Windows Basic Server

Alexander M. Hendren

Nova Scotia Community College, Cyber Security

PROG2022

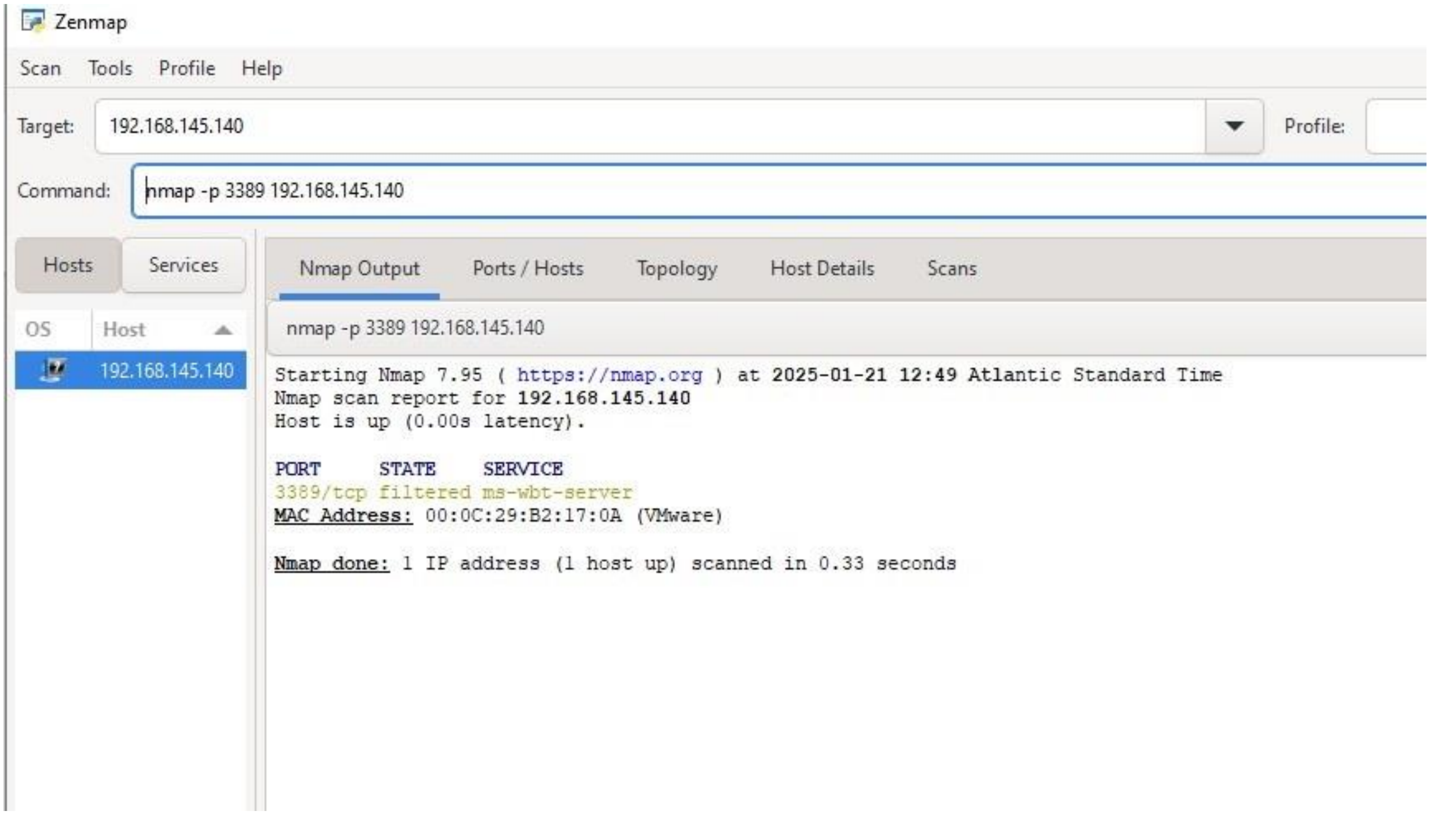
Assignment 1

January 24th, 2025

Table of Contents

Section 1: Show that Remote Desktop is disabled using Nmap

In this section, we will be doing a fresh install of Windows Server 2022. We will then be using nmap to show that the RDP port is closed or filtered. For our fresh install of Windows Server, we will be using VMware Workstation Pro to do a generic fresh install. Once our fresh install of Windows Server is done, we will check that RDP is disabled.



