Drive Encryption

Introduction and/or Background

Data encryption is one very solid security measure/precaution that everyone who owns data with significant personal or objective value should perform. What data encryption does is secure your data when they fall into the wrong hands.

While there are decryption methodologies and techniques that can be used to decrypt any encrypted data, some of it may not be retrieved, or the time and effort that it will take may lead the decryptor to the decision that your data isn't worth it.

LUKS (Linux Unified Key Setup)

An excellent description of LUKS:

> A common usage of LUKS is to provide full disk encryption, which involves encrypting the root partition of an operating system installation, which protects the operating system files from being tampered with or read by unauthorized parties.[13]
>
> On a Linux system, the boot partition (`/boot`) may be encrypted if the bootloader itself supports LUKS (e.g. GRUB). This is undertaken to prevent tampering of the Linux kernel. **However, the first stage bootloader or an EFI system partition cannot be encrypted** (see Full disk encryption#The boot key problem).[13]

(emphasis mine)

LUKS is not designed for encryption on a file by file basis but at a directory or whole disk volume basis. LUKS is one of the ways that a Linux admin may protect against root-kit attacks if the /boot directory is encrypted.

On a Debian system the LUKS system is part of the cryptsetup package found on the standard repositories. Use standard install methods to load cryptsetup. Be aware that there are two packages in the repositories, cryptsetup and cryptsetup:i386 depending on your CPU architecture.

Standard disclaimer as with all encryption – The sucess or failure LUKS is entirely dependent on the strength of the underlying password provided by the administrator.

Objectives

In this project/lab the student will:

- Create and utilize an encrypted drive partition

Equipment/Supplies Needed

- As specified in Lab 0.0.1.

Procedure

Perform the steps in this lab in the order they are presented to you. Answer all questions and record the requested information. Use the Linux Virtual Machine to perform lab activities as directed. Unless otherwise stated, all tasks done as a non-root user. If root access is needed use the sudo command.

Assignment

Shut down the Linux VM if it’s turned on.

Create a Snapshot to act as a restore point if problems occur later.

In the VM’s Settings, add a new Virtual Hard Disk. (reminder here)

Power on the Linux VM. Promote to root user.

Partition and format the new hard drive,

1.
   ```
   fdisk -l
   fdisk /dev/sdb
   Enter ‘p’ followed by ‘n’.
   Select all defaults
   Enter ‘p’ again to assure that the partion is created.
   Enter ‘w’
   fdisk -l
   ```

Mount the drive

```
mount /dev/sdb1 /mnt
```

Create a text file.

2.
   ```
   wget https://georgewbush-whitehouse.archives.gov/independenceday/text/declaration.html
   ```

Display its contents and take a screenshot.

3.
```
cat declaration.html
```

Unmount the drive using the command,

4.
```
umount  /mnt
```

Install cryptsetup.

Encrypt the /dev/sdb1 partition.

5.
```
cryptsetup -v -y --type luks2 luksFormat /dev/sdb1
```

Map the encrypted partition file to the /dev/sdb1 directory.

6.
```
cryptsetup luksOpen /dev/sdb1 sdb1
```

Ensure the mapping is active by checking its status.

7.
```
fdisk -l
```

Dump the LUKS headers and take a screenshot.

8.
```
cryptsetup luksDump /dev/sdb1
```

Create an EXT4 filesystem on the mapped drive. There’s no need to reformat the drive with dd or pv.

9.
```
mkfs.ext4 /dev/mapper/sdb1
```

Mount the new filesystem and confirm that it’s visible.

10.
```
mount /dev/mapper/sdb1 /mnt
df -h
```

Enter,

11.
```
sudo lsblk –fs
```

Take a screenshot of the output.

Unmount the drive

12.
```
umount /mnt
cryptsetup luksClose sdb1
```

Remount the encrypted partition

13.
```
sudo cryptsetup luksOpen /dev/sdb1 backup
sudo mount /dev/mapper/backup /mnt
```

Enter the command `mount` to display information on all mounted devices on the system.

Execute,

14.
```
df -H
```

Take a screenshot of the Terminal window.

Reflection

1. How might the use of an encrypted volume be beneficial?
2. How could it be misused?
3. What happens if you forget the password?

Rubric

Checklist/Single Point Mastery

Concerns Working Towards Proficiency	Criteria Standards for This Competency	Accomplished Evidence of Mastering Competency
	Criteria #1: Screenshot showing the unencrypted drive (21.25 points)	
	Criteria #2: Screenshot showing the LUKS header information for the encrypted drive (21.25 points)	
	Criteria #3: Screenshot showing the encrypted drive mounted to a folder (21.25 points)	
	Criteria #4: Screenshot showing the mount’s partition information (21.25 points)	
	Criteria #5: Answer to reflection	

	question 1 (5 points)	
	Criteria #6: Answer to reflection question 2 (5 points)	
	Criteria #7: Answer to reflection question 3 (5 points)	