A PROJECT REPORT

ON

**DISK ENCRYPTION**



****

**DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING**

**SAGI RAMA KRISHNAM RAJU ENGINEERING COLLEGE**

**[AUTONOMOUS]**

**BHIMAVARAM**

**OUTLINE OF THE PROJECT**

If you're using a computer or a removable USB drive, chances are that you have sensitive data on these devices. Whether it's your home computer with family finances, your work computer with sensitive corporate information, or a thumb drive with government secrets, you want to ensure that there is no unauthorized access to that data if the device is lost or stolen. **FULL DISK ENCRYPTION** protects this data, rendering it unreadable to unauthorized users.

Our objective is to achieve Full Disk Encryption, which protects a disk in the event of theft or accidental loss. Full disk encryption encrypts the entire disk including swap files, system files, and hibernation files. If an encrypted disk is lost, stolen, or placed into another computer, the encrypted state of the drive remains unchanged, and only an authorized user can access its contents.

**ABSTRACT**

Full-disk encryption (FDE) is the encryption of all data on a disk drive, including the program that encrypts the bootable OS partition. FDE converts all device data into a form that can be only understood by the one who has the key to decrypt the encrypted data. An authentication key is used to reverse conversion and render the data readable. FDE prevents unauthorized drive and data access. Data and OSs are automatically encrypted through FDE.

Disk Encryption methods aim to provide three distinct properties: 1.The data on the disk should remain confidential. 2.Data retrieval and storage should both be fast operations, no matter where on the disk the data is stored. 3.The amount of storage used for encrypted data should not be significantly larger than the size of plaintext.

**TABLE OF CONTENTS:**

1. **INTRODUCTION 4**
2. **PROBLEM STATEMENT 6**
3. **METHODOLOGY 7**
4. **CONCLUSION 17**
5. **REFERENCES 20**

**INTRODUCTION**

‘Encryption’ refers to the process of Encoding Data. Disk Encryption is that the information on our computer’s hard drive/ blockable devices is transformed from plaintext to ciphertext, which makes the original information unreadable.

Hard Drive Encryption converts physical disk or logical volume into an unreadable format that cannot be unlocked by anyone without the key or password that wasused for encryption. This prevents unauthorized people or hackers from accessing the information.

**Why do we do Disk Encryption?**

FDE is useful for small electronic devices vulnerable to theft or loss, such as laptops. In a corporate or large computer network environment, a secure username and password policy is a critical requirement.

The following are FDE advantages:

* The majority of data is encrypted, including swap space and temporary files.
* For eliminating the risk of data leaks.
* In order to reduce the liability issues arising at Industries/Companies.
* Authorization is established prior to computer booting (pre-boot authentication).
* Destroying authentication/cryptography keys also destroys data. Physical drive destruction or purging is recommended if future attacks are a concern.

**How do we achieve Disk Encryption?**

We can achieve the Disk Encryption in various ways through open source tools and softwares like Veracrypt, Bitlocker, Ciphershed, Filevault 2, LUKS depends on the type of operating system.

Here, we use **LUKS(Linux Unified Key Setup)** and **Dm-Crypt** tool in order 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.



**KEYS / TOOLS used:**

* **LUKS(LINUX UNIFIED KEY SETUP):**

LUKS is used to encrypt the Disk Partitions & Block Devices at Device levels. It is a key for encryption in which the Encryption is done with a multi-layer approach.

LUKS is used to encrypt the Disk Partitions & Block Devices at Device levels. It is a key for encryption in which the Encryption is done with a multi-layer approach.

* **DM-CRYPT(DEVICE MAPPER-CRYPT):**

DM-CRYPT is a transparent block device encryption subsystem in Linux which gives flexibility so that it can be used for encrypting any disk-backed file systems supported by the operating system, as well as swap space; write barriers implemented by file systems are preserved.

Encrypted volumes can be stored on disk partitions, logical volumes, whole disks as well as file-backed disk images.

**PROBLEM STATEMENT**

The data in a device can be accessible to unauthorized users and can be lead to risk of data loss which could be resulted the people or companies in involving the raise of liability issues or loss of data integrity. These adversaries may lead to Privacy Violation too.

**BACKGROUND RESEARCH/ANALYSIS:**

In order to tackle the above adversaries, there exist a various open sources or premium software, tools and keys like Veracrypt, Bitlocker, Ciphershed, Filevault 2, LUKS. Based on the type of Operating System, Device, configuration and level of Encryption, we can use required tool, key or software to provide encryption.

**RELEVENCE:**

The implementation of Disk Encryption for the Virtual Disk in Linux can be done by using LUKS(Linux Unified Key Setup) and Dm-Crypt tool, which involves encrypting the root partition of an operating system installation that protects the operating system files from being tampered with or read by unauthorized parties.

**SCOPE:**

We are going to provide Encryption for Virtual hard disk of Linux with LUKS and Dm-crypt and can reduce the decrypting action of Brute Force attack on encrypted disk.

**METHODOLOGY**

**STEPS INVOLVED:**

1. **Disk Drive Creation.**
2. **Disk Partition.**
3. **Disk Encryption.**
4. **Prevention of Brute Force Attack.**

**Disk Drive Creation:**

First of all, we have create a disk drive which we are going to encrypt. For this open **storage settings** of **linux** in **Virtual machine**.

>>Then select **controller: SATA** whose type is SSD.



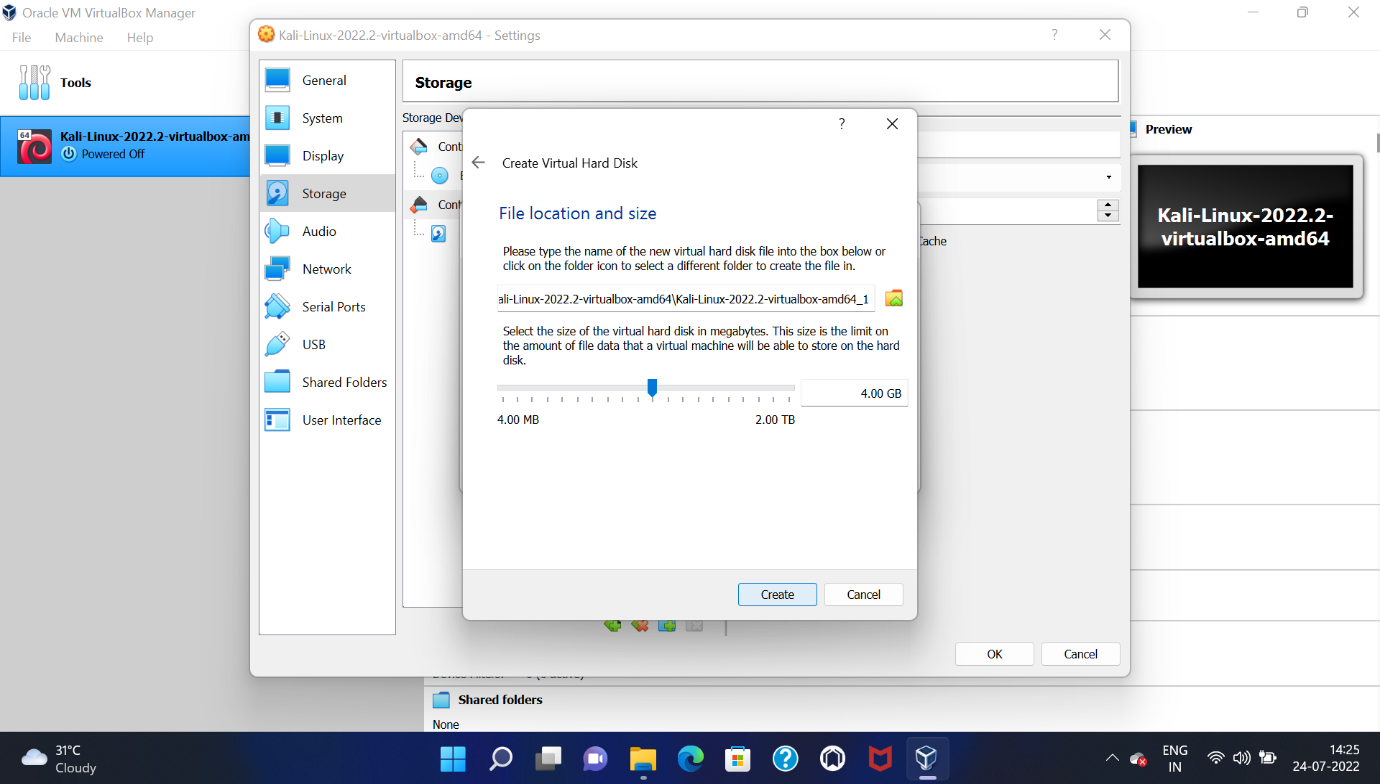
>>Select **create** option for the creation:



>>Select the **type** of size viz. static or dynamic:



