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

	`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

	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**
	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/
2. Sysinternals Suite	https://download.sysinternals.com/files/sysinternalssuite.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/ `Md5deep -rel C:\ > hashes.md5`
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 -
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
```