Lab 5: File/Disk Encryption

Windows 7 login: Password: napier, Kali login: User: root, Password: toor

1 TrueCrypt

No	Description	Result
1	Go to your Windows 7 instance. Now **Create a new volume** and use an **encrypted file container** (use c:\tc_*yourname*) with a Standard TrueCrypt volume. When you get to the Encryption Options, run the tests and outline the results:	CPU (Mean) AES: AES-Twofish: AES-Two-Seperent Serpent -AES Serpent: Serpent-Twofish-AES Twofish: Twofish-Serpent: Which is the fastest: Which is the slowest:
2	Select AES and RIPMD-160 and create a 100MB file. Finally select your password and use FAT for the file system.	What does the random pool generation do, and what does it use to generate the random key?
3	Now mount the file as a drive (such as an X: drive).	Can you view the drive on the file viewer and from the console? [Yes][No]

4	Create some files your TrueCrypt drive and save them. Next dismount your drive, and copy the file to the provided USB stick. Give the USB stick to your neighbour, and see if they can view the file contents.	Without giving them the password, can they read the file? With the password, can they read the files?
5	Now ZIP up your TrueCrypt file, and create a share for it, such as using: http://www.filedropper.com/index.php Now go to your Kali instance and start-up TrueCrypt and mount your TrueCrypt volume into one of the slots.	Which slot have you used: On Kali, are you able to view the files on the TrueCrypt volume:
6	Next add new files to your TrueCrypt volume on Kali, and share the file. Go to your Windows 7 instance, and re-mount the new file.	Can you view the files created on your Windows 7 instance? [Yes][No]

2 TrueCrypt Volumes

The following files have the passwords of “Ankle123”, “foxtrot”, “napier123”, “password” or “napier”. Determine the properties of the files defined in the table:

File	**Size**	**Encryption type**	**Key size**	**Files/folders on disk**	**Hidden partition (y/n)**	**Hash method**
http://asecuritysite.com/tctest01.zip						
http://asecuritysite.com/tctest02.zip						
http://asecuritysite.com/tctest03.zip						