Target: 192.168.145.140

Command: nmap -p 3389 192.168.145.140

192.168.145.140

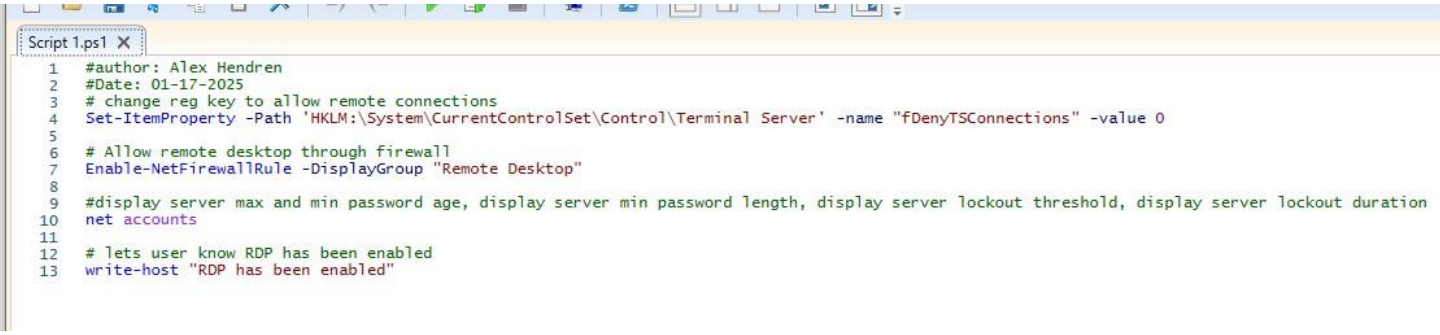
```
nmap -p 3389 192.168.145.140

Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-21 12:49 Atlantic Standard Time
Nmap scan report for 192.168.145.140
Host is up (0.00s latency).

PORT     STATE    SERVICE
3389/tcp filtered ms-wbt-server
MAC Address: 00:0C:29:B2:17:0A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
```

Figure 1. First nmap scan

In the screenshot above, we used nmap to show that the port for RDP is filtered. We did this using the command nmap -p 3389 192.168.145.140 . This command uses nmap to scan if port 3389 (the default RDP port) is open on our servers IP (192.168.145.140). Since it is filtered we can conclude that RDP is disabled on our server.

Section 2: First Powershell Script

In this section we will be creating a script that enables RDP when it is run, it will also inform the user via PowerShell that RDP has been enabled as well as display the max and min password age, the min password length, the lockout threshold and the lockout duration. We will be using PowerShell ISE to write our script.



```
#author: Alex Hendren
#Date: 01-17-2025
# change reg key to allow remote connections
Set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Control\Terminal Server' -name "fDenyTSConnections" -value 0

# Allow remote desktop through firewall
Enable-NetFirewallRule -DisplayGroup "Remote Desktop"

#display server max and min password age, display server min password length, display server lockout threshold, display server lockout duration
net accounts

# lets user know RDP has been enabled
write-host "RDP has been enabled"
```

Figure 2. First Script

In the screenshot above, we have created a PowerShell script to enable RDP, allow it to run through firewall and display the necessary information to the user. To do this we used the Set-ItemProperty command to change the “fDenyTSConnection” reg key value to 0. We set the path to where our server reg keys are kept. This enables RDP connections on our server.

