Table of Contents

CareerTiQ
CHOOSE THE BEST

Project Requirement Document (PRD)

CYBERSECURITY PROJECT

PROJECT: RANSOMWARE ATTACKANALYSISANDRECOVERY

Group members: Kaja Navya

Ravada

Niharika

Kannuru

Hykulu

01
Introduction
Ransomware Attack

02
History
History and itstypes

03
How it Works
Working of Ransomware Attack

04
How to Prevent

05
How to recovery

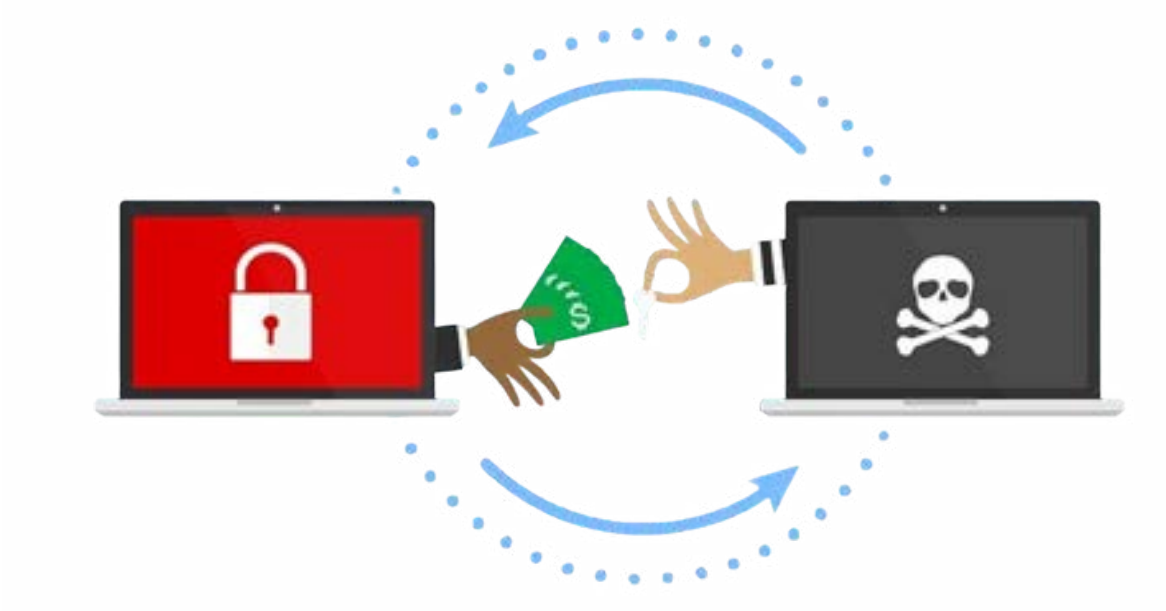
06

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:

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

2.Distribution Methods:

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

3. Impact on Different Sectors:

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

4.Prevention and Mitigation:

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

5.Legal and Ethical Issues:

- 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 BirthofRansomwareisinthemiddleof1980'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.

TheRise 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 in have continued to rise in frequency and sophistication with millions of attacks occurring manually.

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.

<u>How it Works</u>?

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.

<u>How to Prevent</u>?

