










Basic Windows Hardening Guide/Checklist

OS		64 bit []	32 bit []
Hostname			
Domain			
Networking			
MAC			
IPv4		Gateway	Subnet
DNS #1		DNS #2	
Services		Hardware	
1. 2. 3. 4. 5.		RAM: CPU: HDD:	

Remember – Run commands in admin terminals (powershell > cmd > Win+R [Run] > Start Menu)

Done	To-Do
	To quickly fill out the top box- <code>systeminfo</code> <code>getmac</code>
	Is your box in English? Move on. Otherwise... <code>control intl.cpl</code>
	Delete All scheduled tasks <code>schtasks /delete /tn * /f</code>
	Change network type to public & setup LAN like the picture below <code>control netcpl.cpl</code> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <input type="checkbox"/> Client for Microsoft Networks <input type="checkbox"/> QoS Packet Scheduler <input type="checkbox"/> File and Printer Sharing for Microsoft Networks <input type="checkbox"/> Internet Protocol Version 6 (TCP/IPv6) <input checked="" type="checkbox"/> Internet Protocol Version 4 (TCP/IPv4) <input type="checkbox"/> Link-Layer Topology Discovery Mapper I/O Driver <input type="checkbox"/> Link-Layer Topology Discovery Responder </div>
	Setup For PS Scripts (PowerShell) <code>Set-ExecutionPolicy bypass -Force</code> <code>Disable-PSRemoting -Force</code> <code>Clear-Item -Path WSMan:\localhost\Client\TrustedHosts -Force</code> <code>Import-Module ServerManager</code> <code>Import-Module ActiveDirectory</code> <code>Add-WindowsFeature RSAT-AD-Powershell</code> <code>Add-WindowsFeature Powershell-ISE</code> Reset Group Policy (cmd) [Can also manually remove the GPO folders instead of RD] <code>RD /S /Q "%windir%\System32\GroupPolicyUsers"</code> <code>RD /S /Q "%windir%\System32\GroupPolicy"</code> <code>dcpofix /target:both</code> <code>gpupdate /force /logoff</code>

	<p>Firewall Script (cmd) <code>netsh interface set interface name="Local Area Connection" admin=disabled</code> <code>netsh advfirewall reset</code> <code>netsh advfirewall set allprofile state on</code> <code>netsh advfirewall firewall set rule name=all new enable=no</code> <code>netsh interface teredo set state disable</code> <code>netsh interface ipv6 6to4 set state state=disabled undoonstop=disabled</code> <code>netsh interface ipv6 isatap set state state=disabled</code> <code>netsh interface ipv4 set global mldlevel=none</code> <code>netsh interface set interface name="Local Area Connection" admin=disabled</code></p> <p>Disable Universal Plug and Play (PowerShell) <code>New-ItemProperty "HKLM:\SOFTWARE\Microsoft\DirectPlayNATHelp\DPNHUPnP" -Name "UPnPMode" -Value 2 -PropertyType "DWord"</code></p> <p>Delete All Scheduled Tasks (cmd) <code>schtasks /delete /tn * /f</code></p> <p>Preemptive fixes (cmd) <code>sfc /scannow</code></p> <p>Max Out UAC (PowerShell) <code>C:\Windows\System32\UserAccountControlSettings.exe</code></p>
	<p>Windows Firewall with Advanced Security on Local Computer > Windows Firewall Properties</p> <p>Domain Profile</p> <p> Windows Firewall is on.</p> <p> Inbound connections that do not match a rule are blocked.</p> <p> Outbound connections that do not match a rule are blocked.</p> <hr/> <p>Private Profile is Active</p> <p> Windows Firewall is on.</p> <p> Inbound connections that do not match a rule are blocked.</p> <p> Outbound connections that do not match a rule are blocked.</p> <hr/> <p>Public Profile</p> <p> Windows Firewall is on.</p> <p> Inbound connections that do not match a rule are blocked.</p> <p> Outbound connections that do not match a rule are blocked.</p> <hr/> <p>Under all profiles > Advanced > Allow Unicast Response > No</p>
	<p>Open Device Manager <code>mmc devmgmt.msc</code></p> <p>View > Show Hidden Devices</p> <p>Right Click > Disable:</p> <ul style="list-style-type: none"> • Network Adapters > WAN Miniport (IPv6) • Network Adapters > Microsoft ISATAP Adapter • Network Adapters > Teredo Tunneling Pseudo Interface (IPv6 tunnel) <p>Right Click > Properties > Disable:</p> <ul style="list-style-type: none"> • Non-Plug and Play Drivers > Remote Access IPv6 ARP Driver • Non-Plug and Play Drivers > NETBT