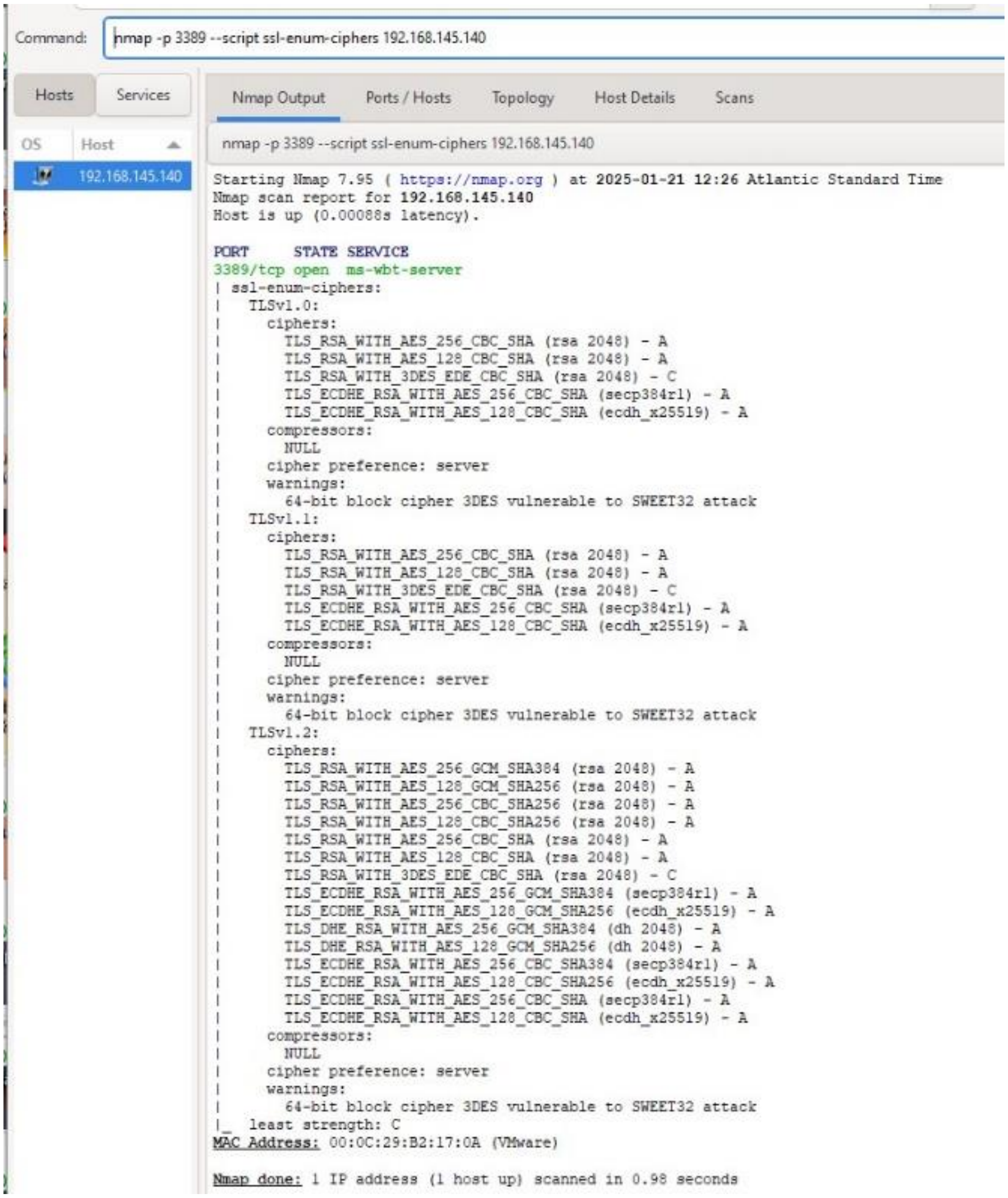
We then use the Enable-NetFirewallRule with the -DisplayGroup “Remote Desktop” parameter. This will allow incoming connections to port 3389 through the firewall.

Our next step is to use the net accounts command. This command will list the force user logoff length, the min and max password age, min password length, length of password history maintained, the lockout threshold, the lockout duration, the lockout observation window and the computer role.

Lastly, we use the write-host command to let the user know that RDP has been enabled.

Section 3: Show That RDP is Enabled Using Nmap, as well as the Default SSL/TLS Ciphers

In this section, we will be showing that RDP is enabled using nmap, as well as showing the default SSL/TLS ciphers and protocols.