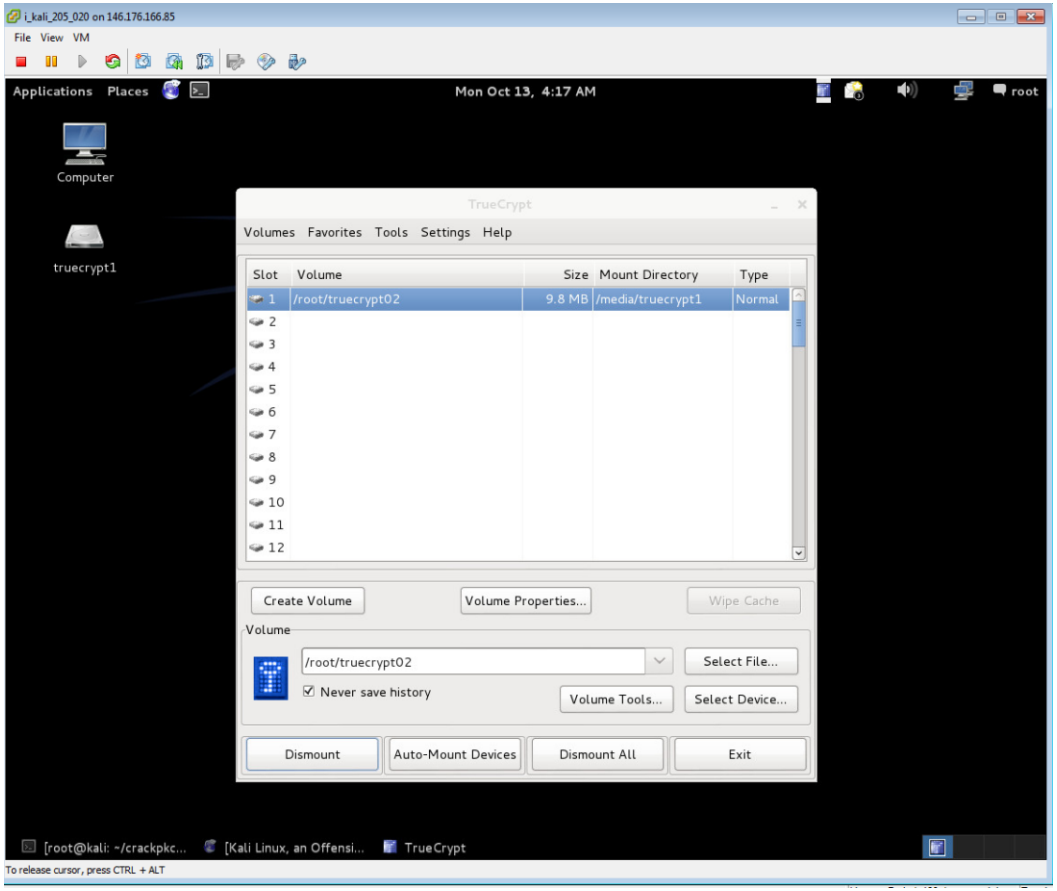

Figure 1: Kali mount

3 EFS

Undertake the following.

No	Description	Result
1	Go to your Windows 7 instance. Now create a folder named: **My_Enc_*yourname*** Add some files to the folder, and then right click on the folder and encrypt it.	How does the name of the folder change when it is encrypted?
2	Now use: Cipher /u	Which files are encrypted on your drive:
3	Using: Cipher /c *filename*	Which encryption type and key size has been used for the file encryption?
4	Make sure you can view your files. Now export your certificates with: Cipher /r:*filename*	Which are the names of the files created? View the CER and PFX file. What is the difference between the two files?
5	Go to Control Panel -> Internet Options Then click on the Content tab and select the Certificates button.	Outline some of the details of the EFS certificate. When does it expire?

	Now view your EFS certificate.	What type of encryption does it use? What is the length of the encryption key? Who has signed it?
6	Now delete the EFS certificate from the store and reboot your instance.	After reboot, can you access your files? [Yes][No]
7	Now import the PFX certificate that you created.	Can you access your files? [Yes][No]

4 EFS (with USB)

Undertake the following, but this time mount a USB stick, and encrypt on the USB device. First delete your existing EFS certificate.

No	**Description**	**Result**
1	Go to your Windows 7 instance. Now create a folder named: **My_Enc_*yourname*** Add some files to the folder, and then right click on the folder and encrypt it.	How does the name of the folder change when it is encrypted?
2	Now use: Cipher /u	Which files are encrypted on your USB disk:

3	Using: Cipher /c *filename*	Which encryption type and key size has been used for the file encryption?
4	Make sure you can view your files. Now export your certificates with: Cipher /r:*filename*	Which are the names of the files created? View the CER and PFX file. What is the difference between the two files?
5	Go to Control Panel -> Internet Options Then click on the Content tab and select the Certificates button. Now view your EFS certificate.	Outline some of the details of the EFS certificate. When does it expire? What type of encryption does it use? What is the length of the encryption key? Who has signed it?
6	Now delete the EFS certificate from the store and reboot your instance.	After reboot, can you access your files? [Yes][No]
7	Now import the PFX certificate that you created.	Can you access your files? [Yes][No]
8	Now dismount your drive, and give the USB stick to your neighbour. 1. Ask them to access the files on the USB disk without importing the certificate.	Can they access your files before certificate import? [Yes][No]

	2. Ask them to access the files on the USB disk after importing the certificate.	Can they access your files after certificate import? [Yes][No]

5 Cracking digital certificates and file types

Undertake the following.