>>Select the required **amount** of size and click on **create:**



>>Now we have created a new **Disk Partition:**

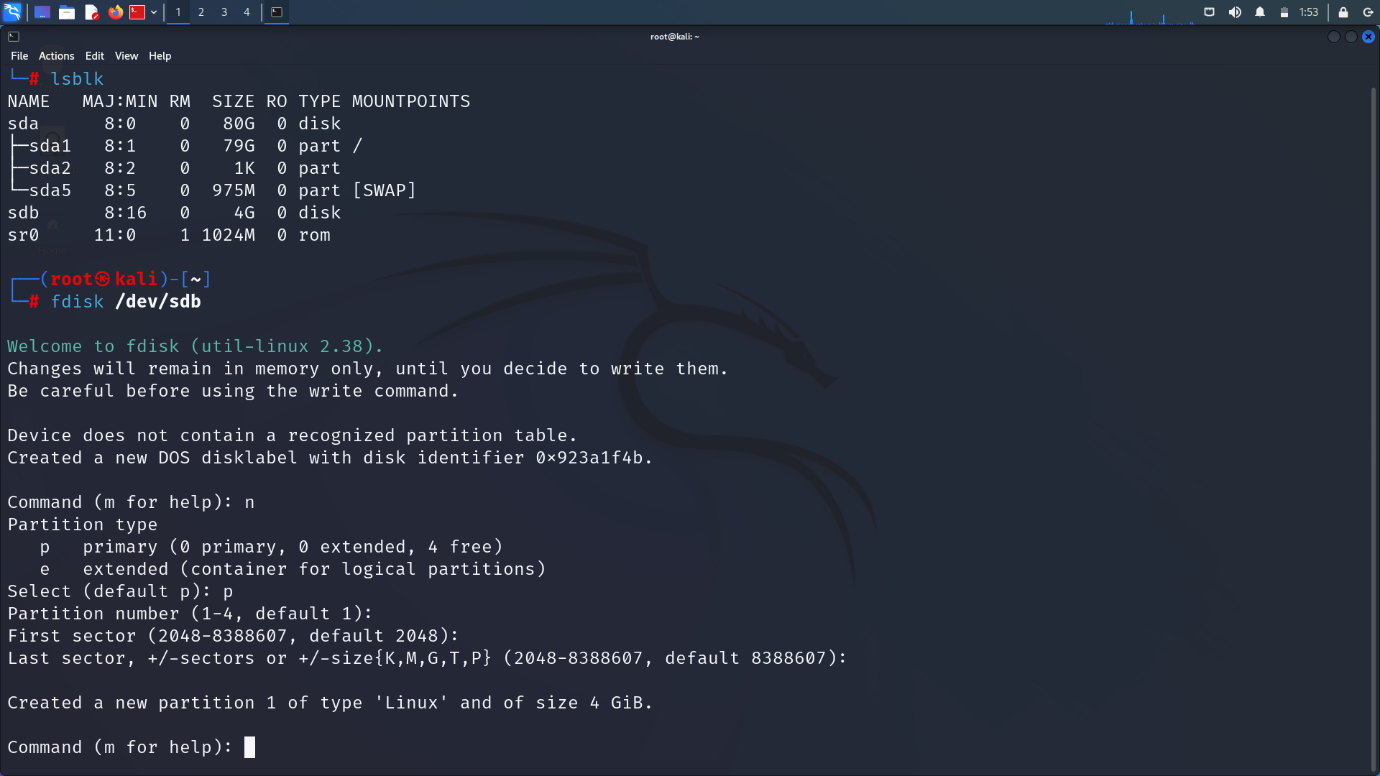


After creating a Disk Drive, we have to make a partition to be encrypted. For that open the **terminal** in Linux.

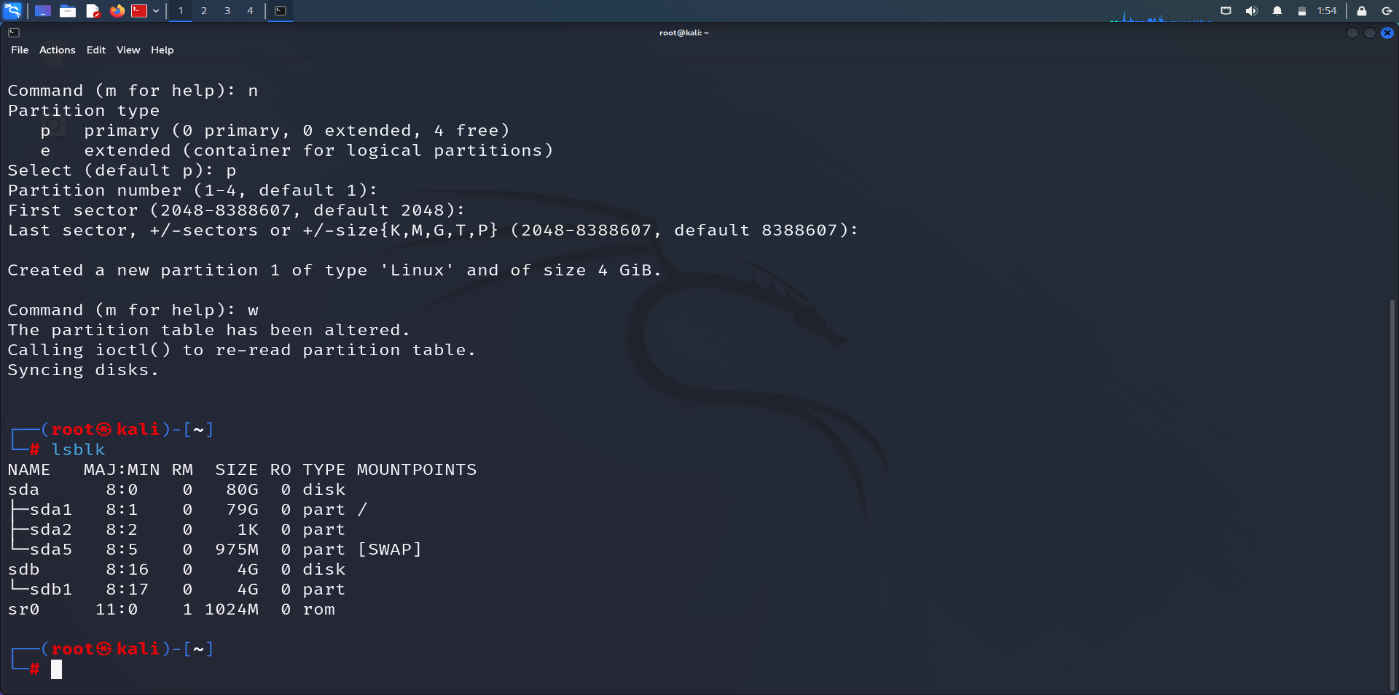
>> We have see list of block devices(disks) exist in the linux- ( *lsblk* ):

In the list, **sdb** is our created disk.

>>Create a new partition in our disk-(*fdisk*):



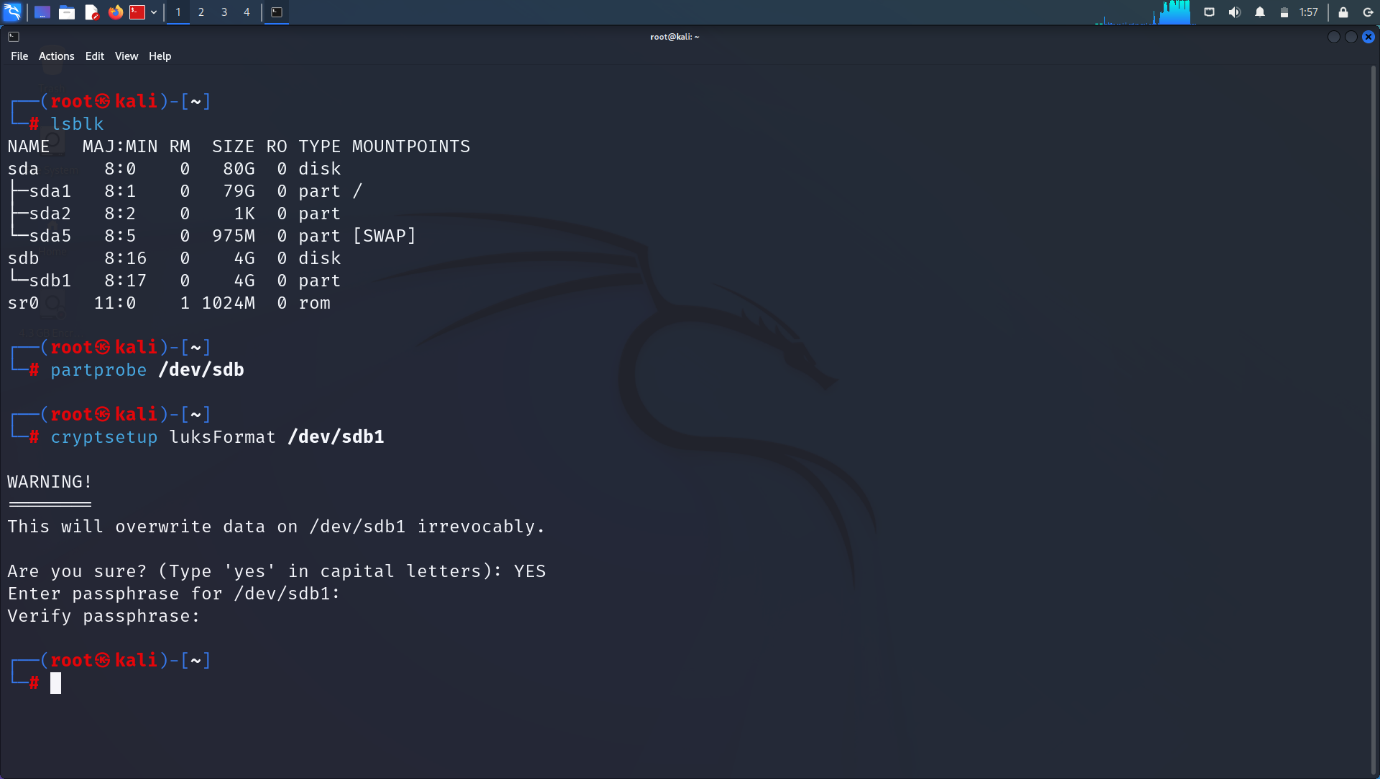
>>If we check partition table again with *lsblk*, we will get our partition:



**Disk Encryption:**

>>Now notify the OS about our newly created disk with *partprobe* cmd:

>>Format and Encrypt the disk with LUKS an Dm-crypt by any Password:

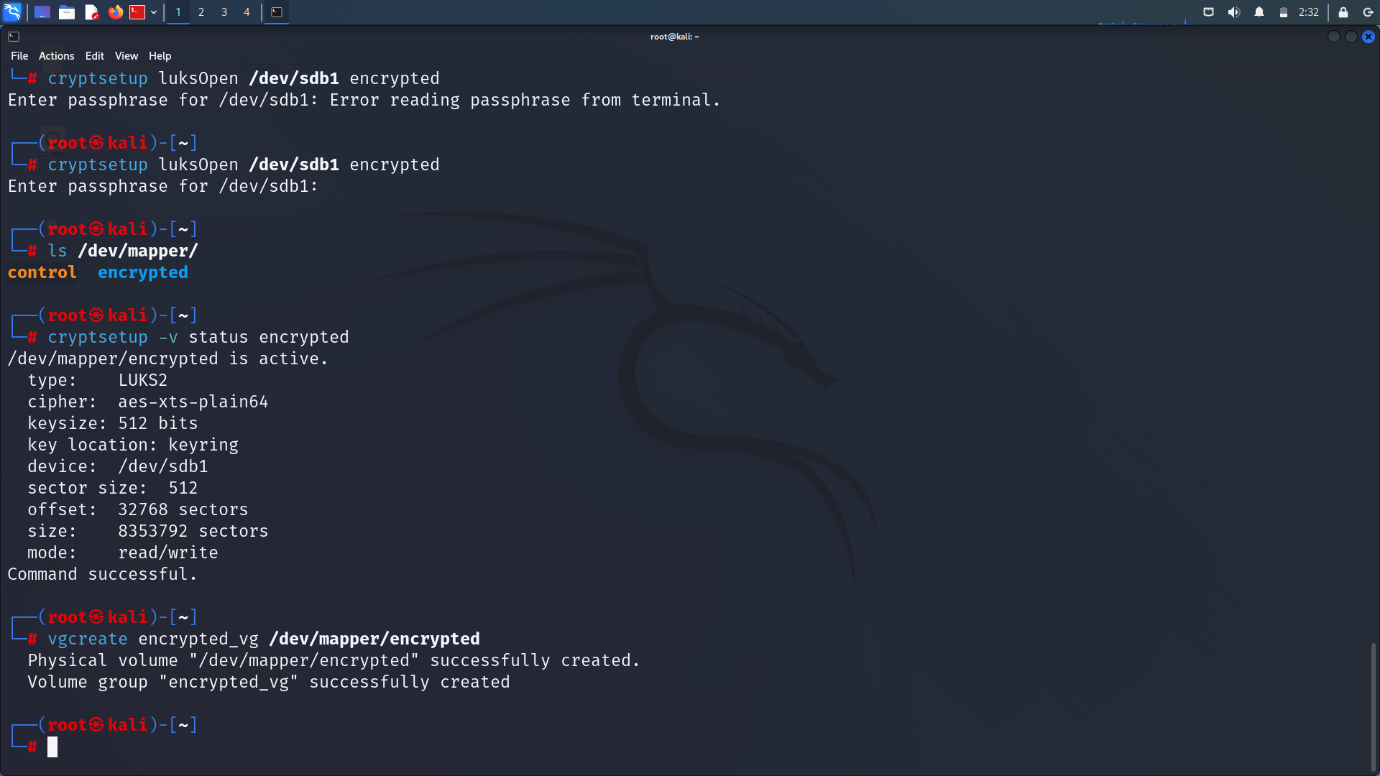




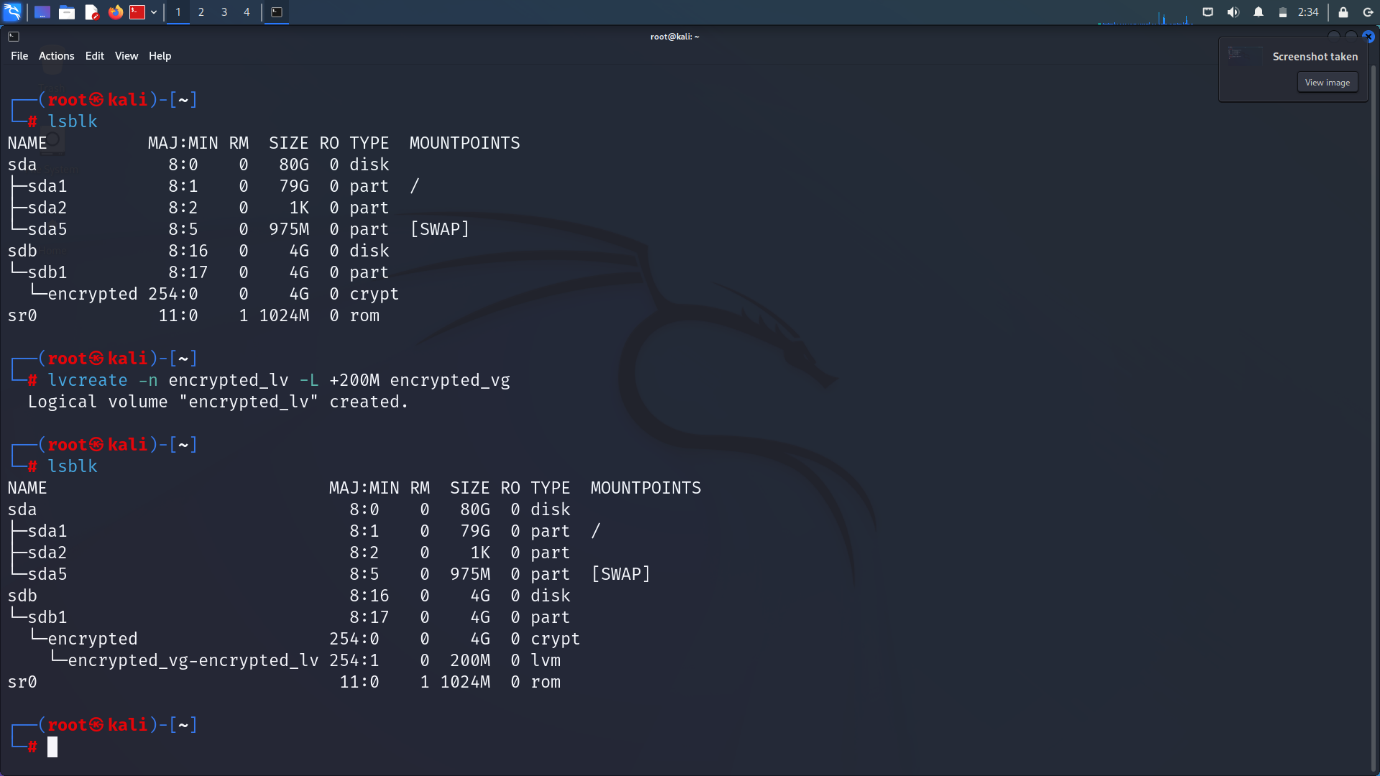




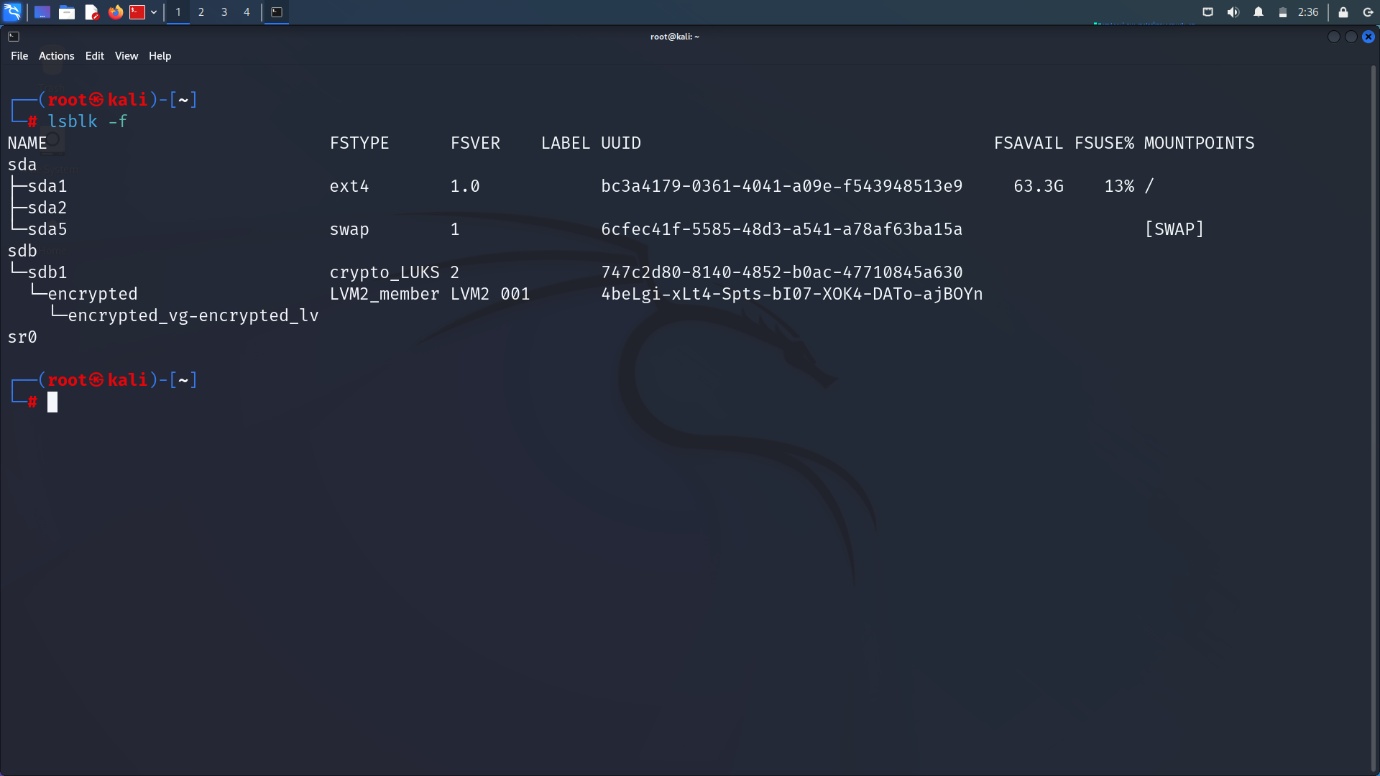