Command: nmap -p 3389 --script ssl-enum-ciphers 192.168.145.140

nmap -p 3389 --script ssl-enum-ciphers 192.168.145.140

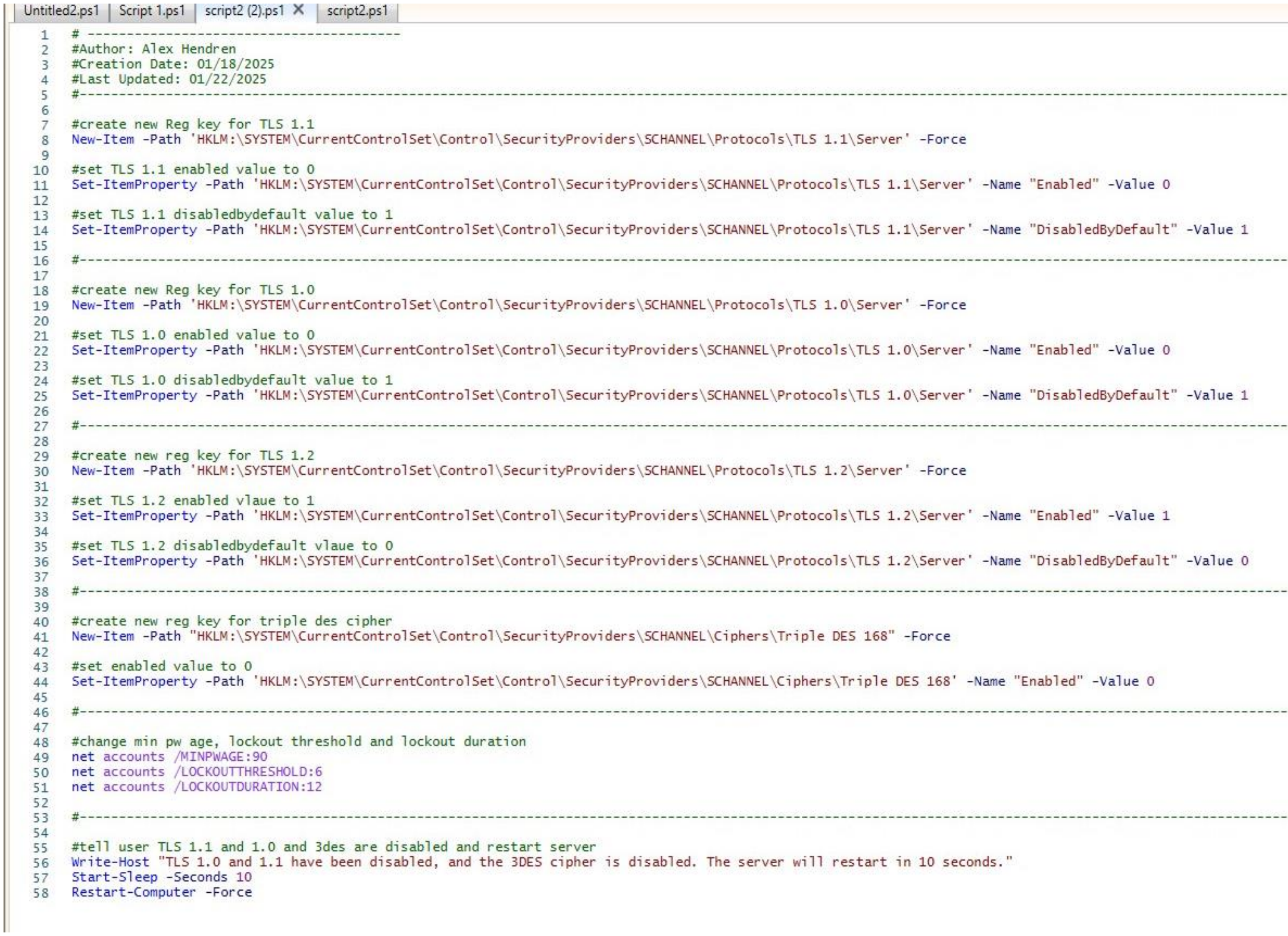
```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-21 12:26 Atlantic Standard Time
Nmap scan report for 192.168.145.140
Host is up (0.00088s latency).

PORT     STATE SERVICE
3389/tcp open  ms-wbt-server
| ssl-enum-ciphers:
|   TLSv1.0:
|     ciphers:
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp384r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - A
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|   TLSv1.1:
|     ciphers:
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp384r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - A
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|   TLSv1.2:
|     ciphers:
|       TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp384r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (ecdh_x25519) - A
|       TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 2048) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp384r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp384r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - A
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|_  least strength: C
MAC Address: 00:0C:29:B2:17:0A (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.98 seconds
```

Figure 3. Second nmap Scan

To do this, we use the command nmap -p 3389 –script ssl-enum-ciphers 192.168.145.140 to show that RDP has been enabled. The parameter -p 3389 specifies the port 3389 (RDP port) and uses the script ssl-enum-ciphers to show the default ciphers as well.

