**Basic Windows Hardening Guide/Checklist**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **OS** |  | | | | | **64 bit [ ]** | | **32 bit [ ]** |
| **Hostname** |  | | | | | | | |
| **Domain** |  | | | | | | | |
| **Networking** | | | | | | | | |
| **MAC** |  | | | | | | | |
| **IPv4** |  | **Gateway** |  | | **Subnet** | |  | |
| **DNS #1** |  | **DNS #2** |  | | | | | |
| **Services** | | | | **Hardware** | | | | |
|  | | | | **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-  systeminfo  getmac |
|  | Is your box in English? Move on. Otherwise…  control intl.cpl |
|  | Delete All scheduled tasks  schtasks /delete /tn \* /f |
|  | Change network type to public & setup LAN like the picture below  control netcpl.cpl |
|  | **Setup For PS Scripts (PowerShell)**  Set-ExecutionPolicy bypass –Force  Disable-PSRemoting -Force  Clear-Item -Path WSMan:\localhost\Client\TrustedHosts –Force  Import-Module SeverManager  Import-Module ActiveDirectory  Add-WindowsFeature RSAT-AD-Powershell  Add-WindowsFeature Powershell-ISE  **Reset Group Policy (cmd) [Can also manually remove the GPO folders instead of RD]**  RD /S /Q "%WinDir%\System32\GroupPolicyUsers"  RD /S /Q "%WinDir%\System32\GroupPolicy"  dcgpofix /target:both  gpupdate /force /logoff  **Firewall Script (cmd)**  netsh interface set interface name="Local Area Connection" admin=disabled  netsh advfirewall reset  netsh advfirewall set allprofile state on  netsh advfirewall firewall set rule name=all new enable=no  netsh interface teredo set state disable  netsh interface ipv6 6to4 set state state=disabled undoonstop=disabled  netsh interface ipv6 isatap set state state=disabled  netsh interface ipv4 set global mldlevel=none  netsh interface set interface name="Local Area Connection" admin=disabled  **Disable Universal Plug and Play (PowerShell)**  New-ItemProperty "HKLM:\SOFTWARE\Microsoft\DirectPlayNATHelp\DPNHUPnP" -Name "UPnPMode" -Value 2 -PropertyType "DWord"  **Delete All Scheduled Tasks (cmd)**  schtasks /delete /tn \* /f  **Preemptive fixes (cmd)**  sfc /scannow  **Max Out UAC (PowerShell)**  C:\Windows\System32\UserAccountControlSettings.exe |
|  | Windows Firewall with Advanced Security on Local Computer > Windows Firewall Properties    Under all profiles > Advanced > Allow Unicast Response > No |
|  | **Open Device Manager**  mmc devmgmt.msc  View > Show Hidden Devices  Right Click > Disable:   * Network Adapters > WAN Miniport (IPv6) * Network Adapters > Microsoft ISATAP Adapter * Network Adapters > Teredo Tunneling Pseudo Interface (IPv6 tunnel)   Right Click > Properties > Disable:   * Non-Plug and Play Drivers > Remote Access IPv6 ARP Driver * Non-Plug and Play Drivers > NETBT   + 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.   Consider Disabling Mic’s / Webcams on laptops  *There are slight differences in this category for Windows 10* |
|  | Delete Personal Settings + Reset IE  RunDll32.exe InetCpl.cpl,ResetIEtoDefaults  control inetcpl.cpl  Connections>LAN Settings  Setup CCDC Proxy (Regional) + Uncheck “Automatically Detect Settings” |
|  | Create New Local Admin Account (Get from Policy Team Docs.)   * Name: * Password:   net user <user> <password> /ADD  net localgroup Administrators <user> /ADD  Remember that “.\<user>” forces local logon and bypasses domain. |
|  | Check your startup & disable unnecessary things.  msconfig |
|  | Login to new local admin & Check all local users   * Disable, Change Password, Remove from Local Admin grp, add to guests only   net user  net user <user>  net user <user> /active:no  net user <user> <password>  To quickly change all users…  net user > C:\temp\users.txt  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.  Example:  *net user admin1 super\_good\_password1234!*  *net user guy1 not\_great\_password4321!*  *net user guy2 not\_great\_password4321!*  *net user guy3 not\_great\_password4321!* |
|  | Check if anyone is logged in, etc.  query session  query user  query process |
