Windows Server Core 2016 Hardening and Documentation

By: John Long, Young Chen

3/11/19

NECCDC-2019

Document Description:

This document outlines useful commands for hardening Windows Server Core 2016. Since Core is literally just a terminal the commands outlined in this document will either be run from cmd.exe or powershell.exe

Escalate Privileges:

Via Powershell

```
powershell -Command "Start-Process cmd -Verb RunAs"
```

Via CMD

```
runas /user:administrator cmd
```

Disable RDP:

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 1 /f
```

Enable RDP:

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f
```

Disable Remote Assistance:

```
reg add "HKLM\SYSTEM\CurrentControlSet\Control\Remote Assistance" /v fAllowToGetHelp /t REG_DWORD /d 0 /f
netsh advfirewall firewall set rule group="Remote Assistance" new enable=no
```

Update Windows:

```
wuauclt.exe /updatenow
```

View Network Shares:

```
net share
```

Disable Network Sharing:

```
net share <SHARE_NAME>$ /DELETE
```

OR

net stop lanmanserver (Disables File Sharing on all folders on a local computer)

Type in net share and you should get the following prompt

```
C:\>net share
The Server service is not started.
Is it OK to start it? (Y/N) [Y]: n
```

Turn off a Windows Feature:

dism /online /Get-Features (Gets enabled and disabled features)

```
dism /online /Disable-Feature /<FEATURE_NAME>
```

Turn on a Windows Feature:

```
dism /online /Enable-Feature /<FEATURE_NAME>
```

Check for multiple instances of cmd.exe:

```
wmic process list brief /every:1 | find "cmd.exe"
```

Find Process ID for cmd:

```
title mycmd
tasklist /v /fo csv | findstr /i "mycmd"
```

Determine if Credential guard is configured (POWERSHELL):

```
$DevGuard = Get-CimInstance –ClassName Win32_DeviceGuard –Namespace
root\Microsoft\Windows\DeviceGuard
```

```
if ($DevGuard.SecurityServicesConfigured -contains 1) {"Credential Guard configured"}
```

Determine if Credential guard is running (POWERSHELL):

```
if ($DevGuard.SecurityServicesRunning -contains 1) {"Credential Guard running"}
```