Domain Hardening

* Change Default Passwords
* Change Admin PWD
* Disable/Delete Guest account
* Protect accounts from being deleted
* Update/Disable SMB to mitigate eternalBlue
* Enable Server Signing
* Install AntiVirus/AntiSpyware
* Look for DDoSs and Webapp Attacks

## Tools:

* <https://github.com/nccgroup/WinShareEnum>

## Commands:

* Full Defender scan == "%ProgramFiles%\Windows Defender\MpCmdRun.exe" -scan -scantype 2

### PowerShell methods

Here are the steps to detect, disable and enable SMBv1 client and server by using PowerShell commands.

Note

The computer will restart after you run the PowerShell commands to disable or enable SMBv1.

* Detect:
* PowerShell
* Get-WindowsOptionalFeature -Online -FeatureName SMB1Protocol
* Disable:
* PowerShell
* Disable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol
* Enable:
* PowerShell
* Enable-WindowsOptionalFeature -Online -FeatureName SMB1Protocol

#### SMBv1 on SMB Server

* Detect:
* PowerShell
* Get-SmbServerConfiguration | Select EnableSMB1Protocol
* Disable:
* PowerShell
* Set-SmbServerConfiguration -EnableSMB1Protocol $false
* Enable:
* PowerShell
* Set-SmbServerConfiguration -EnableSMB1Protocol $true

#### SMB v2/v3 on SMB Server

* Detect:
* PowerShell
* Get-SmbServerConfiguration | Select EnableSMB2Protocol
* Disable:
* PowerShell
* Set-SmbServerConfiguration -EnableSMB2Protocol $false
* Enable:
* PowerShell
* Set-SmbServerConfiguration -EnableSMB2Protocol $true

## Protect from NTLM relay with signing

1. Open ‘Group Policy Management’ tool
2. Right-click ‘Servers’ and click ‘Create new GPO, and link it here’
3. Type ‘Enable Signing’ in the Name box and click ‘ok’
4. Right click the new policy and click ‘edit’
5. Under computer config
   1. Open Policies > Windows Settings > Security Settings > Local Policies > Security Options
6. Now look for:
   1. Microsoft network client: Digitally sign communications (always)
   2. Microsoft network server: Digitally sign communications (always)
   3. Network security: LDAP client signing requirements
7. Once these are enabled close the policy editor and right click ‘workstations’
8. Click ‘Link Existing GPO’
9. Look for the one called ‘Enable Signing’ then click ‘ok’

## Protect from Kerberoasting with a domain-controller policy

1. Open ‘Group Policy Management’
2. Right-click ‘Domain Controllers’
   1. Be sure to add this policy to DC’s as that is what kerberoasting targets
3. Click ‘Create new GPO, then link it here’ name it ‘Anti-Kerberoast’
4. Right-click the new policy and check the enforce box
   1. This will not allow it to be over-ran by a higher GPO
5. Now right-click again and click ‘edit’
6. Under computer config
   1. Open Policies > Windows Settings > Security Settings > Local Policies > Security Options
7. Now look for:
   1. Network security: Configure encryption types allowed for Kerberos
      1. Click Define > AES128 > AES256 > Future
      2. Click ‘Apply’
   2. Now you can close GPedit
8. Now in Group Policy Management right-click the ‘Domain Controllers’ and click ‘Update Group Policy’
   1. Or run ```gpupdate /force``` in CMD

## Protect from Token Impersonation with ‘protected users’

1. Open ‘Active Directory Users and Computers’
2. Find user in question.
   1. Open user properties.
   2. Click ‘Member of’ tab
   3. Click ‘add’ and search for ‘Protected Users’
   4. Click ‘apply
3. You will now be protected from token impersonation.