Name: John Ryan C. Paderna

Date Started: September 15, 2023

Date Finished: September 17, 2023

LAB 1: Encrypting Files from the Command Prompt

Objectives:

STEP 1. Power up the VM
STEP 2: Encrypt a file using the command line utility using cipher.

Requirements:

1. Screen shots all the windows configuration from Step 1 to Step 2. 2. Label the necessary result in the configuration.

3. Display the Final Result for each Steps.

4. Answer all the questions.

Background / Scenario

The best defense for privacy of data, in transit or in storage, is solid encryption built on top of a solid identification/authentication/authorization process.

The widespread use of laptop computers in business has brought serious data loss problems. Laptops are lost or stolen frequently, and once an attacker has physical possession of a computer, it is a simple matter to bypass the authentication system by placing the laptop's hard drive into another computer on which the attacker has full rights and permissions. Full disk encryption is becoming a popular method for securing data stored on laptops.

Microsoft systems now support the Encrypting File System (EFS), which allows the encryption of folders and files and, full drive encryption using BitLocker.

After completing this lab, you will be able to:

1. **The use of digital certificate in EFS.**
2. **Encrypt files from a command prompt.**

Note: You will need installation privileges and some knowledge of the process to install Windows server 2012 R2.

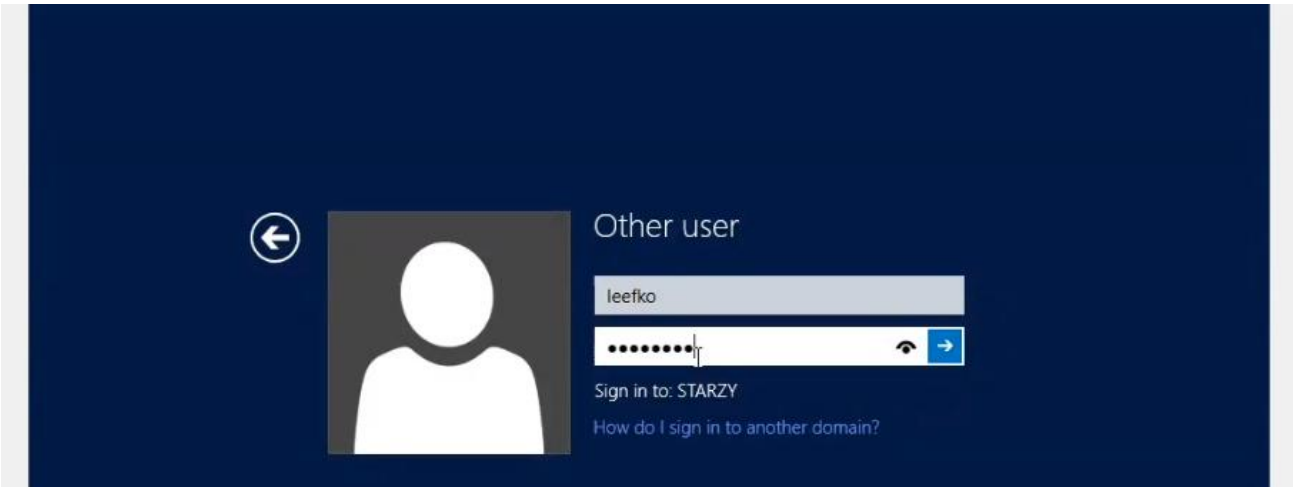
Required Resources

- **PC**
- **VM Virtual Manager**
- **Windows Server 2012 R2**

STEP 1. Power up the VM

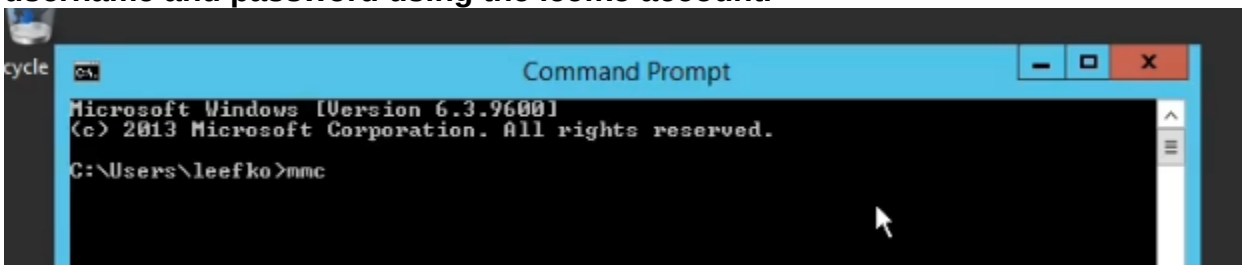
1. Power the Virtual Box by clicking Start, then run the Server.

2. Click the Start window, log in to leefko and provide the Password

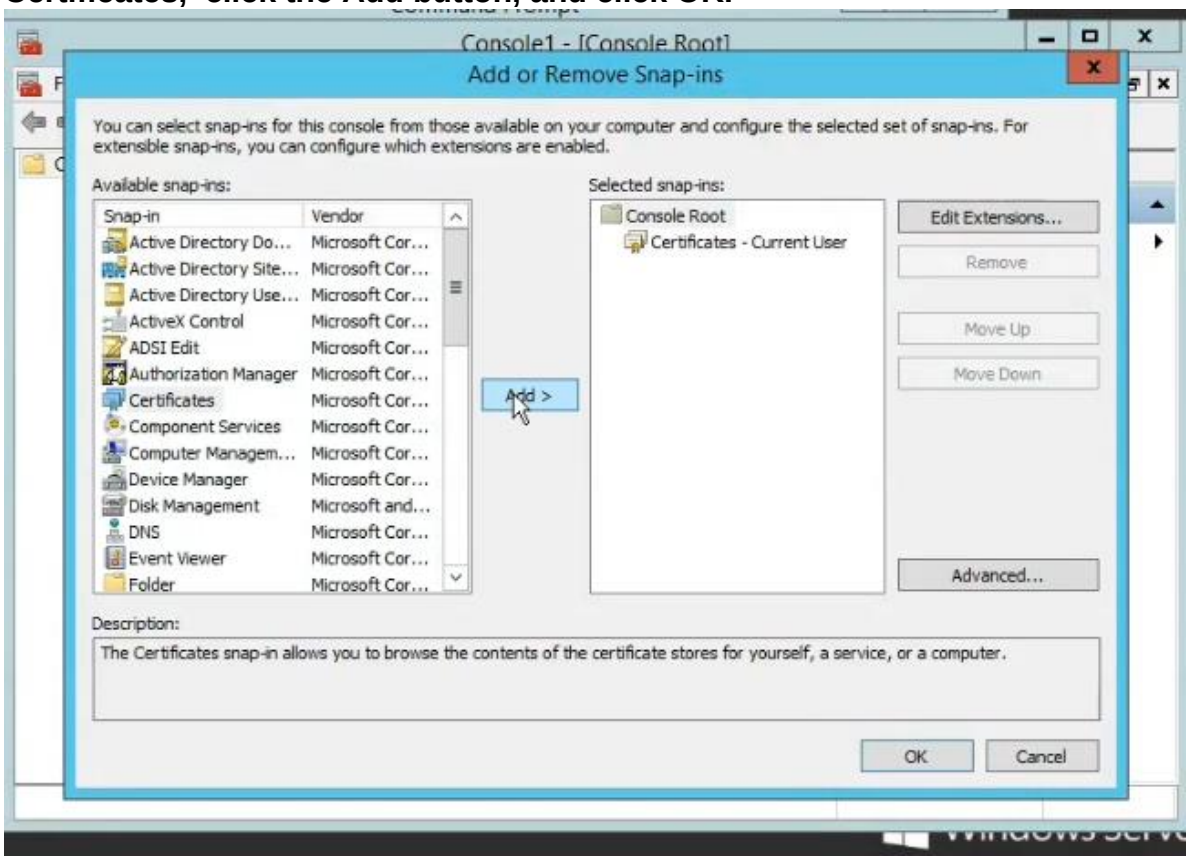


STEP 2: Encrypt a file using the command line utility using cipher.

