -

Windows Defender Firewall -

1. Ensure Windows Defender Firewall is on.
2. Restore Default Policy: Right-click “Windows Firewall w/ Advanced Security on Local Computer” and select “Restore Default Policy”.
3. Disable every Inbound rule except:
    a. Allow Core Networking ICMPv4 in
    b. Allow Core Networking DHCP (Dynamic Host Config Protocol) in
    c. ADD Allow Port UDP 1514 in (Local Subnet Only: Right-click rule → Scope → Add Local IP)
4. Disable every Outbound rule except:
    a. Internet Explorer, TCP 80,443 | UDP 53
    b. ADD Allow Port UDP 1514 out (Local Subnet Only: Right-click rule → Scope → Add Local IP)

Miscellaneous Tools/Notes -

- Microsoft Security Compliance Toolkit (SCT): **Windows 10 ONLY!!!** Download from Microsoft. Compare current GPOs with Microsoft-recommended GPO baselines or other baselines, edit them, and apply them through AD or local policy.
- Microsoft Security Configuration Wizard (SCW): **Windows Server ONLY!!!** Comes with Server Manager. Server Manager → Tools → Security Configuration Wizard.
- Microsoft Baseline Security Analyzer (MBSA): **Windows 7, Windows Server 2008, and later ONLY!!!** Download from Microsoft. Identifies missing security updates and common security misconfigurations.
- Microsoft Enhanced Mitigation Experience Toolkit (EMET): **Windows 7, Windows Server 2008, and later ONLY!!!** Download from Microsoft. Helps prevent vulnerabilities in software from being successfully exploited.
- Microsoft Security Essentials: **Windows 7 ONLY!!!** Download from Microsoft. Alternative to Windows Defender.

Extra Ideas: AppLocker, BitLocker

Windows Server Core 2016

Note: Follow the above guide for Windows 10 in addition to the below.

Initial Steps -

- Change your account password
- Remove unnecessary user accounts
- Ensure only one account has administrator access (Create a new Admin, disable local administrator)
- Update Windows

Network Time Protocol -

NECCDC 2019
Champlain College

CentOS

<Ella>
Initial Steps -

- Change root password: passwd
- Disable root login: nano /etc/ssh/sshd_config
    - Disable
- Remove

Ubuntu

<Ella>