Section 4: Hardening RDP and the Server

In this section, we will be hardening the remote desktop protocol as well as the server. To do this we will be creating a second PowerShell script that will disable TLS 1.0 and 1.1, create a new registry key for TLS 1.2 and enable it, as well as disable the 3DES cipher and finally will change the lockout threshold, lockout duration and the min password age.



```
# ---------------------------------------
#Author: Alex Hendren
#Creation Date: 01/18/2025
#Last Updated: 01/22/2025
#--------------------------------------------------------------------------------------------------------------------------------------------

#create new Reg key for TLS 1.1
New-Item -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server' -Force

#set TLS 1.1 enabled value to 0
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server' -Name "Enabled" -Value 0

#set TLS 1.1 disabledbydefault value to 1
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server' -Name "DisabledByDefault" -Value 1

#--------------------------------------------------------------------------------------------------------------------------------------------

#create new Reg key for TLS 1.0
New-Item -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server' -Force

#set TLS 1.0 enabled value to 0
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server' -Name "Enabled" -Value 0

#set TLS 1.0 disabledbydefault value to 1
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server' -Name "DisabledByDefault" -Value 1

#--------------------------------------------------------------------------------------------------------------------------------------------

#create new reg key for TLS 1.2
New-Item -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server' -Force

#set TLS 1.2 enabled vlaue to 1
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server' -Name "Enabled" -Value 1

#set TLS 1.2 disabledbydefault vlaue to 0
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server' -Name "DisabledByDefault" -Value 0

#--------------------------------------------------------------------------------------------------------------------------------------------

#create new reg key for triple des cipher
New-Item -Path "HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\Triple DES 168" -Force

#set enabled value to 0
Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\Triple DES 168' -Name "Enabled" -Value 0

#--------------------------------------------------------------------------------------------------------------------------------------------

#change min pw age, lockout threshold and lockout duration
net accounts /MINPWAGE:90
net accounts /LOCKOUTTHRESHOLD:6
net accounts /LOCKOUTDURATION:12

#--------------------------------------------------------------------------------------------------------------------------------------------

#tell user TLS 1.1 and 1.0 and 3des are disabled and restart server
Write-Host "TLS 1.0 and 1.1 have been disabled, and the 3DES cipher is disabled. The server will restart in 10 seconds."
Start-Sleep -Seconds 10
Restart-Computer -Force
```

Figure 4. Second PowerShell Script

The screenshot above shows our second PowerShell script. This script uses the new-item command to create a new registry key for TLS 1.1, the -force parameter is used to overwrite any existing keys. We then use the set-item property to change the enabled value to 0 and the disabled value to 1, this disables TLS 1.1 and makes it disabled by default. We then repeat these three commands for TLS 1.0 as well.

We then do the same process for TLS 1.2, except we change the enabled value to 1 and the disabledbydefault value to 0, this enables TLS 1.2 and sets TLS 1.2 to be enabled by default.

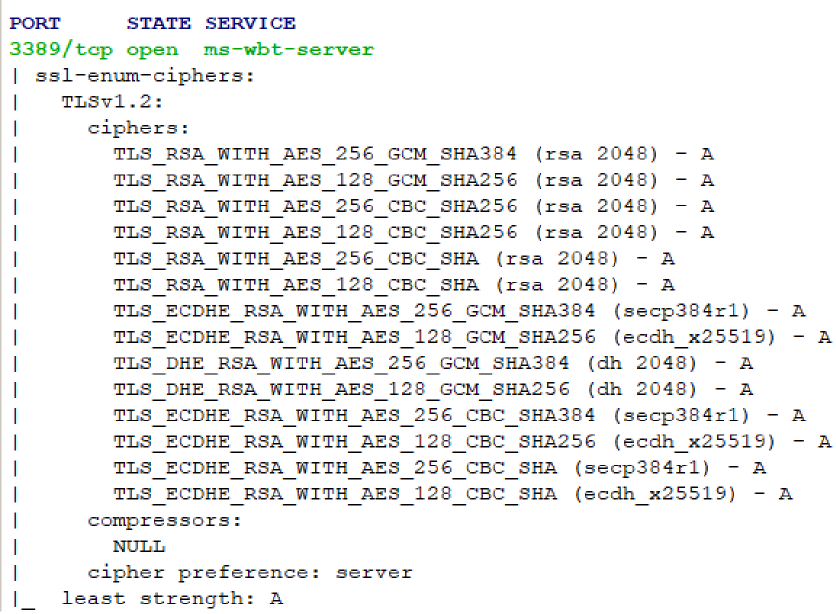
We then use the new-item command again to create a new registry key for Triple DES 168. We must make sure the path we are using leads to \Ciphers, and not \Protocols which is what we used for the TLS registry keys. We then change the enabled value for Triple DES 168 to 0, which will disable the 3DES cipher from TLS 1.2.