>>Now initialize the partition and create a volume group:



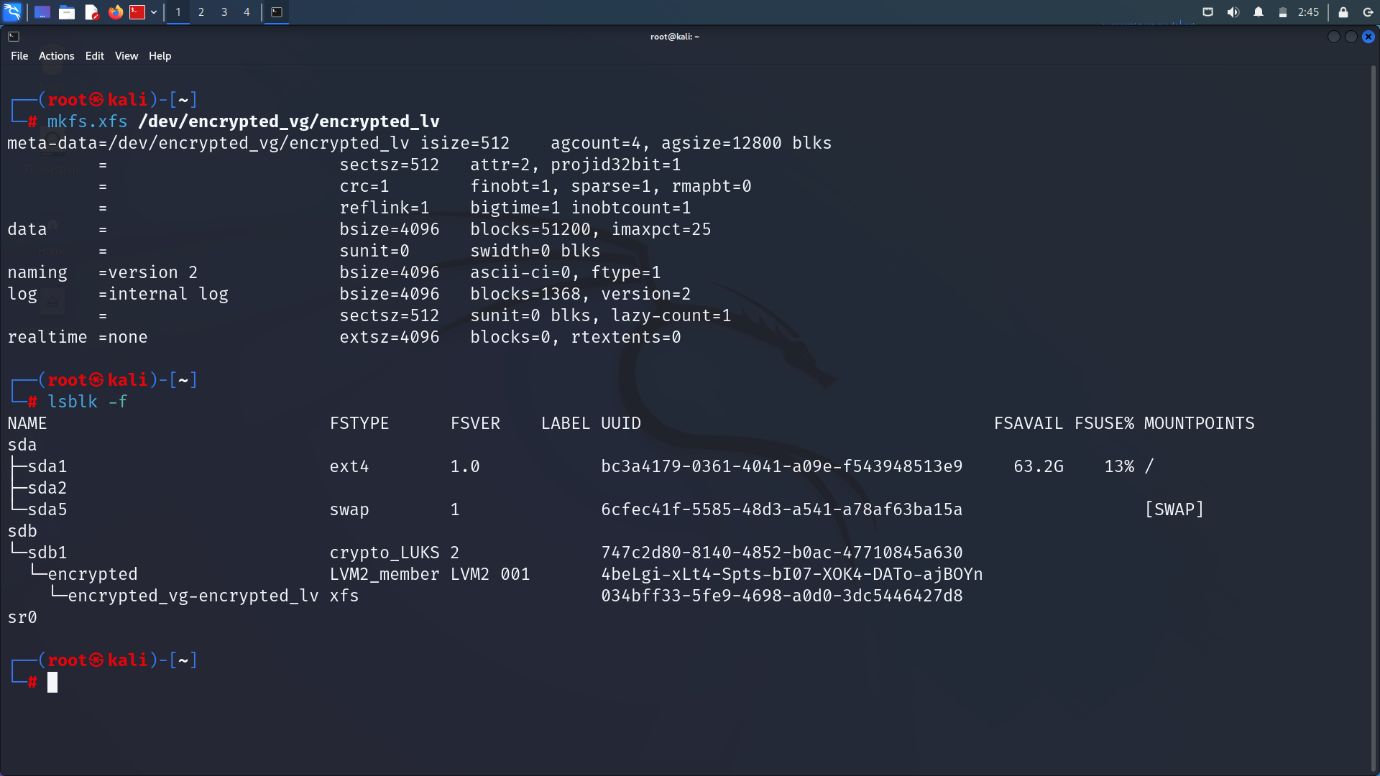
>>Inside that volume group, create a logical volume to provide encryption at kernel level:



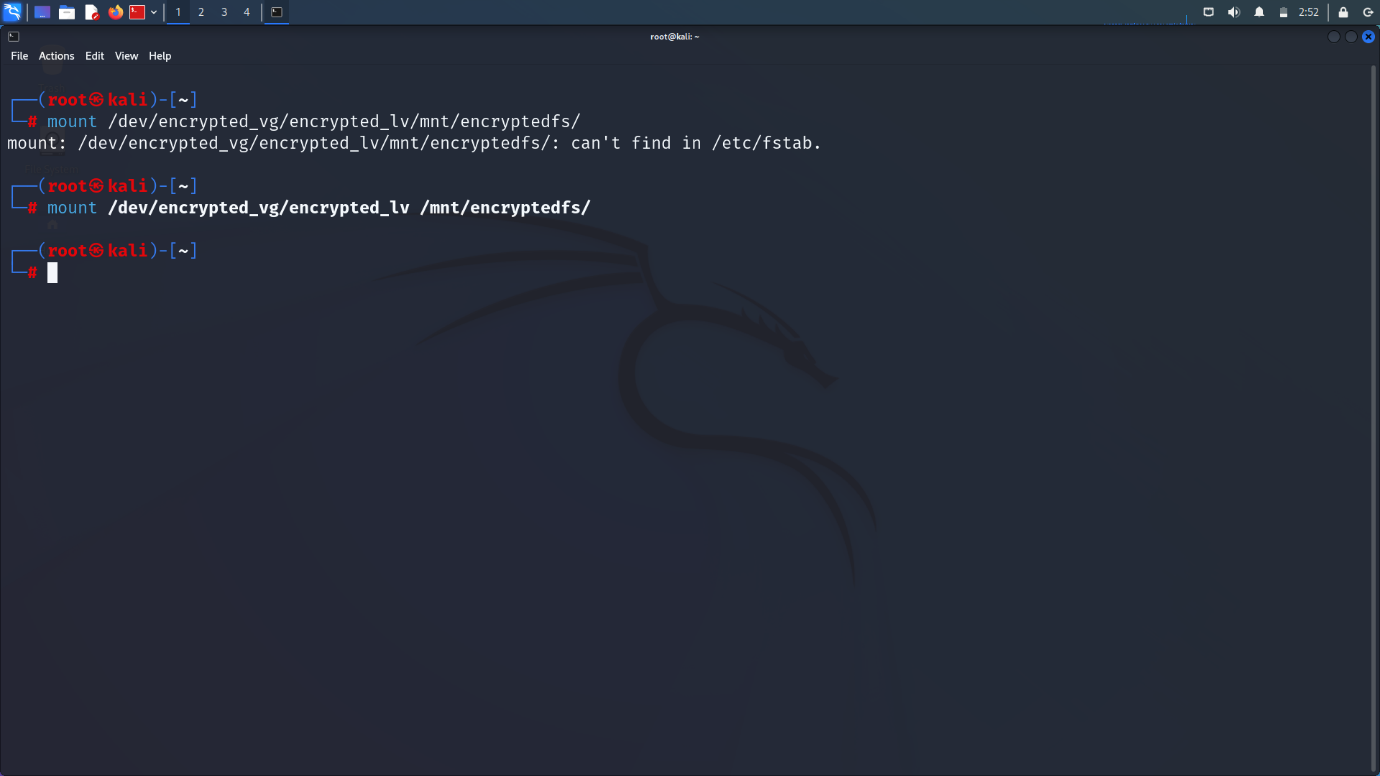
>>Check the File Systems of existed block devices:



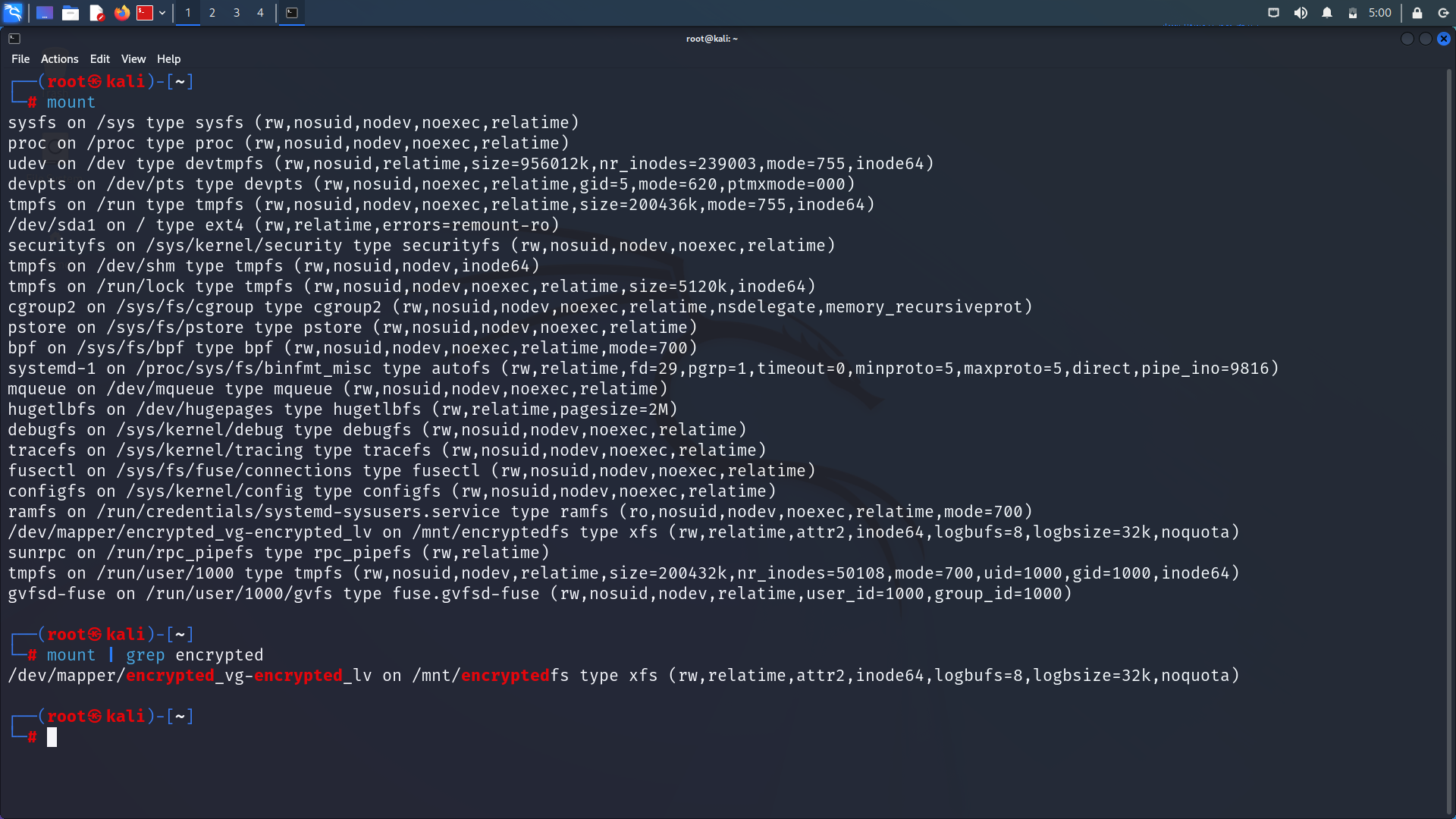
>>Assign a file system to our created Volume Group:



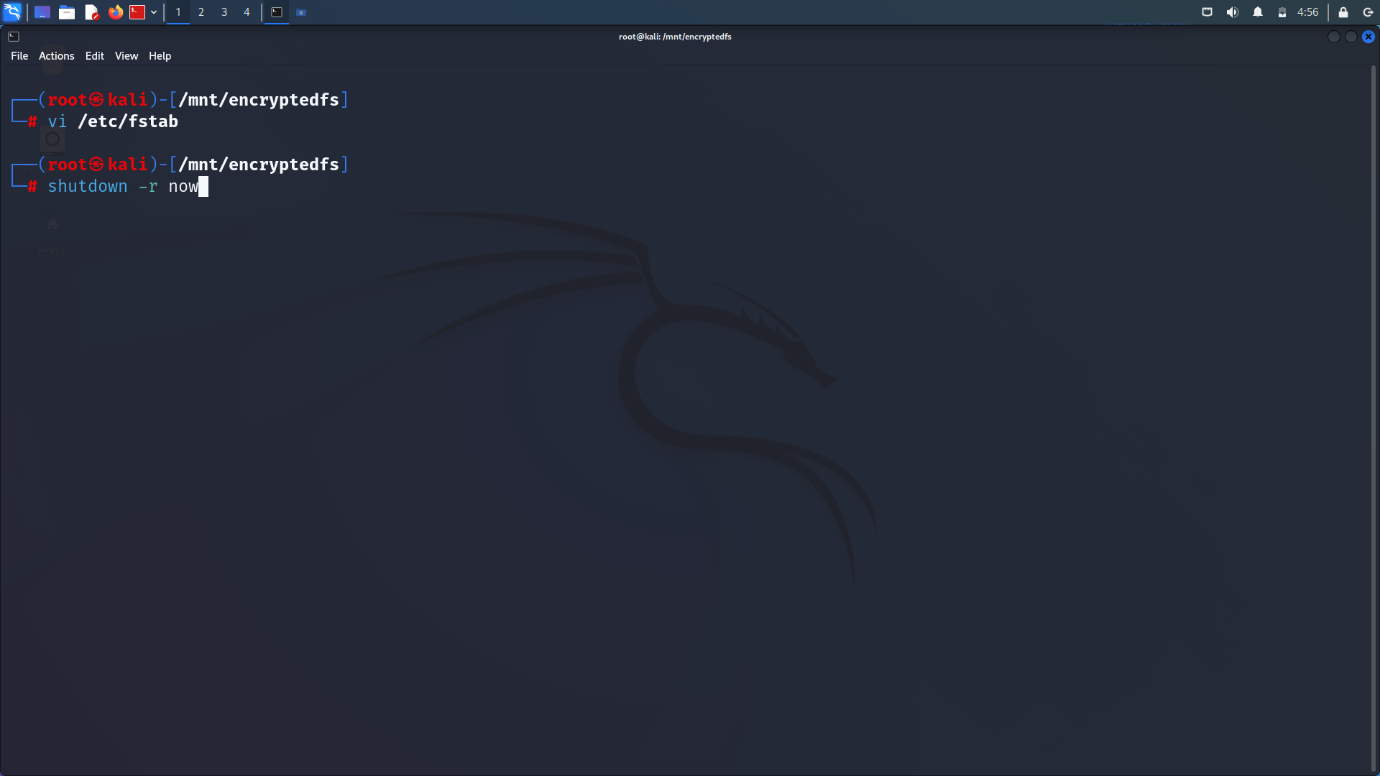
>>Mount the volume group to the OS:



>>Check mounted devices and Partitions:

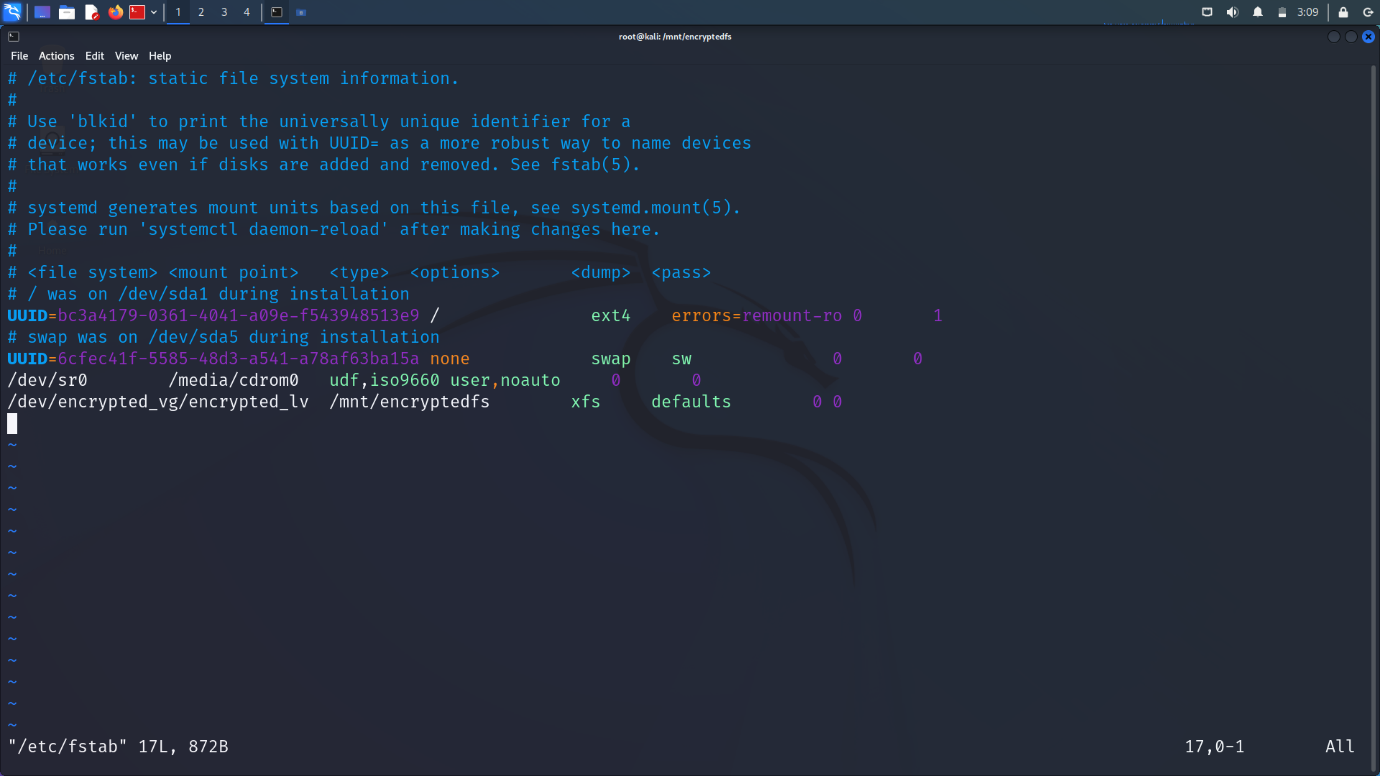


>>Implement the encryption from kernel level to boot process level and write the changes permanently:

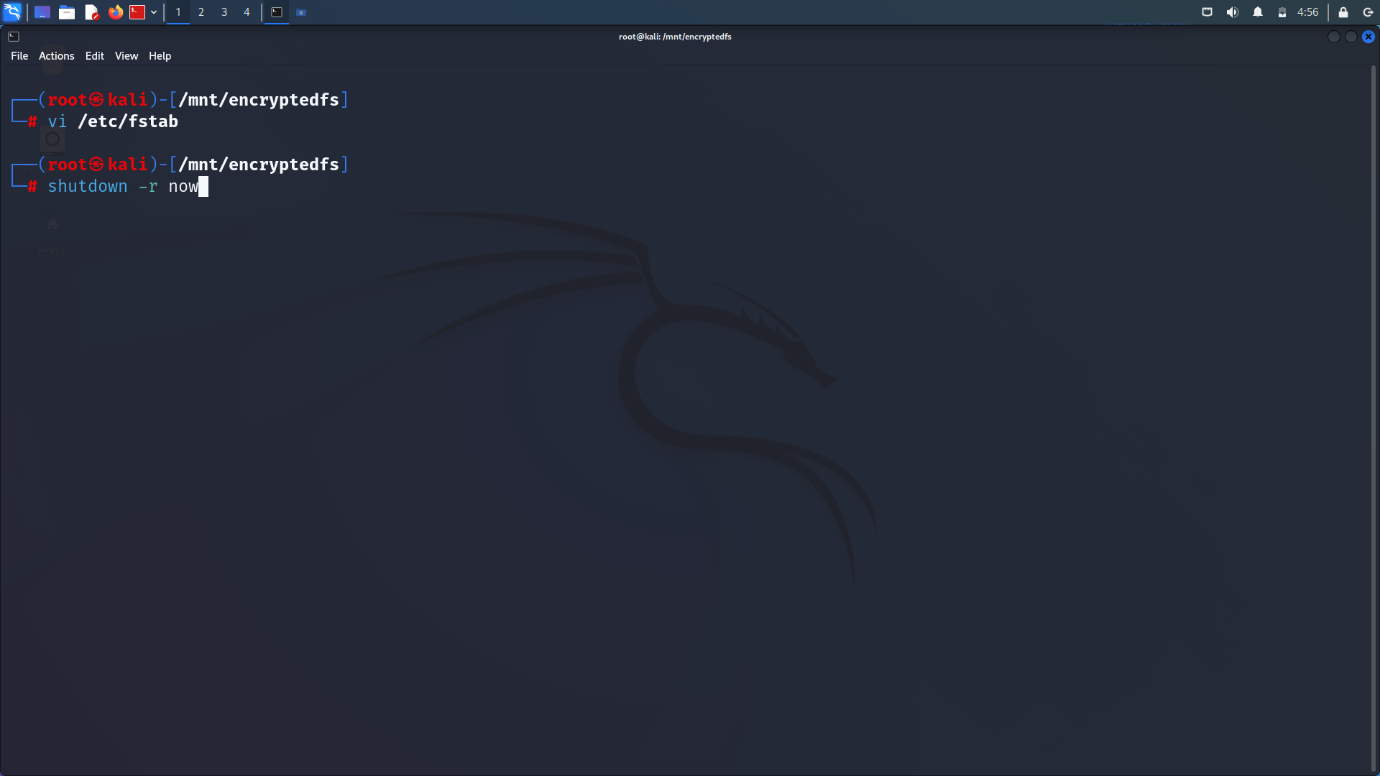


>>Write the partition details manually and make them permanent of order as follows:

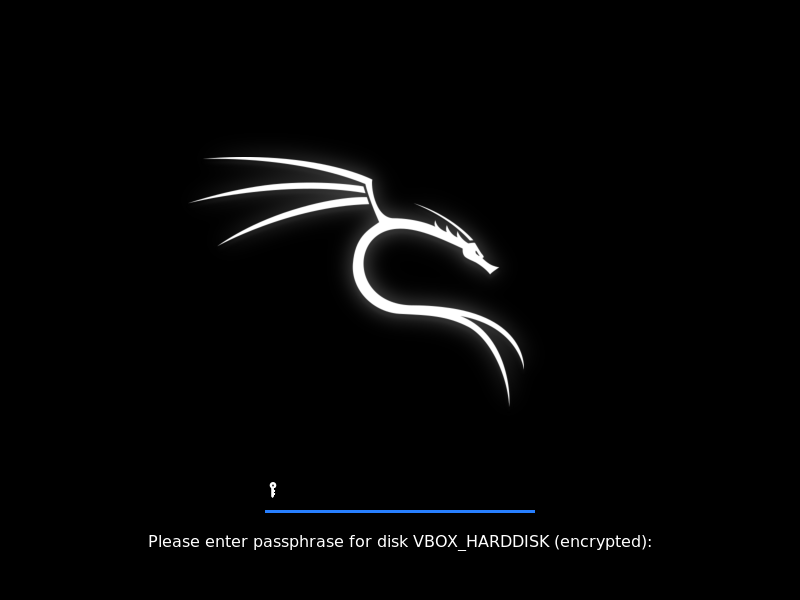
[dev name] [dev root] [FS type] [dump options]