	<ul style="list-style-type: none"> Note: AD probably needs this. Make sure it's running "SYSTEM" or "AUTOMATIC" and not "DISABLED" which is more of a workstation (w7) thing, basically, be careful. <p>Consider Disabling Mic's / Webcams on laptops <i>There are slight differences in this category for Windows 10</i></p>
	<p>Delete Personal Settings + Reset IE <code>RunDll32.exe InetCpl.cpl,ResetIEToDefaults</code></p> <p><code>control inetcpl.cpl</code> Connections>LAN Settings Setup CCDC Proxy (Regional) + Uncheck "Automatically Detect Settings"</p>
	<p>Create New Local Admin Account (Get from Policy Team Docs.)</p> <ul style="list-style-type: none"> Name: Password: <p><code>net user <user> <password> /ADD</code> <code>net localgroup Administrators <user> /ADD</code></p> <p>Remember that ".\<user>" forces local logon and bypasses domain.</p>
	<p>Check your startup & disable unnecessary things. <code>msconfig</code></p>
	<p>Login to new local admin & Check all local users</p> <ul style="list-style-type: none"> Disable, Change Password, Remove from Local Admin grp, add to guests only <p><code>net user</code> <code>net user <user></code> <code>net user <user> /active:no</code> <code>net user <user> <password></code></p> <p>To quickly change all users... <code>net user > C:\temp\users.txt</code></p> <p>Open users.txt and remove the fluff, put each name on a line and put "net user" in front of it and the password after it and save the file as a .bat and run it.</p> <p>Example:</p> <pre>net user admin1 super_good_password1234! net user guy1 not_great_password4321! net user guy2 not_great_password4321! net user guy3 not_great_password4321!</pre>
	<p>Check if anyone is logged in, etc. <code>query session</code> <code>query user</code> <code>query process</code></p>
	<p>Delete Unnecessary Shares (C\$, ADMIN\$, IPC\$, SYSVOL, NETLOGON – All Expected!)</p> <p><code>net share</code> <code>net share <ShareName> /delete</code></p>
	<p><code>control sysdm.cpl</code></p> <p>>Advanced>Performance>Visual Effects>Adjust for Best Performance>Ok >Advanced>Performance>Data Exec Prev.>Turn on DEP for all programs and services... >Advanced>Startup & Recovery>Write Debugging>(none) ...>Remote>Disable 'Allow Remote Assistance...'>Ok</p> <p><code>control folders</code> (View Tab)</p>

	<ul style="list-style-type: none"> • Check <ul style="list-style-type: none"> ○ Always Show Menus ○ Display Full path in title bar ○ show hidden files, folders and drives • Uncheck <ul style="list-style-type: none"> ○ hide empty drives in computer folder ○ hide extensions for known file types ○ hide protected operating system files
	<p>Manual Firewall Rules <i>(For Convenience, Right click on I/O and Filter by State "Enabled")</i></p> <ul style="list-style-type: none"> • Outbound - Deny <ul style="list-style-type: none"> ○ %SystemRoot%\System32\WindowsPowerShell\v1.0\powershell.exe ○ %SystemRoot%\System32\WindowsPowerShell\v1.0\powershell_ise.exe ○ %SystemRoot%\System32\cmd.exe • Outbound - Allow <ul style="list-style-type: none"> ○ service 'Windows update' ○ service 'Windows Time' ○ program '\program files\windows defender\msacui.exe' ○ program <Firefox/Chrome/Opera, whichever browser you use> ○ program \program files\Internet explorer\iexplore.exe ○ program \program files x86\Internet explorer\iexplore.exe ○ program <your antivirus update program> ○ Core Networking DHCP-out (IPv4 Only – If available) ○ Allow graded services / AD Required Services • Inbound - Allow <ul style="list-style-type: none"> ○ Core Networking DHCP in (IPv4 Only – If available) ○ Allow graded services / AD Required Services
	<p><u>Comp/Policies/WindowsSettings/SecuritySettings...</u></p> <p>Restrict NTLM: Incoming Traffic Enable</p> <p>/Account Policies/Account Lockout Policy</p> <p>Account lockout duration 30 minutes</p> <p>Account lockout threshold 2 invalid logon attempts</p> <p>Reset account lockout counter after 30 minutes</p> <p>/Account Policies/Kerberos Policy</p> <p>Enforce user logon restrictions Enabled</p> <p>Maximum lifetime for service ticket 600 minutes</p> <p>Maximum lifetime for user ticket 10 hours</p> <p>Maximum lifetime for user ticket renewal 7 days</p> <p>Maximum tolerance for computer clock synchronization 5 minutes</p> <p>/Local Policies/Audit Policy</p> <p>Audit account logon events Success, Failure</p> <p>Audit account management Success, Failure</p>