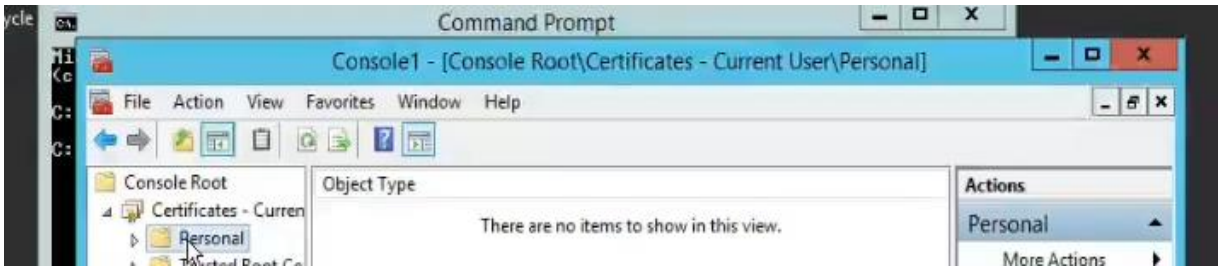
1. **Open a Windows PowerShell, type mmc, and then press Enter. Provide the username and password using the leefko account.**

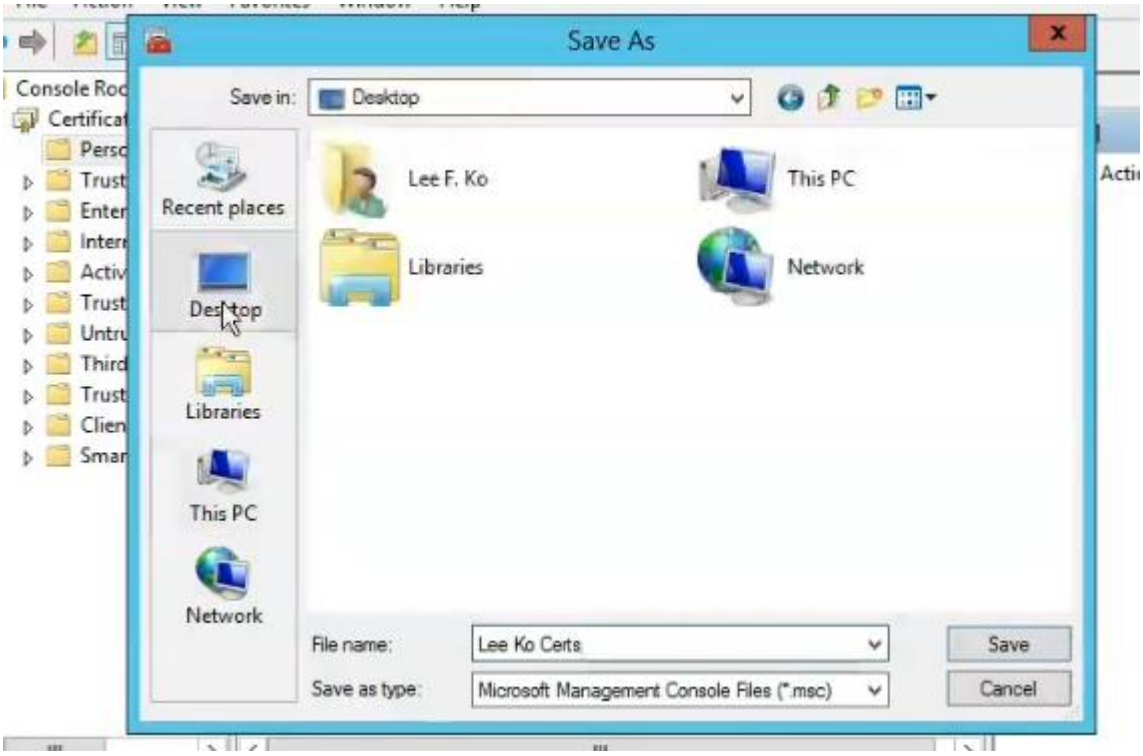


2. **In the Console 1 window, from the File menu, click Add/Remove Snap-in. In the Add or Remove Snap-ins window, in the Available snap-ins box, select Certificates, click the Add button, and click OK.**