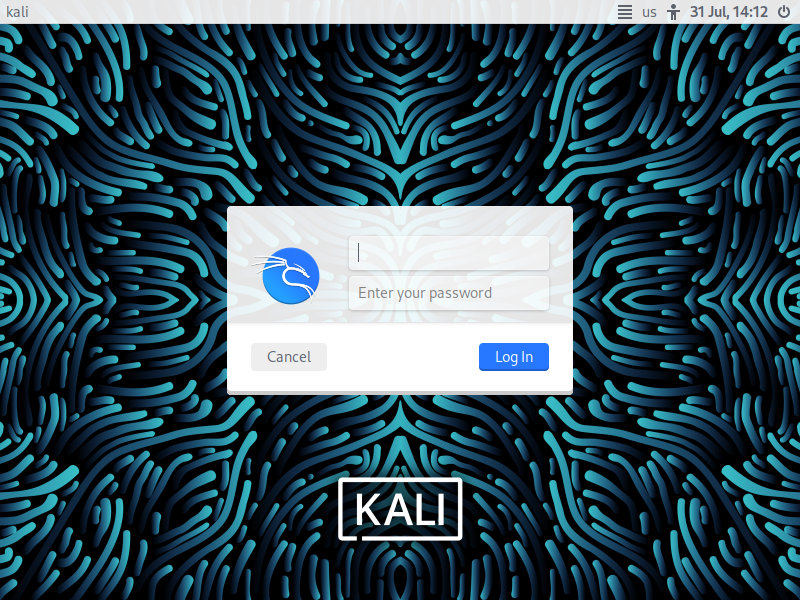
>>Do shutdown right now:



>>Encryption is Done for the Disk. If we turn on the **linux** now, we will get as follows and Enter the password used to encrypt the device to open:



>>After that we will get the entry into Linux:



**CONCLUSION**

Like a coin has two sides, Disk Encryption too has two sides that which we have discussed earlier is a bright side and a dark side is also exist. On that side, there lie the disadvantages of Disk Encryption like:

* Slow down the performance of the system or device.
* Recovery of Data becomes complicate.
* Do not protect the data in transit through Mails and many more.

**COUNTER MEASURES:**

In order to tackle the hacking of Encrypted Disks, we will prevent the Brute Force Attack.

**Prevention of Brute Force Attack on Encrypted Disks:**

**Brute Force Attack:**

A brute force attack is a hacking method that uses trial and error to crack passwords, login credentials, and encryption keys. It is a simple yet reliable tactic for gaining unauthorized access to individual accounts and organizations’ systems and networks. The hacker tries multiple usernames and passwords, often using a computer to test a wide range of combinations, until they find the correct login information.

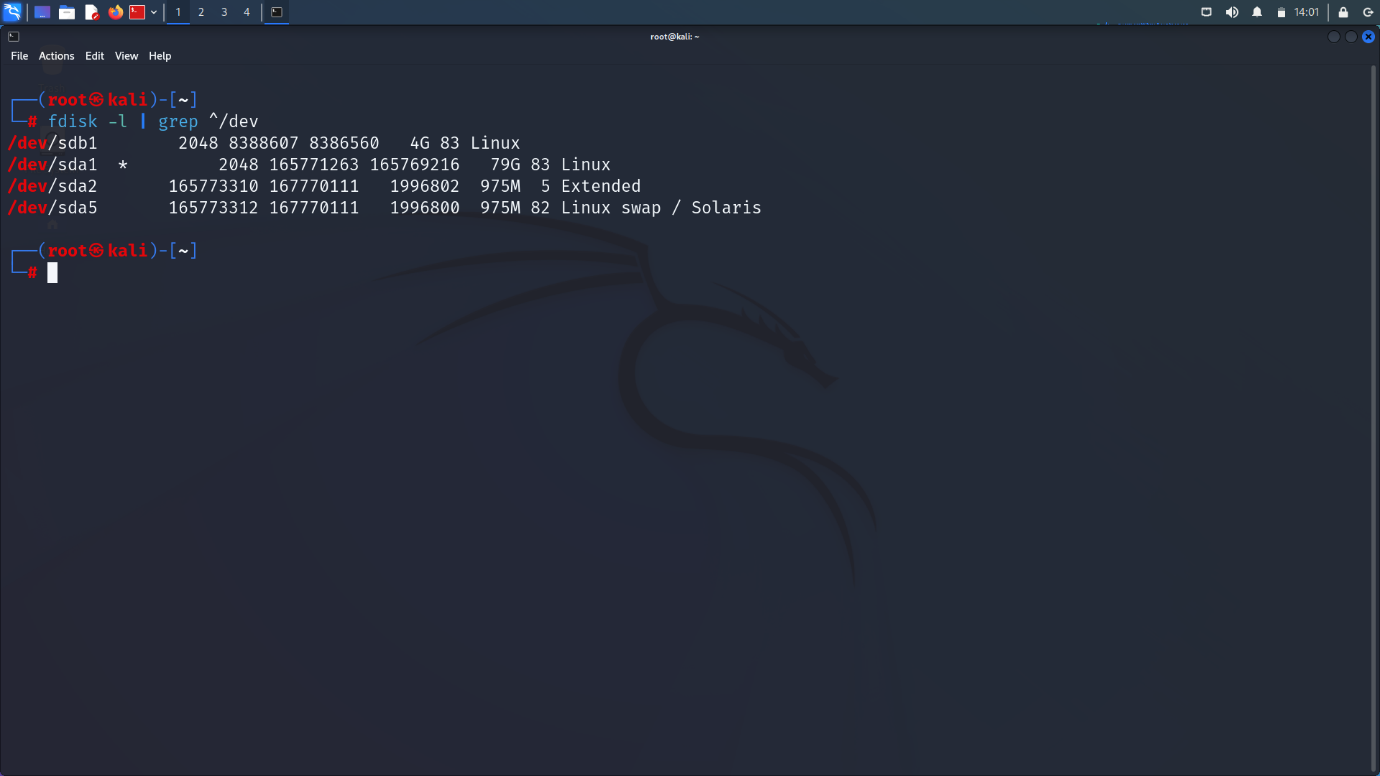


The name "brute force" comes from attackers using excessively forceful attempts to gain access to user accounts. Despite being an old cyberattack method, brute force attacks are tried and tested and remain a popular tactic with hackers.

**Prevention:**

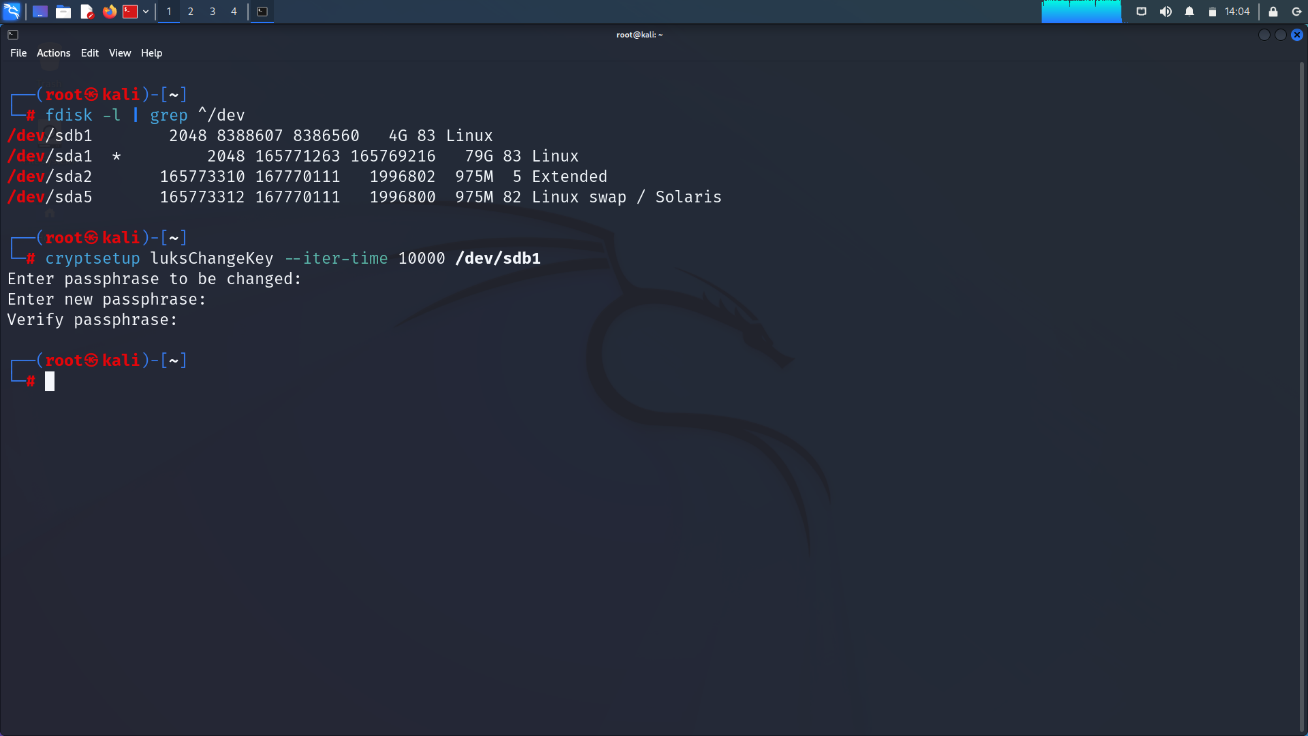
The prevention of the brute force attack on the encrypted disk is done by delaying the iteration time for the entry of the every two successive passwords whether they may be correct or not by desired amount of time.