The next set of commands in our script will change the server's lockout threshold, lockout duration and minimum password age. To do this we use the net accounts command, followed by what we want to change. Net accounts /MINPWAGE will change the minimum password age, net account /LOCKOUTTHRESHOLD will change the lockout threshold and net accounts /LOCKOUTDURATION will change the lockout duration.

Lastly, we use the write-host command to let the user know we have disabled 3DES, TLS 1.1 and TLS 1.2. We use the start-sleep command with the parameter -seconds 10 to suspend the script for 10 seconds, and then the restart-computer command with the -force parameter to finally restart the server.

Step 4. Confirmation

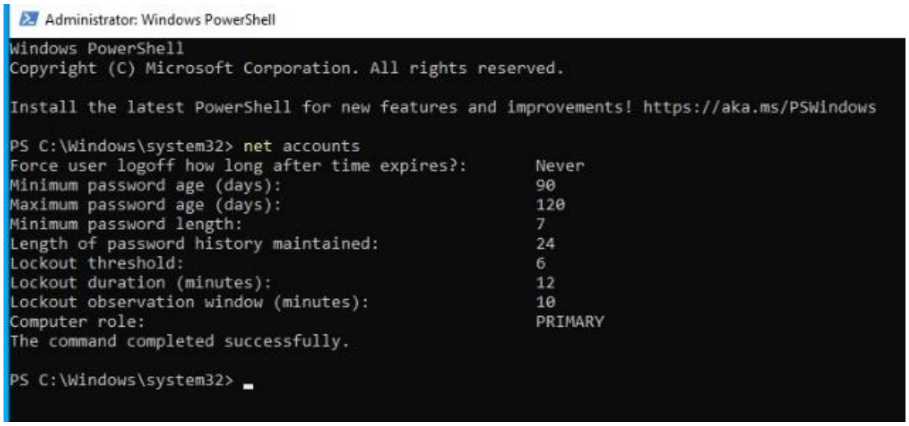
In this section we will be using nmap to confirm that RDP only accepts TLS 1.2 connections, as well as showing the new lockout threshold. Lockout duration and minimum password age.



```
PORT     STATE SERVICE
3389/tcp open  ms-wbt-server
| ssl-enum-ciphers:
|   TLSv1.2:
|     ciphers:
|       TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (secp384r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (ecdh_x25519) - A
|       TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (dh 2048) - A
|       TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (dh 2048) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (secp384r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (ecdh_x25519) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (secp384r1) - A
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (ecdh_x25519) - A
|     compressors:
|       NULL
|     cipher preference: server
|_  least strength: A
```

Figure 5. Third nmap Scan

The screenshot above is the nmap results for our scan to confirm RDP only accepts TLS 1.2 connections. To do this we use the same nmap command we used for the last nmap scan which is nmap -p 3389 –script ssl-enum-ciphers 192.168.145.140. The results of this scan show that our server is only accepting TLS 1.2 connections, and that the 3DES cipher is not enabled.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Windows\system32> net accounts
Force user logoff how long after time expires?:       Never
Minimum password age (days):                          90
Maximum password age (days):                          120
Minimum password length:                              7
Length of password history maintained:                24
Lockout threshold:                                    6
Lockout duration (minutes):                           12
Lockout observation window (minutes):                 10
Computer role:                                        PRIMARY
The command completed successfully.

PS C:\Windows\system32> _
```

Figure 6. PowerShell Results

In the screenshot above, we have shown our new password policies. To do this we use PowerShell to show the new lockout threshold, lockout duration and minimum password age. To do this we use the command net accounts. By looking through our results, we can see that the new minimum password age is 90, the lockout duration is 12 minutes, and the lockout threshold is 6.