|  | Delete Unnecessary Shares (C$, ADMIN$, IPC$, SYSVOL, NETLOGON – All Expected!)  net share  net share <ShareName> /delete |
|  | control sysdm.cpl  >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  control folders (View Tab)   * Check   + Always Show Menus   + Display Full path in title bar   + show hidden files, folders and drives * Uncheck   + hide empty drives in computer folder   + hide extensions for known file types   + hide protected operating system files |
|  | Manual Firewall Rules *(For Convenience, Right click on I/O and Filter by State “Enabled”)*   * **Outbound - Deny**   + %SystemRoot%\System32\WindowsPowerShell\v1.0\powershell.exe   + %SystemRoot%\System32\WindowsPowerShell\v1.0\powershell\_ise.exe   + %SystemRoot%\System32\cmd.exe * **Outbound - Allow**   + 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**   + Core Networking DHCP in (IPv4 Only – If available)   + Allow graded services / AD Required Services |
|  | **Comp/Policies/WindowsSettings/SecuritySettings...**  Restrict NTLM: Incoming Traffic **Enable**  **/Account Policies/Account Lockout Policy**  Account lockout duration **30 minutes**  Account lockout threshold **2 invalid logon attempts**  Reset account lockout counter after **30 minutes**  **/Account Policies/Kerberos Policy**  Enforce user logon restrictions **Enabled**  Maximum lifetime for service ticket **600 minutes**  Maximum lifetime for user ticket **10 hours**  Maximum lifetime for user ticket renewal **7 days**  Maximum tolerance for computer clock synchronization **5 minutes**  **/Local Policies/Audit Policy**  Audit account logon events **Success, Failure**  Audit account management **Success, Failure**  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**  **Computer/Policies/AdminTemplates...**  **/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.**  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**   * Avira > AVG > Kapersky >McAfee > Microsoft Security Essentials   Expect a lot of these to outright fail on Server OS’s |
|  | **Install EMET**   * 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.) |
|  | **Active Directory Only Notes**  **Critical Services:**   * 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   **Should be Operational:**   * LDAP - 389 * SMB - 445 * RPC - 135 * NetBIOS - 138, 137, 139, (42) * DHCP - 67, 2535   **IIS?**   * HTTP/S - 80, 443   **Email?**   * Exchange - 143, 993, 110, 995, 593, 2535   **Probably Block These...**  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/> |
| 1. **Sysinternals Suite** | <https://download.sysinternals.com/files/sysinternalssuite.zip> |
| 1. Nmap | <https://nmap.org/download.html> |
| 1. Glasswire | <https://www.glasswire.com/> |
| 1. Tiny Firewall | <http://tinywall.pados.hu/> |
| 1. **Avira AV** | <http://www.avira.com/en/avira-free-antivirus> |
| 1. **EMET (Needs .NET4)** | <https://www.microsoft.com/en-us/download/details.aspx?id=46366> |
| 1. Md5deep | <http://md5deep.sourceforge.net/>  Md5deep –rel C:\ > hashes.md5 |
| 1. Wireshark | <https://www.wireshark.org/download.html> |
| 1. 7zip | <http://www.7-zip.org/download.html> |
| 1. Notepad++ | <https://notepad-plus-plus.org/download/> |
| 1. WinPatrol | <http://www.bleepingcomputer.com/download/winpatrol/> |
| 1. GPO Viewer | <http://blogs.technet.com/b/secguide/archive/2016/01/22/new-tool-policy-analyzer.aspx> |
| 1. **WSUS Update** | <http://download.wsusoffline.net/wsusoffline1031.zip> |
| 1. **NET Framework 4** | <http://www.microsoft.com/en-ca/download/details.aspx?id=17718> |
| 1. **Disable IPv6** | <https://support.microsoft.com/en-us/kb/929852> |
| 1. Ambush IPS | <http://ambuships.com> |
| 1. Artillery | <https://github.com/trustedsec/artillery> |
| 1. **OSSec** | [**https://ossec.github.io/downloads.html**](https://ossec.github.io/downloads.html) |
| 1. 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**](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**](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 -NoTypeInformation  #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 |