>>Get the root of our device/partition using following command:





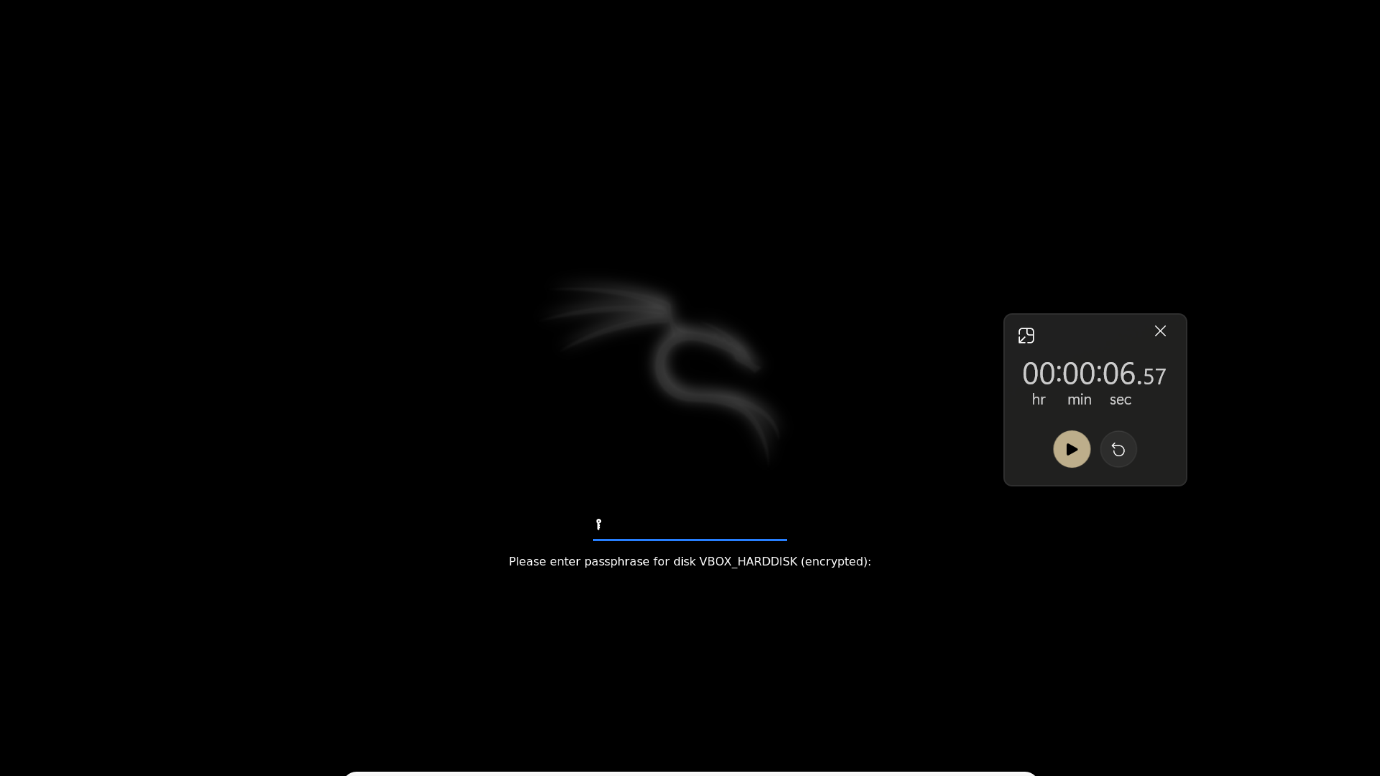
>>Now change the iteration time and password:



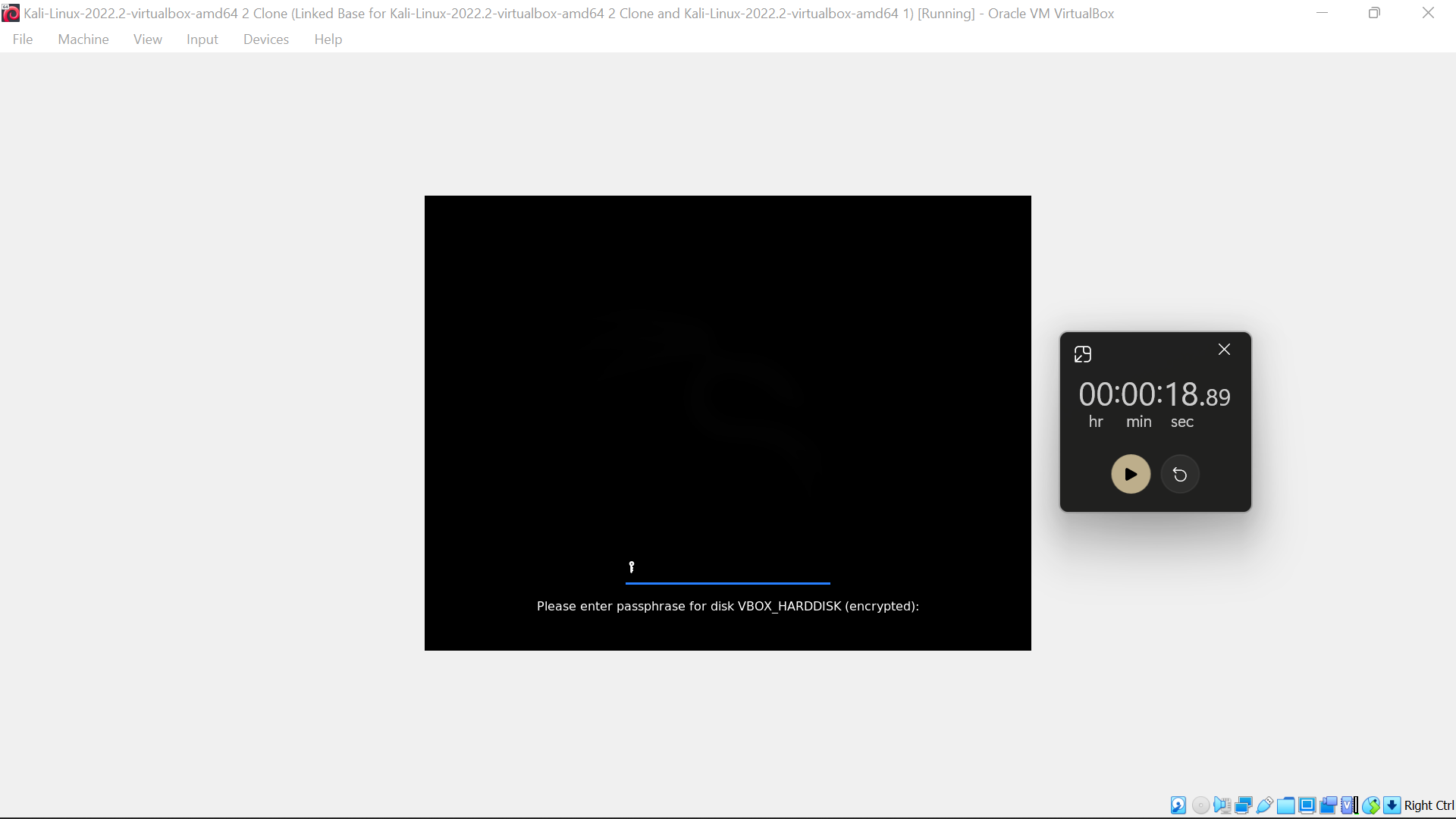
Now The Iteration time of the Encrypted Disk is changed.

>> I have two Linux machines such that both of them are encrypted but one of them is encrypted with iteration time of +10 seconds.

1.Iteration time of Encrypted but default iteration time and I got 6 seconds.



2.Iteration time of Encrypted and +10 secs iteration time and I got 18 seconds:



Based on the above observations, we made to delay the iteration time and reduce manual entry of passwords of Brute Force Attack.

**REFERENCES**

* Encrypting Partitions With LUKS:[Encrypting Partitions With LUKS: Guide To Encrypt Linux Partitions - LinuxForDevices](https://www.linuxfordevices.com/tutorials/linux/encrypting-partitions-with-luks#:~:text=%20Step-By-Step%20Encrypting%20Partitions%20With%20LUKS%20%201,a%20LUKS%20partition%20behind%20a%20password...%20More%20)**.**
* RedHat Enterprises: [What is LUKS disk encryption and how can it be implemented? - Red Hat Customer Portal](https://access.redhat.com/solutions/100463).
* Wikipedia: [Disk encryption - Wikipedia](https://en.wikipedia.org/wiki/Disk_encryption).
* Bruteforce:<https://superuser.com/questions/1643918/increase-time-to-brute-force-luks-full-disk-encryption>