<p> Audit directory service access Success, Failure Audit logon events Success, Failure Audit object access Success, Failure Audit policy change Success, Failure Audit privilege use Success, Failure Audit process tracking None Audit system events None /Local Policies/Security Options Accounts: Local Administrator account status Disabled Accounts: Local Guest account status Disabled Accounts: Limit local account use of blank passwords to console logon only Enabled Accounts: Rename administrator account "AdminRenamed" Accounts: Rename guest account "GuestsNotAllowedHere" Accounts: Block Microsoft Accounts 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 days Domain member: Require strong (Windows 2000 or later) session key Enabled Interactive logon: Message title for users attempting to log on: GPO MSG Interactive logon: Message text for users attempting to log on: GPO APP Interactive logon: Number of Previous logons to cache 1 Microsoft network client: Digitally sign communications (if server agrees) Enabled Microsoft network client: Send unencrypted password to third-party SMB servers Disabled Network security: LAN Manager auth. lvl Send NTLMv2 response only\refuse NTLM & LM Network security: Do not store LAN Manager hash value on next password chg Enabled Network access: Do not allow anon enumeration of SAM accounts and shares Enabled Network access: Do not allow anon enumeration of SAM accounts Enabled Network access: Allow anon SID/name translation Disabled /Event Log Prevent local guests group from accessing application log Enabled Prevent local guests group from accessing security log Enabled Prevent local guests group from accessing system log Enabled Network Access: Remotely Accessible Registry paths and sub paths Disabled /Local Policies/Security Options/User Rights Assignment Deny RDP Enabled <u>Computer/Policies/AdminTemplates...</u> /System/GroupPolicy Disallow Interactive Users from generating Resultant Set of Policy data Disabled Group Policy refresh interval for computers 5min / 5min /Windows Comp/Remote Desktop Services/Remote Desktop Session Host\Sec. </p>	
---	--

	Set client connection encryption level High
	Uninstall unnecessary programs (TightVNC, TeamViewer, etc.) Control appwiz.cpl Check your startup & disable unnecessary stuff (usually almost all of it) Msconfig Check your browsers for malicious toolbars, etc. Reset FireFox/Chrome if possible. Reboot
	Try doing a windows update – focus on security updates. If WSUS is broken just try removing / re-adding the feature. Worst case, fall back to the offline WSUS tool.
	Install AntiVirus <ul style="list-style-type: none"> Avira > AVG > Kapersky > McAfee > Microsoft Security Essentials Expect a lot of these to outright fail on Server OS's
	Install EMET <ul style="list-style-type: none"> DEP – Always on SEHOP – always on ASLR – app opt in Apps > Add Application > Windows\System32\wuauclt.exe Apps > Add Application > Windows\servicing\trustedinstaller.exe Apps > Add Application > Internet Facing Service (AV / Browsers, etc.)
	<p style="text-align: center;">Active Directory Only Notes</p> <p>Critical Services:</p> <ul style="list-style-type: none"> File Replication Services (FRS) Distributed File System Replication (DFSR) DNS Client & Server Kerberos Distribution Center (KDC) Netlogon Windows Time Active Directory Domain Services (AD DS) Active Directory Web Services (AD WS) Remote Procedure Call (RPC) service <p>Should be Operational:</p> <ul style="list-style-type: none"> LDAP - 389 SMB - 445 RPC - 135 NetBIOS - 138, 137, 139, (42) DHCP - 67, 2535 <p>IIS?</p> <ul style="list-style-type: none"> HTTP/S - 80, 443 <p>Email?</p> <ul style="list-style-type: none"> Exchange - 143, 993, 110, 995, 593, 2535 <p>Probably Block These...</p>

FTP, Telnet, Terminal Services – 21, 23, 69, 3389

GPO Problems?

Check your sysvol folders are not marked as Read-Only! Try the resets & gpupdate again.