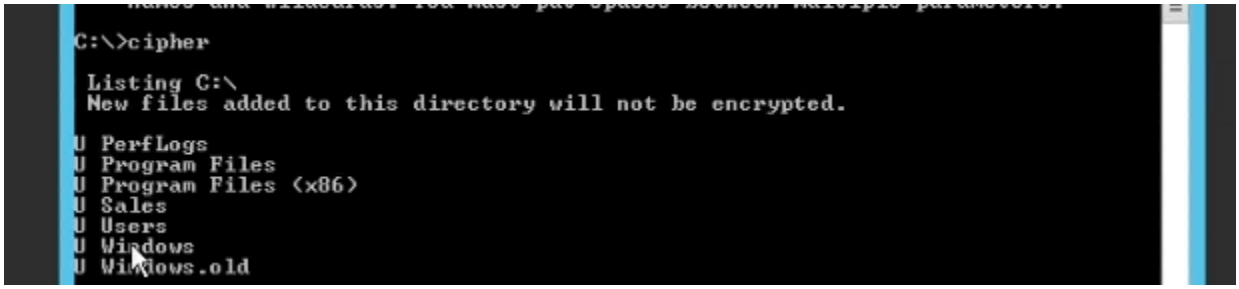


3. **In the Console l window, expand the Certificates node in the left pane and select the Personal folder. The Object Type pane in the middle indicates that there are no items to show. From the File menu, click Save As; in the File name box, type Lee Ko Certs, click the Desktop icon to direct the file to your desktop, and click Save. Close the Lee Ko Certs console.**

