Windows Domain Checklist

1. **Turn on Windows Firewall**
   1. After DC disables Group Firewalls run ***gpupdate /force*** on each machine
      1. DC -> gpmc.msc in the search bar and find “default domain policy”
      2. Group firewall settings are in Policies -> Windows Settings -> Windows firewall with advanced security.
   2. Configure Properly for each separate box, only allow services in that need to talk to the host, such as rdp, smb, http, etc….
      1. In the search bar: wf.msc
2. **Create Snapshots Right Away!**
3. **Account management**
   1. **Set passwords for all user accounts!**

Import-Module ActiveDirectory

Get-ADUser -Filter \* | Set-ADAccountPassword -Reset -NewPassword (ConvertTo-SecureString -AsPlainText “**PASSWORD**” -Force)

gwmi -class win32\_useraccount -filter localaccount=true | % {net user $\_.name “**PASSWORD**”}

* 1. Disable unneeded user accounts
  2. Check both local and AD accounts
     1. Turn on LAPS for local accounts
  3. Make sure accounts are in the correct groups
     1. Check Domain Admins, Schema Admins, and Enterprise Admins
  4. Rename built-in admin account (non-DC only)
     1. In the search bar: lusrmgr.msc
  5. Check sharing permissions

1. **Install Firewall and defense software**
   1. Install a firewall if there is none.
   2. Enable Windows Defender, download MalwareBytes
      1. <http://bit.ly/2HSL7NB>
   3. Get Comodo KillSwitch
      1. <http://bit.ly/2FAyftZ>
2. **Check external facing services**
   1. Visit your own hosted services and make sure you aren’t exposing any critical information
      1. Check SMB shares, http sites, ftp servers, etc…
   2. Run netstat or KillSwitch, make sure you don’t have any unneeded ports open
3. **Make Backups of all critical services**
   1. DNS Right Click Zone, Change to store locally, not in AD, copy, change back to store in AD. File is Located in C:\Windows\System32\dns

*dnscmd* ***zonename*** */zoneexport* ***Zone.com*** *backup\zone1.com.dns.bak*

Export-DnsServerZone -Name **\_msdcs.ccdc.lan** -FileName **\_msdcs.ccdc.lan.bkp**

* 1. Web
  2. FTP

1. **Check Startup Programs**
   1. shell:startup
   2. Check Scheduled Tasks
      1. Both of these are part of the comodo suite
2. **Patch Critical Vulnerabilities**
   * 1. For XP, 2000 and 2003 patch MS08\_067
     2. For Vista and 2008 patch MS09\_050
     3. For Windows Server 2012,2016, Windows 7,8,10 patch Eternal Blue and BlueKeep
3. **Set Policies - Active Directory – Add Group Policy Object MMC**
   1. XPassword Policies
      1. Min Length - 14
      2. Enforce Password history - min 3
      3. maximum age - < 3 days
      4. min age - none
      5. reversible encryption - SHOULD BE SET TO DISABLED
   2. Audit Policies
   3. Security Policies
   4. Warning Messages
   5. Change Services
   6. Turn on DEP bcdedit.exe /set {current} nx AlwaysOn
   7. Disable Remote Desktop if unscored
4. **Download tools (and place them in a shared folder)**
   1. Sysinternals
      1. Autoruns
      2. TCPView
   2. Microsoft Baseline Security Analyser
      1. <http://bit.ly/2TxPnUP>
   3. EMET 5.5.2
5. **Remove unwanted viruses and software**
   1. Also check Add/Remove Programs
   2. Remove unneeded Windows components
   3. Run MBAM
   4. Check Task Manager
   5. Check msconfig
   6. Check “C:\Windows\Temp”
6. **Patch at the very end!**
   1. Turn on windows updates

**Report for Local User Password Changes (Powershell)**

gwmi -class win32\_useraccount | % {$\_.name+”:**PASSWORD**”} | Out-File users.txt

**Report for AD Password Changes (Powershell)**

$users = Get-ADUser -filter \*; $results = foreach ($u in $users) { $u.SamAccountName + “:**PASSWORD**”}; $results | Out-File adusers.txt

**Change Local Account Passwords (PowerShell as ADMIN):**

gwmi -class win32\_useraccount -filter localaccount=true | % {net user $\_.name “**PASSWORD**”}

**Change Domain Account Passwords (PowerShell):**

Get-ADUser -Filter \* | Set-ADAccountPassword -Reset -NewPassword (ConvertTo-SecureString -AsPlainText “**PASSWORD**” -Force)

**Change Single Domain Account Password (PowerShell):**

Set-ADAccountPassword -Identity USERNAME -Reset -NewPassword (ConvertTo-SecureString -AsPlainText “PASSWORD -Force)

**Backup For Changing Local Account Passwords (PowerShell):**

foreach ($x in (Get-wmiobject -class win32\_useraccount -filter localaccount=true | select-object name)){ net user $x.name “PASSWORD” }

**Disable SMBv1**

Windows 8.1, Windows 10, Windows 2012 R2, and Windows Server 2016

Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol

Windows 8 and Windows Server 2012

Set-SmbServerConfiguration -EnableSMB1Protocol $false

Windows 7, Windows Server 2008 R2, Windows Vista, and Windows Server 2008

Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" SMB1 -Type DWORD -Value 0 –Force

**Install Microsoft Security Essentials on Server 2012**

Change .exe compatibility to Windows 7

mseinstall.exe /disableoslimit

**Enable AD Powershell Module**

Import-Module ActiveDirectory

**Password Policy & Account Lockout (GPO - Default Domain Policy)**

Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies

**Windows Firewall (GPO)**

Computer Configuration > Policies > Windows Settings > Security Settings > Windows Defender Firewall

**Logon Message (GPO)**

Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options > Interactive Logon

**Install Microsoft Security Essentials on Server 2012**

Change .exe compatibility to Windows 7

mseinstall.exe /disableoslimit

**Backup DNS**

Powershell as Admin. These files are stored in C:\Windows\System32\dns. Copy them somewhere else!

Export-DnsServerZone -Name **ccdc.lan** -FileName **ccdc.lan.bkp**

Export-DnsServerZone -Name **\_msdcs.ccdc.lan** -FileName **\_msdcs.ccdc.lan.bkp**

**Restore DNS**

Copy DNS file to C:\Windows\System32\dns\**ccdc.lan.dns**

Create New Zone > Primary Zone > **ccdc.lan** > Use existing file > **ccdc.lan.dns** > Do not allow dynamic updates > Finish > Right-Click new zone > Properties > Change type > Make sure it is Primary Zone & check Store zone in AD > Change Dynamic updates to Secure Only

**On domain ccdc.lan:**

dsquery user ou=Users,dc=**ccdc**,dc=**lan** | dsmod user -pwd RedTeamSucks! -mustchpwd (user must change password) yes

**Random useful commands:**

Regedit: HKEY\_LOCAL\_MACHINE->SOFTWARE->Policies->Microsoft->Windows Firewall->FirewallRules

SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\FirewallRules

Install Gui for Server Core: Add-WindowsFeature Server-Gui-Shell, Server-Gui-Mgmt-Infra\

@echo off

netsh advfirewall set allprofiles firewallpolicy blockinboundalways,blockoutbound

@echo off

netsh advfirewall set allprofiles firewallpolicy allowinbound,blockoutbound