Assignment 1 - Windows Basic Server

Your task will be to create two PowerShell scripts to run on a fresh install of Windows Server 2019 or 2022 Standard (Desktop Experience). Each script must be well-commented so that anyone can read these scripts and understand every action being taken. You will also provide before and after pictures regarding some of the configuration.

Note: that because we are making configuration changes to the machine, you will have to run your scripts from an elevated command prompt.

Note: Your server's execution policy (the policy that allows scripts to be run) may be set to restricted by default. If you get an error message while trying to run your scripts about running scripts being disabled, you will have to change your execution policy. You can change your execution policy to LocalRemote (which only allows scripts not downloaded from the Internet to be run) using the command below. It is not recommended, from a security standpoint, to set your execution policy to unrestricted.

```
Set-ExecutionPolicy RemoteSigned
```

Step 1: Observe the default configurations

1. Do a fresh install of Windows server
2. Show that Remote Desktop is disabled or filtered using Nmap

Step 2: First PowerShell Script

1. Create a script that when you run it enables RDP. It should inform the user via the PowerShell console that RDP has been enabled after the user runs it.
2. Show that RDP is enabled using Nmap, as well as the default SSL/TLS ciphers and protocols

Step 3: Hardening RDP

1. Create a second PowerShell script that creates new registry keys to disable TLS 1.0 and 1.1 as a server (not client), as well as setting them to be disabled by default
2. The script should also create registry keys to set TLS 1.2 to be enabled and enabled by default
3. The script should then disable the 3DES cipher from TLS 1.2 with PowerShell
4. The script should then inform the user running it that TLS 1.0 and 1.1 have been disabled, and the 3DES cipher is disabled. It should also inform the user that the server will restart in 10 seconds
5. Lastly, the script should restart the server after 10 seconds

Step 4: Confirmation

1. Use Nmap to confirm that RDP only accepts TLS 1.2 connection, and doesn't list the 3DES cipher as a cipher

Rubric:

All submissions must be in PDF Format

Item	Requirements	Score			
		Excellent (8-10)	Satisfactory (5-7)	Minimal Understanding (1-4)	Did Not Attempt (0)
Script 1 (Total: 10)	Are all objectives met?				
Script 2 (Total: 15)	Are all objectives met				
Script Quality (Total: 5)	Are scripts properly commented? Do scripts give alerts after being run?				
Report Quality (Total: 10)	Are all pieces of before-and-after evidence included in the report? Does the report explain the objectives and outcomes effectively? Are there spelling or grammar mistakes?				
Total /40					