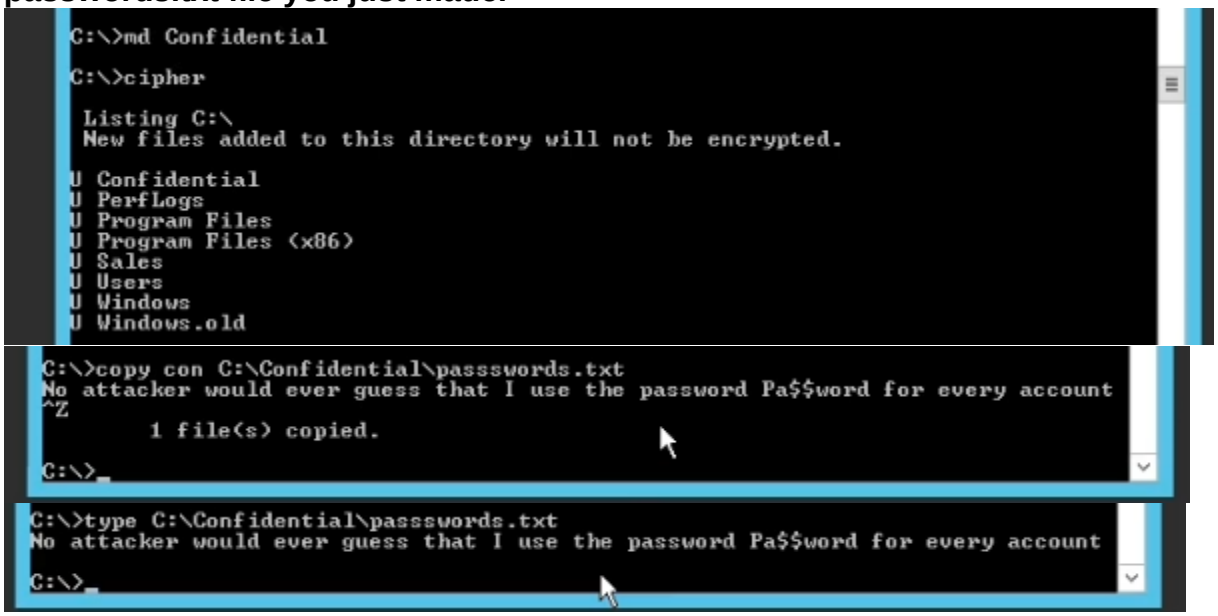




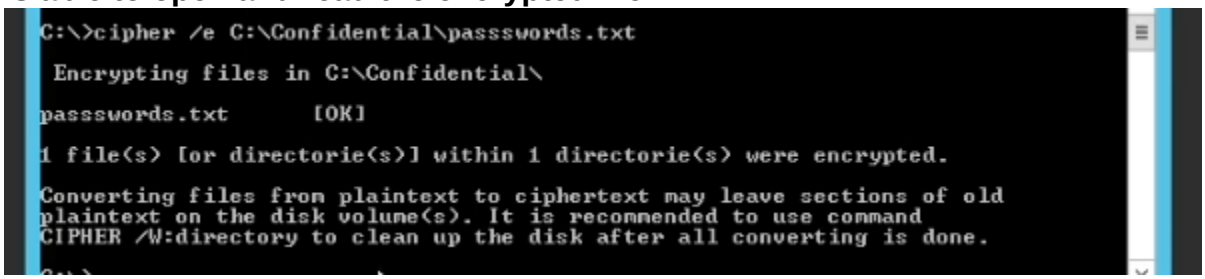
4. **Access the command prompt, on Click Start Window, type cmd (command prompt) then Enter. Navigate to the root of c: by typing cd\ and pressing Enter. Type cipher /?, press Enter, review the syntax and options used by the cipher command. Type cipher and press Enter. The "U" indicates that the items listed are uncrypted.**

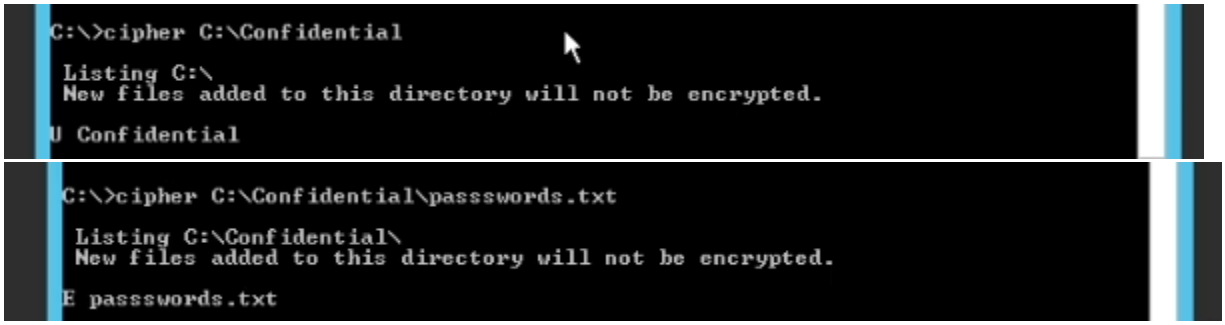


5. Type **md Confidential** and press Enter. Use the cipher command again to determine the encryption status of the Confidential directory. It should be unencrypted. Type **copy con C:\Confidential\passwords.txt** and press Enter. Type **"No attacker would ever guess that I use the password Pa$$word for every account"**. Press Enter followed by **Ctrl+z**, and then press **Enter** again. Type **type C:\Confidential\passwords.txt** and press Enter. You should see the content of the passwords.txt file you just made.



