Dom Moore
Protecting data at rest- Bitlocker

## Part 1: Staging

To complete this lab, you will need:

- A Windows 10 environment capable of Bitlocker
- A Linux environment (Ubuntu 20.04 Focal Fossa is a safe choice)
    - eCryptfs installed
    - LUKS installed
- A USB flash drive

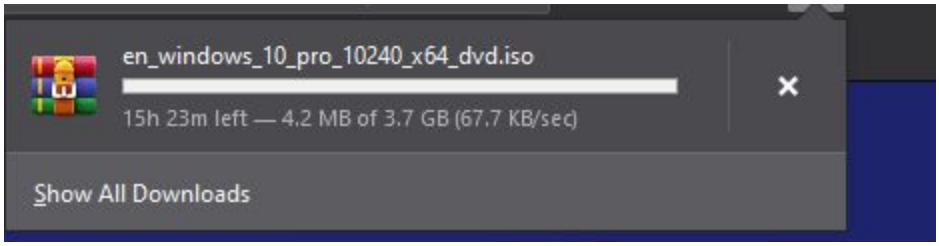
**Problem Area:**

This lab required the use of windows pro or enterprise so the os that I have installed is a windows home edition and does not come with the BitLocker feature, so I had to pivot and use other methods to complete the lab.

**Solution**:

To complete the first part of the lab I pivoted to using a cloud base service and was able to create a win 10 pro edition within their virtual machine, the second have i worked with team members to verify that once USB was encrypted that it was disabled in other devices.

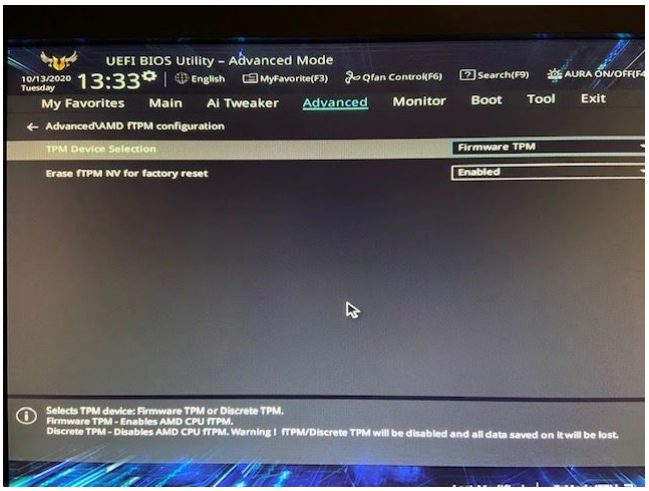
**Win Pro ISO install**



## Part 2: Windows FDE

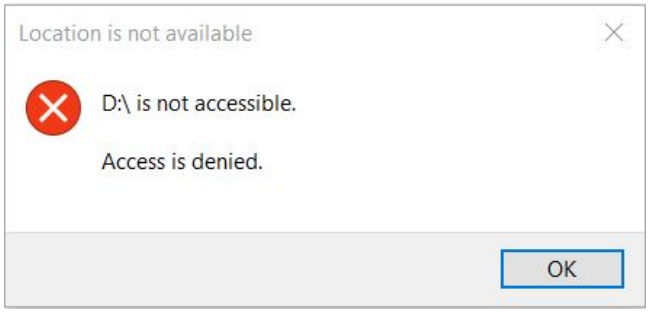
- Access your Windows 10 computer's BIOS and look for evidence of a TPM chip. Include a photo or screenshot of the TPM chip information in the BIOS.
- Use Bitlocker to encrypt a USB flash drive in Windows 10.
- Safely remove the USB flash drive and attempt to access its data on another system without the Bitlocker key.
- Include a screenshot or photo of the access failure.

**Windows Bios**




**Bitlocker**


**Classmate USB:**

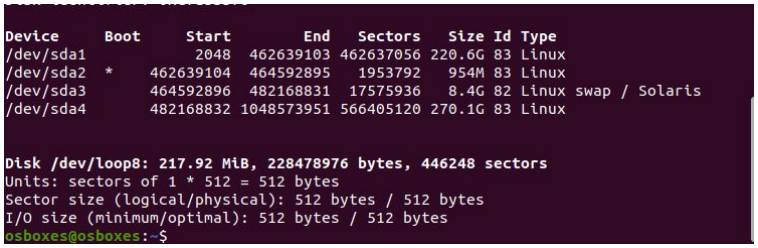


## Part 3: Linux Disk Encryption with LUKS

Use LUKS to encrypt and decrypt a drive or partition in a Linux VM.

