ask the people, what about CCDC scoring user

check for users, scripting users.

**Windows OS/Server hardening, configuration**

**Initial checks (First Hour)**

1. Change Local Admin accounts name/password
   1. Windows Server LAN UN/PW (administrator/!Password123) CHANGE
   2. Windows 10 LAN UN/PW (jane/changeme) Internal? (minion/kingbob) CHANGE
   3. Windows 10 Docker PC
   4. DSRM Domain Controller password, CHANGE
   5. https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/appendix-d--securing-built-in-administrator-accounts-in-active-directory
2. Secure AD – steps #1 thru #6
3. Remove any not needed accounts
4. Check services
5. Disable guest account
6. Check security groups
7. Turn on windows firewall with highest security
8. Check what roles/features are installed.
   1. *SETUP ROLES/FEATURES from below*
9. Run windows updates (windows update assistant maybe?)
10. Set DHCP Default Router IP address’
    1. Local IP = 172.20.241.27 public IP = 172.25.team#.83

Install GlobalProtect on that Windows 10 box.

1. Reinstall features
2. Fix reverse lookups
3. Run GPO reset of default domain policy restore command
4. Log on as a domain administrator to a DC.
5. Start a command session.
6. To reset the Domain GPO, type  
   dcgpofix /target:Domain  
   To reset the Default DC GPO, type  
   dcgpofix /target:DC  
   To reset both the Domain and Default DC GPOs, type  
   dcgpofix /target:both  
   4.After you enter the appropriate command in Step 3, enter Y to both prompts.
7. Close the command window.

**Windows 10 Update Assistant**

<https://support.microsoft.com/en-us/topic/windows-10-update-assistant-3550dfb2-a015-7765-12ea-fba2ac36fb3f>

**Microsoft Security Toolkit**

<https://www.microsoft.com/en-us/download/details.aspx?id=55319>

<https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-security-configuration-framework/security-compliance-toolkit-10>

**Configure AD/DNS/DHCP setup**

<https://knowledgeacademy.io/windows-server-2019-a-step-by-step-tutorial-on-system-center-configuration-manager-sccm-with-practical-example-part-2/>

**Secure AD**

* + - 1. <https://petri.com/active-directory-security-5-steps-to-secure-ad/>
         1. <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/appendix-d--securing-built-in-administrator-accounts-in-active-directory>
         2. Securing Enterprise Admins groups in AD

<https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/appendix-e--securing-enterprise-admins-groups-in-active-directory#step-by-step-instructions-for-removing-all-members-from-the-enterprise-admins-group>

* + - 1. Securing Domain Admins Groups in AD
         1. <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/appendix-f--securing-domain-admins-groups-in-active-directory#step-by-step-instructions-to-secure-domain-admins-in-active-directory>
      2. Securing Administrators Groups in AD
         1. <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/appendix-g--securing-administrators-groups-in-active-directory#step-by-step-instructions-for-removing-all-members-from-the-administrators-group>
      3. Ensure proper access to ADDS/DB/Logfile/Sysvol directory
         1. <https://go.microsoft.com/fwlink/?LinkId=230534>
      4. Disable insecure encryption
         1. <https://learn.microsoft.com/en-us/services-hub/health/remediation-steps-ad/disable-the-allownt4crypto-setting-on-all-affected-domain-controllers>
      5. get-adcomputer -filter \* | out-file C:\useraccounts.txt (list of all computer objects in domain)
      6. Policies --> Windows Settings -> Security Settings --> Account Policies.Graphical user interface, text, application, email

         Description automatically generated
  1. **gpresult /H C:\passwords-policy-settings.html (**detailed report on the implemented account policies.

1. <https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/monitoring-active-directory-for-signs-of-compromise>
   1. https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/monitoring-active-directory-for-signs-of-compromise

**Secure DNS**

* 1. dnscmd /Config /CacheLockingPercent 100 (DNS Cahce locking percent default to 100, prevents cache entry overwrihgt during TTL)
  2. dnscmd /Config /SocketPoolSize 10000 (makes cache tampering attacks more difficult)
     1. run from elevated command prompt
  3. Configure DNSSEC
     1. Text

        Description automatically generated
  4. Split DNS needed?
  5. <https://learn.microsoft.com/en-us/training/modules/secure-windows-server-domain-name-system/1-introduction>
  6. https://knowledgeacademy.io/windows-server-2019-a-step-by-step-tutorial-on-system-center-configuration-manager-sccm-with-practical-example-part-2/
  7. <https://computingforgeeks.com/install-and-configure-dns-server-in-windows-server/>

**Secure DHCP**

* + - 1. <https://www.techtarget.com/searchnetworking/tip/A-guide-to-Windows-DHCP-server-configuration>
      2. MAC Address filtering
      3. Run DHCP server backup
      4. Assign DHCP server to Windows Server IP address (172.20.241.27)
    1. <https://computingforgeeks.com/how-to-install-and-configure-dhcp-server-on-windows-server/>

Script to change user passwords

Script to revert group policy

Change Windows 2012 AD/DNS/DHCP server Administrator password

* Disable weird accounts.

Change Windows 10 Administrator password

* Remove user from local admin group

Change Windows 2016 Administrator password

* Remove user from local admin group

C#D3nver3202-<systemVMdesignation>-<username>

Run Domain GPO fix for both domain and default

Dcgpofix /target:both

Run through GPO fixing Appendices D-G

ENABLE DNSSEC

ENABLE MAC ADDRESS FILTERING

AD Should be good

Reinstall DNS/DHCP

Scripts

# Password Rest from File

# Script: ResetPwd.ps1

# Description: Reset the password for bulk number of users, and

# set the property to change passwrod required at next logon

#

# Written by: Anand Venkatachalapathy

#

Import-Module ActiveDirectory

# Set the default password

$password = ConvertTo-SecureString -AsPlainText “TodayIsTheDayWeWinIn2023!” -Force

# Get the list of accounts from the file on file

# List the user names one per line

$users = Get-Content -Path c:\MyScripts\UserList.txt

ForEach ($user in $users)

{

# Set the default password for the current account

Get-ADUser $user | Set-ADAccountPassword -NewPassword $password -Reset

#If you need to set the property “Change password at next logon”,

#leave the next alone. If not, comment the next line

#Get-ADUser $user | Set-AdUser -ChangePasswordAtLogon $true

Write-Host “Password has been reset for the user: $user”

}

# ————- End ———–

#GetAdUser list to CSV

$path = ‘C:\myscripts\userlist.csv’

Get-ADUser -Filter 'enabled -eq $true' | Select-Object SamAccountName | Export-Csv -Path $Path -notypeinformation