Name: ____John Ryan Paderna_____

Date Started: ____October 23, 2023____

Date Finished: ____October 23, 2023____

LAB 2: Demonstrating Encryption Security

Objectives:

STEP 1. Power up the VM
STEP 2: Create a Security of the file you encrypted in Lab 1M.

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 Encrypting File System is not, strictly speaking, a file system, due to the fact that it does not track data location. (A file system is a scheme by which the operating system and the BIOS [Basic Input/Output System] track where data is located on storage media.) Instead, it uses asymmetric and symmetric encryption to increase data confidentiality. When a user encrypts a file, a File Encryption Key (FEK) is generated. This is a symmetric key; it both encrypts and decrypts the file. Once the file is encrypted, one copy of the FEK is encrypted using the user's public key, and the encrypted FEK is attached to the file. Another copy of the FEK is encrypted using the recovery agent's public key and is also attached to the file. Thus, only someone who has access to either the user's private key or the recovery agent's private key would be able to decrypt the file.

After completing this lab, you will be able to:

1. Demonstrate how the EFS protects data from unauthorized users.
2. Obtain information regarding the certificated that are associated with an encrypted file.
3. Explain how asymmetric and symmetric encryption is used by EFS. 4. Use the run as command to assume the credentials of different users in order to test configurations.

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 raintree and provide the Password

STEP 2: Create a Security of the file you encrypted.

1. Open a command prompt. Navigate to C:\Confidential. Type dir and press Enter to verify that the passwords.txt file is in the C:\Confidential directory. Type type passwords.txt and press Enter.

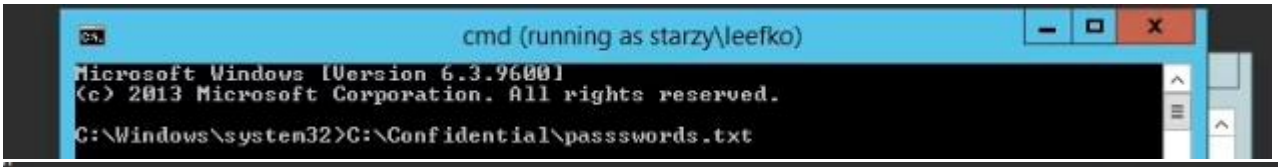
What result did your get? Why?

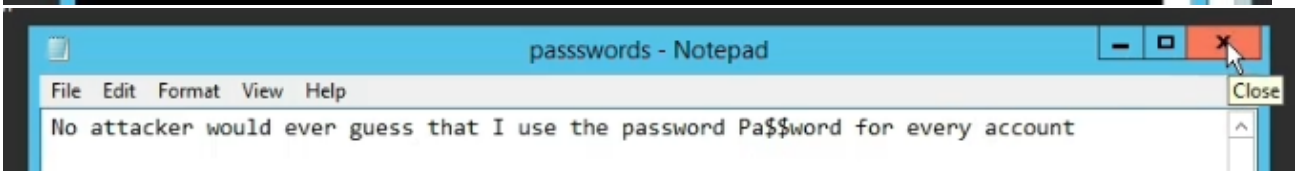
The passwords.txt file or even the C:\Confidential directory is not accessible by raintree since this is encrypted by leefko.

2. Type C:\Confidential\runas /user:starzy\leefko cmd and press Enter. Type the password of leefko and press Enter. raintree cannot open the passwords.txt file because it was encrypted using a file encryption key that itself has been encrypted

using leefko's public key. By switching to leefko's credentials, the proper private key becomes available.

3. In the new command prompt, navigate to C:\Confidential and type type passwords.txt and press Enter. The file now opens. Note that only the program launched using the runas command--the md program in this case recognizes leefko as having been authenticated. Any other programs running in raintrees' desktop, including the first command prompt, are only aware of raintree as having been authenticated.



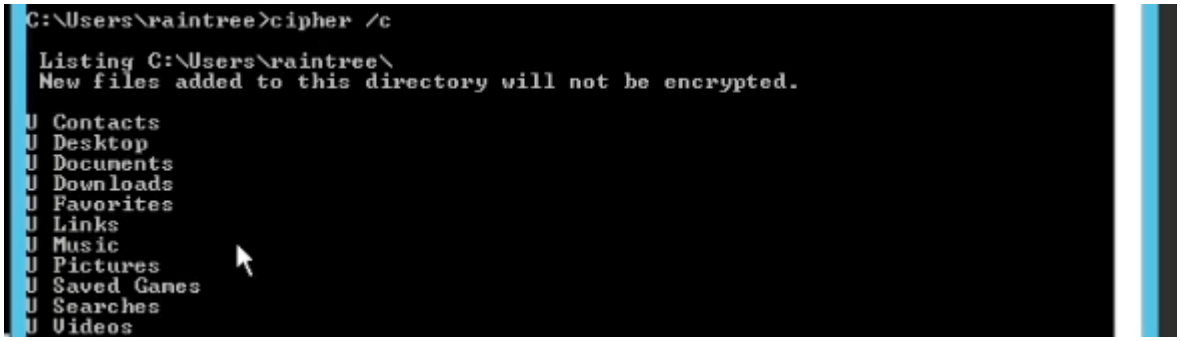


4. In the original command prompt, try the type passwords. txt command again.

What was the result? Why?

The result was still not accessible by raintree since only the program launched using the runas command--the md program in this case recognizes leefko as having been authenticated

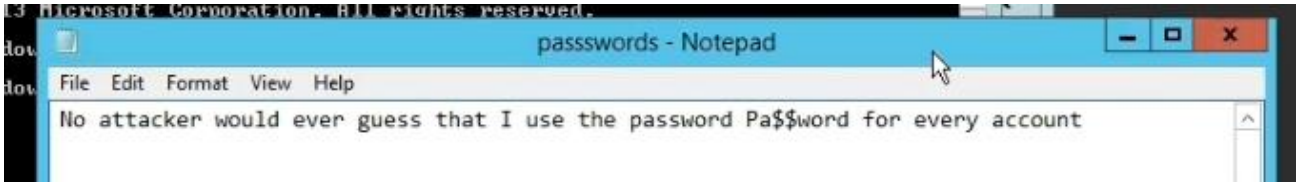
6. Type cipher /c and press Enter.



Why is there more than one user account that can decrypt the passwords.txt file? Explain.

Because as long as the user recognizes as having been authenticated it can decrypt the passwords.txt file.

7. Type C:\Confidential\runas /user:starzy\administrator cmd and press Enter. Type the password of the administrator and press Enter. In the new command prompt, change directories to C:\Confidential then type passwords. txt and press Enter.



Why can't the administrator decrypt passwords.txt?

In the performed procedure, administrator can actually decrypt the passwords.txt file. Since it recognized the user as having been authenticated.

8. Close all windows and log off.