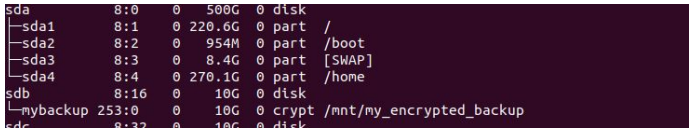
- First, create a partition to encrypt.
- Using cryptsetup format the volume with LUKS.
- Create a file system.
- Mount the data.
- Confirm success by viewing LUKS details.

**Partition list**

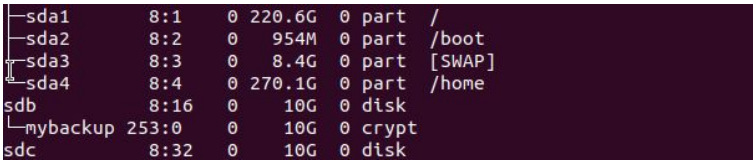



**Create Partition**


**Sdb disk mounted in LUKS**



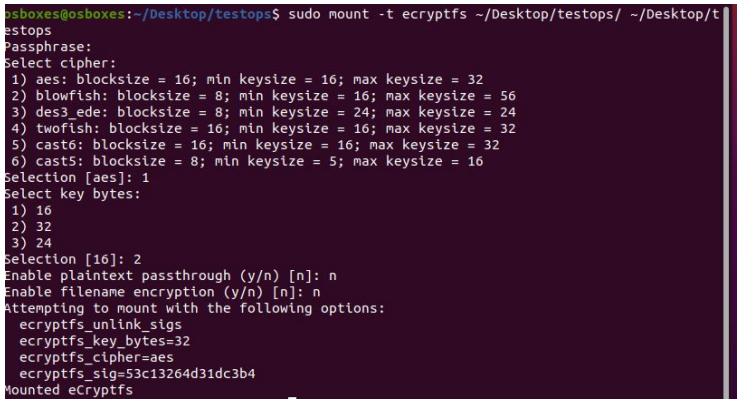

**Encrypted Disk LUKS**



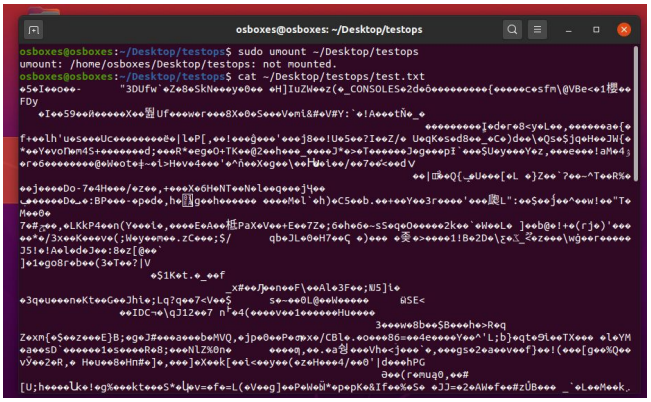
## Part 4: Linux Directory Encryption with eCryptfs

- Mount a new encrypted directory using eCryptfs.
- Create a new .txt document within the encrypted directory.
- Try viewing the document. You should be able to see the document because the directory is currently mounted.
- Unmount the directory with the umount command.
- Try viewing the document. You should now only see the ciphertext. Include a screenshot of the ciphertext on your submission.

**Mount Directory**




**Unmount**



## Part 5: Reporting

- What is the purpose of the TPM chip and why is it required in order to operate Bitlocker on a Windows 10 PC?
    - The TPM is the trusted platform module and is used as a security feature for hardware and software and provides keys for encryption of data on a Windows OS. TPM allows data to be secured within using a USB without it you can still use BitLocker but will need additional tools.
- Are laptop computers secured against theft out of the box? What precautions can be taken to ensure data confidentiality in the event of laptop theft?
    - No computers are not secure out of the box and should be equipped with user PW and some form of protection against data tampering or loss either through backups or file data protection strategy.
- What data theft scenarios do today's tools *not* defend against?
    - Social engineering and trusting others / social media
- Consider data at rest VS data in motion. How do these two categories affect how you approach securing data? The main difference in approach would take into consideration the route of data in transit and ensure that the route is secure and for data at resting the time, it would take to retrieve that data if it was requested.