No	Description	Result
1	Go to your Windows 7 instance and run Networksims. Now run Toolkit client (Figure 2). Goto the Encryption tab and select Digital Certificate from the left-hand menu. Next click on the Dictionary Search button, and load each of the following files (remember to extract to PFX): http://asecuritysite.com/log/fred.zip http://asecuritysite.com/log/sample01.zip	What are the passwords for the PFX files?
2	For the following compressed files: http://asecuritysite.com/newfiles.zip Install a hex viewer (such as Hex Editor Neo) on the instance. Next determine the file types.	File01: File02: File03: File04: File05:

		File06: File07:

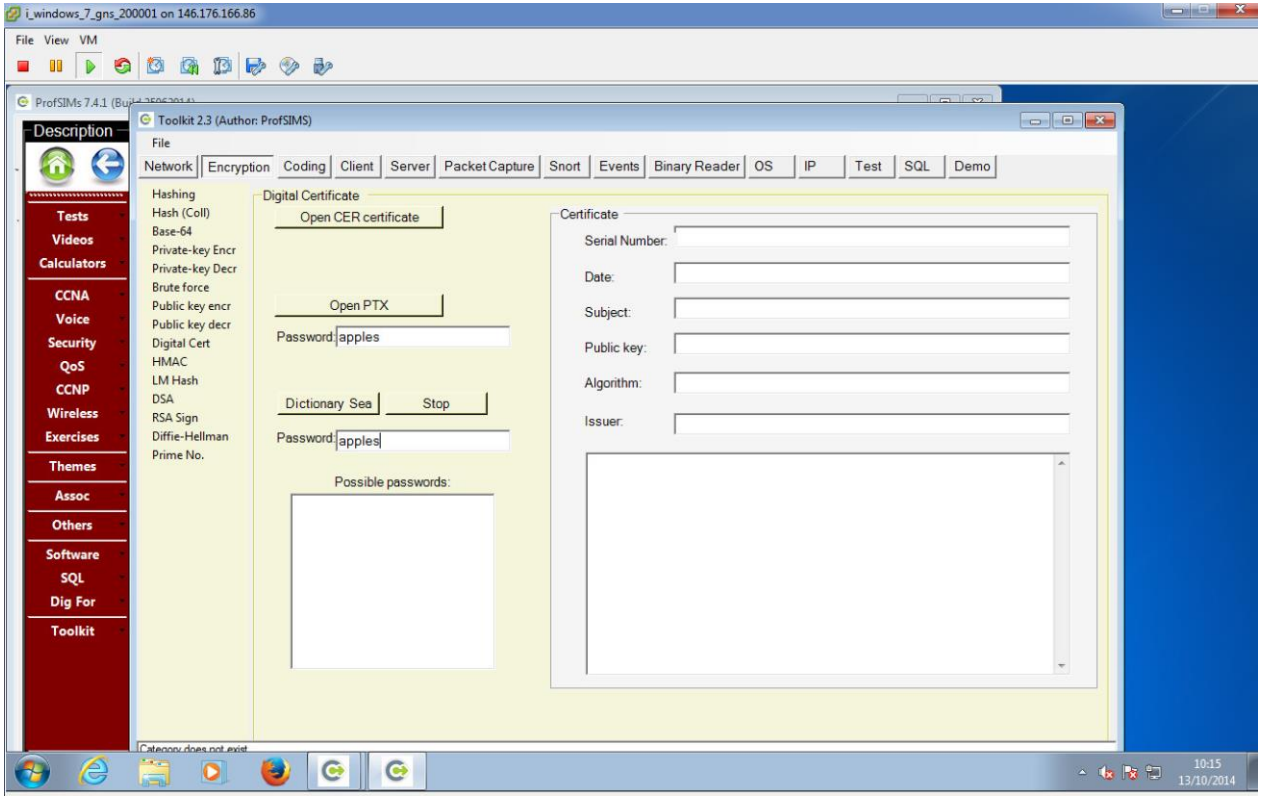

Figure 2: Dictionary search