Security Tools	
1. Ninite installer	https://ninite.com/
2. Sysinternals Suite	https://download.sysinternals.com/files/sysinternalsuite.zip
3. Nmap	https://nmap.org/download.html
4. Glasswire	https://www.glasswire.com/
5. Tiny Firewall	http://tinywall.pados.hu/
6. Avira AV	http://www.avira.com/en/avira-free-antivirus
7. EMET (Needs .NET4)	https://www.microsoft.com/en-us/download/details.aspx?id=46366
8. Md5deep	http://md5deep.sourceforge.net/ <code>Md5deep -re1 C:\ > hashes.md5</code>
9. Wireshark	https://www.wireshark.org/download.html
10. 7zip	http://www.7-zip.org/download.html
11. Notepad++	https://notepad-plus-plus.org/download/
12. WinPatrol	http://www.bleepingcomputer.com/download/winpatrol/
13. GPO Viewer	http://blogs.technet.com/b/secguide/archive/2016/01/22/new-tool-policy-analyzer.aspx
14. WSUS Update	http://download.wsusoffline.net/wsusoffline1031.zip
15. .NET Framework 4	http://www.microsoft.com/en-ca/download/details.aspx?id=17718
16. Disable IPv6	https://support.microsoft.com/en-us/kb/929852
17. Ambush IPS	http://ambuships.com
18. Artillery	https://github.com/trustedsec/artillery
19. OSSec	https://ossec.github.io/downloads.html
20. PUTTY	http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

Upgrading PowerShell for W2K8

Run "Windows PowerShell Modules" (Admin Tools / Start Menu)

- Install .NET Framework 4.0 or **.NET Framework 4.5**
 - <https://www.microsoft.com/en-us/download/details.aspx?id=17851>
 - <https://www.microsoft.com/en-us/download/details.aspx?id=30653>
- Install W2K8R2 ServicePack 1
 - <https://www.microsoft.com/en-us/download/details.aspx?id=5842>
- Install **Windows Management Framework 3.0 or 4.0 (6.1)**
 - <https://www.microsoft.com/en-us/download/details.aspx?id=34595>
 - <https://www.microsoft.com/en-us/download/details.aspx?id=40855>

Reboot a few times...cross your fingers

one_cmd.ps1

```
gps cmd | kill
saps cmd.exe -ArgumentList "/k title DoNotClose"
$truecmd = (gps cmd).StartTime
while ($true){
    if (gps cmd | ? {$_.StartTime -gt $truecmd}){
        gps cmd | ? {$_.StartTime -gt $truecmd} | kill | Out-Null
        write-host "Killed cmd.exe @" (Get-Date -f "HH:mm:ss") -f red
    }
}
```

ps_kill.ps1

```
"Running"
while ($true){
    $getproc = gps Ps* | Select Id
    $id = $getproc.Id
    if ($getproc){
        $id
        kill $id -Force -EA SilentlyContinue
    }
}
```

gen_whitelist.ps1

```
$file = "C:\Users\$env:username\Desktop\wl.txt"
gps | % {$_.processname} | Out-File $file -en ascii -fo
cat $file | sort -u | % {$_.TrimEnd()} | sc $file -fo
```

whitelist.ps1

```
clear
while ($true){
    foreach ($i in gps){
        $pn = $i.ProcessName
        if ((Get-Content wl.txt) -notcontains $pn){
            write-host $pn "| " -f red -n
            write-host (((Get-WmiObject -cl win32_Process -f "name LIKE '$pn%'").getowner() | Select User).User) -f red -n
            write-host " | " (Get-Date -f "HH:mm:ss") -f red
            gps $pn | kill -f
            sleep -s 1
        }
    }
}
```

mass_pass.ps1

```
$pass = 'HOW neat is 2016!?!?'
foreach ($user in (Get-ADUser -Filter *)){
    write-host "Setting password for" $user.name
    Set-ADAccountPassword -Identity ($user.SamAccountName) -NewPassword (ConvertTo-SecureString -
    AsPlainText $pass -Force)
}
Disable-ADAccount -Identity 'Guest'
```

Hash.ps1

```
Write-Host "Working...started - " (Get-Date -format g)
Get-FileHash ((gci 'C:\' -Recurse -ErrorAction SilentlyContinue).FullName) -Algorithm
MD5 -ErrorAction SilentlyContinue | epcsv "FileHashes.csv" -Encoding ASCII -
NoTypeInfoInformation
#Ask Whiteteam if CSV is okay. No? Replace epcsv stuff with 'Out-File "FileHashes.txt"
-Encoding ascii' which will require word-wrapping off to view correctly as a .txt
```