Assignment 2 - Active Directory

This assignment will be split up into 2 parts.

For the first part, you will modify your existing Win-RM GPO to accept traffic over HTTPS. To do so, you will need to create a certificate authority on your DC. You can consult the SSL Certificates slide deck in Module 2 on Brightspace on how to set this up. You will also be using Wireshark to gain evidence on Win-RM commands being sent over HTTP and HTTPS. Wireshark will mimic an adversary-in-the-middle attack between your DC and workstation. If you've never used Wireshark before, you can consult the Wireshark slide deck in Module 2 of Brightspace. You must complete the following objectives, and provide screenshots for every step taken along with a brief description for each screenshot. You do not need to provide any screenshots for setting up your certificate authority. You should not log in or run any commands from your workstation except for "gpupdate /force", all other commands should be done on your DC or via Win-RM for your workstation.

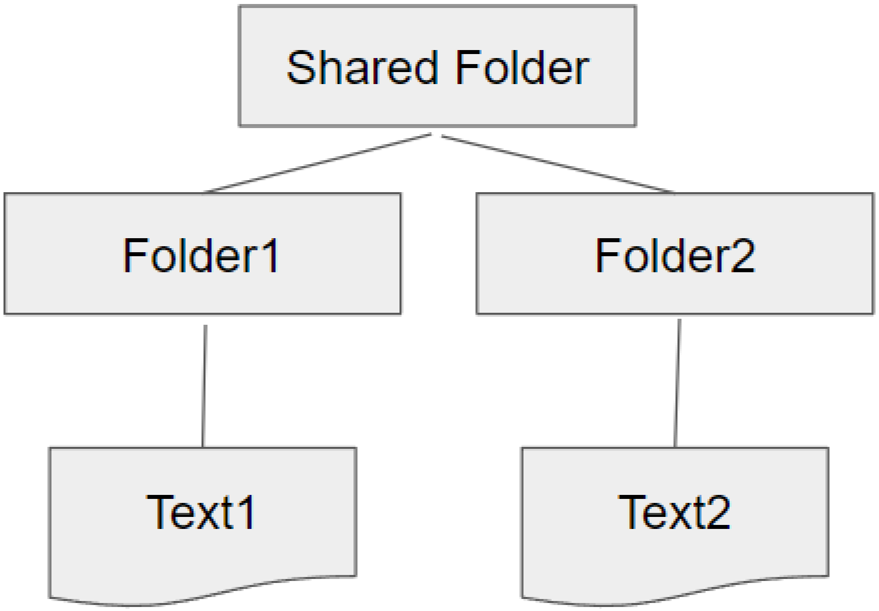
1. Use the Invoke-Command PowerShell command to run the "hostname" and "whoami" commands over Win-RM over HTTP from your DC to your workstation at the same time. Both commands must be run in a single line using Invoke-Command. Use Wireshark to capture the traffic and show that Win-RM is running over HTTP.
2. Edit your Win-RM GPO to allow Win-RM traffic over HTTPS.
3. Use the Enter-PSSession command from your DC to configure your Workstation to accept Win-RM traffic over HTTPS.
4. Edit your Win-RM GPO to disallow Win-RM HTTP traffic
5. Run the same Invoke-Command commands in Step 1 using SSL and capture the traffic with Wireshark. Show that the traffic is going over HTTPS.

The second step will involve file-sharing over your domain. You will complete the following objectives providing screenshots and brief descriptions for each screenshot.

1. You will first create 2 groups and create 2 Domain Users, and place one user in one group and the other user in the other group. The Users must be called User1 and User2, and the groups Group1 and Group2.
2. You will then create a folder structure on your DC's C drive and share it. You may call this folder whatever you'd like. Generally, you do not want to place a shared folder in any User's folders, so the C drive is a good place. DO NOT share the entire C drive. The folder will then have 2 folders inside called Folder1 and Folder2. Inside Folder 1 and Folder 2 will be a text document called Text1.txt and Text2.txt. Place "Text1" as content for Text1.txt, and "Text2" and content for Text2.txt Consult the figure below the objectives.
3. You will then configure Folder1 to have read/write permissions from members of Group 1, and Folder2 to only have read permissions for members of Group2.
4. You will logon to your workstation as User1 and show that you can access Text1.txt in Folder1. You will also write a new text document called Text3 and save it to the folder.

You can write whatever content you'd like for Text3, but must show that it has been saved in Folder1. You will then show that you do not have access to Folder2.

5. You will then login to your workstation as User2 and show that you have access to read Text2.txt in Folder2. You will then attempt to write a new text document to this folder, and show that you cannot. Also show that you cannot access Folder1.



Rubric:

<u>All submissions must be in DOCX or PDF Format</u>

Item	**Requirements**	**Score**			
		Excellent	Satisfactory	Minimal Understanding	Did Not Attempt
Part 1 (Total: 15)	Are all objectives met? Are all necessary screenshots present? Are all screenshots explained?	(11-15)	(6-10)	(1-5)	(0)
Part 2 (Total: 15)	Are all objectives met? Are all necessary screenshots present? Are all screenshots explained?	(11-15)	(6-10)	(1-5)	(0)
Report Quality (Total: 10)	Does the report explain the objectives and outcomes effectively? Are there spelling or grammar mistakes?	(8-10)	(5-7)	(1-4)	(0)
Total /40					