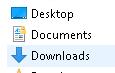
SECTION 1: Hands-On Demonstration

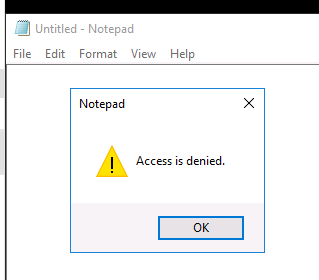
Part 1. Configure Microsoft Encrypted File System (EFS)

1. encrypted Documents folder (screen capture):



Part 2. Test the EFS Security

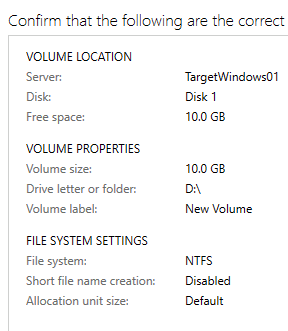
1. Notepad and the error message (screen capture):



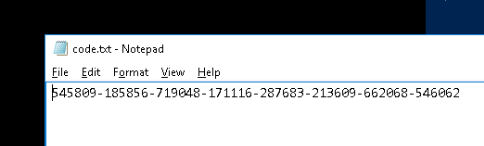
Part 3. Configure BitLocker

1. the assigned drive letter: D

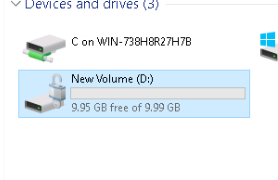
1. the settings on the Confirm selections page (screen capture):



1. Notepad and the BitLocker recovery key (screen capture):



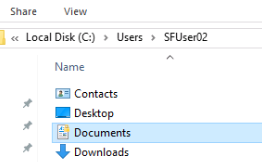
1. This PC folder with the unlocked drive (screen capture):



SECTION 2: Applied Learning

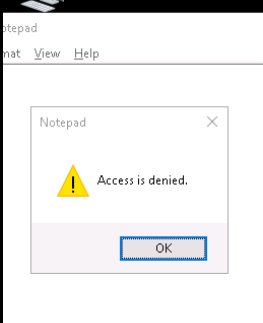
Part 1. Configure Microsoft Encrypted File System (EFS)

1. encrypted Documents folder (screen capture):



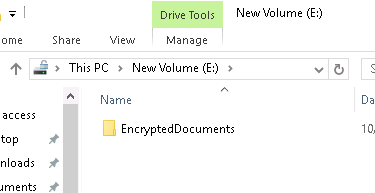
Part 2. Test the EFS Security

1. Notepad and the error message (screen capture):

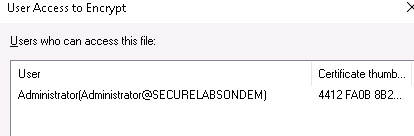


Part 3. Configure BitLocker

1. unlocked E: drive in the File Explorer (screen capture):



1. user access details for the Encrypt folder (screen capture):



SECTION 3: Observation Summary

We use RDP to connect to the network as SFUser01. We navigate to the Documents folder and create a text file named “anil\_SFfile” and we write a sentence in it. Then we encrypt the contents of the “Documents” folder.   
  
We use RDP to connect to the network as SFUser02. We navigate to the Documents folder of SFUser01 and try to open “anil\_SFfile” file.  
  
We go to the server manager to create a new volume of drive with the letter “D” using the 10GB disk with the default options. We install bitlocker using Windows PowerShell. We then connect to the network using the “Administrator” user, lock the D drive, generate the Bitlocker recovery key and paste it on a notepad. Then we unlock the D drive with the key.  
  
We connect to the network using the SFUser02. We navigate to the Documents folder. We create a text file with the name ”anil\_SFfile\_S2” and write some text in it and then encrypt it.   
  
We RDP into the second network and open server manager. We bring the Disk 1 online. We create a new volume. We create a VHD (virtual hard disk). We initialize the new disk. Create and format a new volume. We create a folder in Disk 2 named EncryptedDocuments. Then we turn on the bitlocket for This disk. We reconnect to the network, remount the E drive, and navigate to it. Then we encrypt the folder that contains the BitLocker key. This way only administrator who knows the password can access it.