6. Type **cipher /e C:\Confidential\passwords.txt** and press **Enter**. When the encryption process has completed, type **cipher C:\Confidential** and press **Enter**. The directory C:\Confidential is still unencrypted. Type **cipher C:\Confidential passwords.txt** and press Enter. The "**E**" indicates that the passwords.txt file has been encrypted. Type **type C:\Confidential passwords.txt** and press **Enter**. Lee Ko is able to open and read the encrypted file.

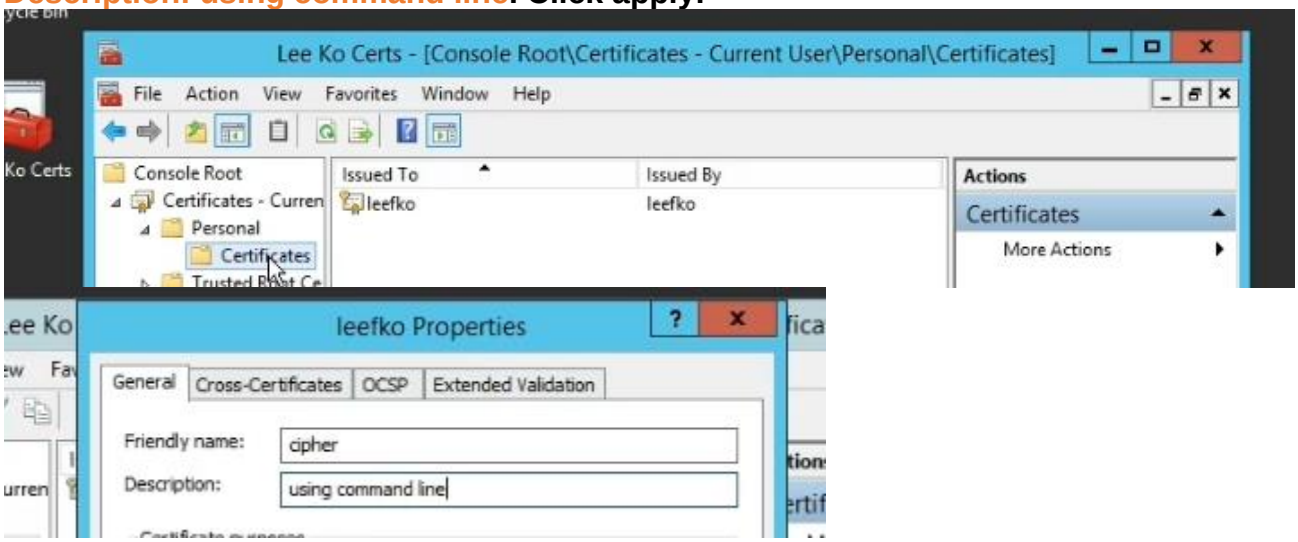




How can this be if the file is encrypted?

If it is encrypted, the authorized user must only be able to open it since the concept of encryption in the context of cryptography is using keys to open an encrypted file.

7. **From the desktop, open Lee Ko Certs. If necessary, expand the Certificates node, and expand the Personal folder. It has changed from its state in Step 3. Click the Certificates folder inside the Personal folder. Double-click the leefko digital certificate in the middle pane. Right click the certificate, then properties, in the General tab, determine the purpose of this certificate Friendly name: cipher Description: using command line. Click apply.**



Click the link certificates in Learn more about certificates, and then read the three articles: Using Certificates, Public and Private Keys, and Certificate File Formats.

Examine the information provided on the Details and Certification Path tabs of leefko digital certificate.

8. Close all windows (Click Yes when asked to save console settings to Lee Ko Certs) and log off.