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

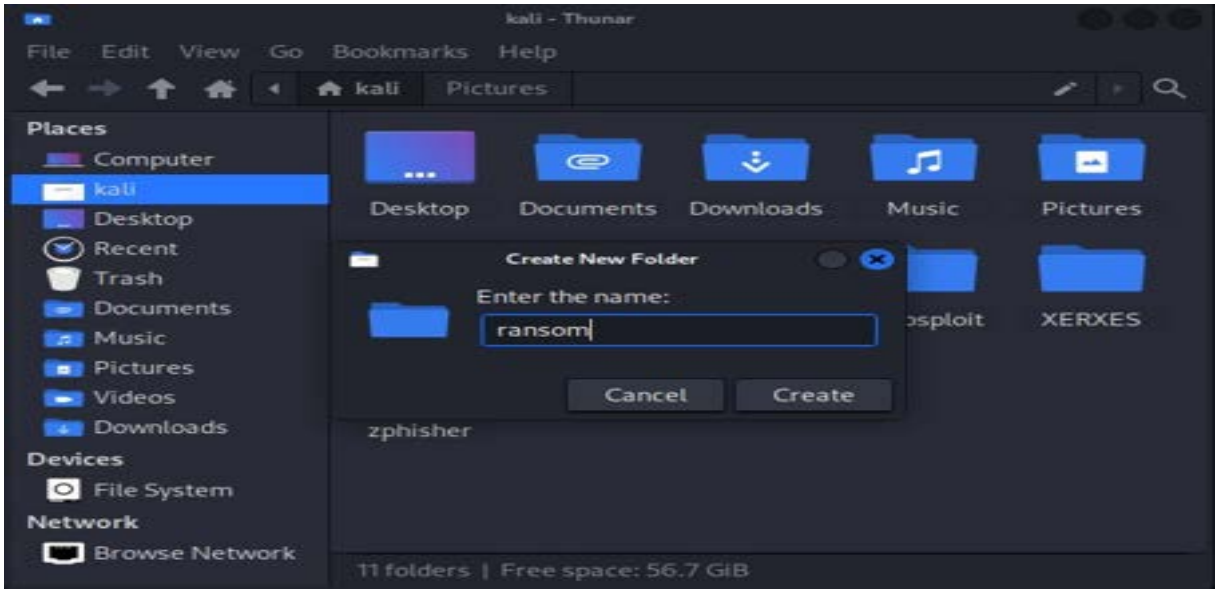
- Use reliable anti-malware or anti-ransomware software to scan and remove ransomware from your system

Implementation of Ransomware using Virtual Box [Kali Linux]

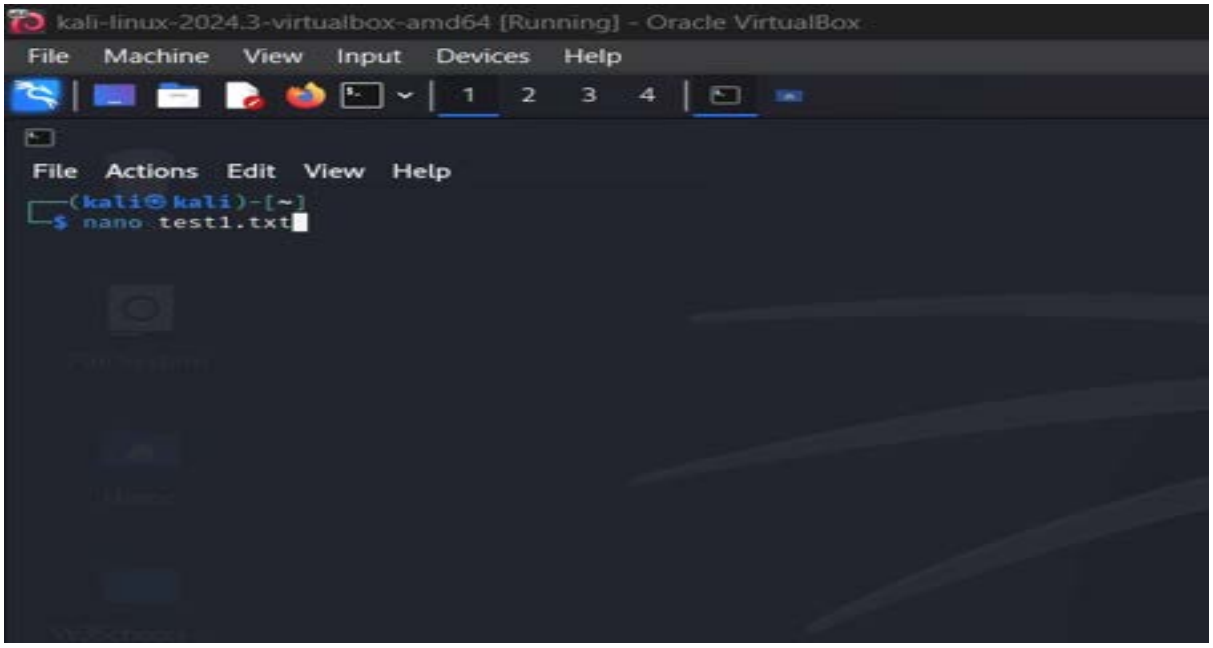
1.

Step 1: Go to Kali Linux

Step 2: Create a new folder as ‘ransom’

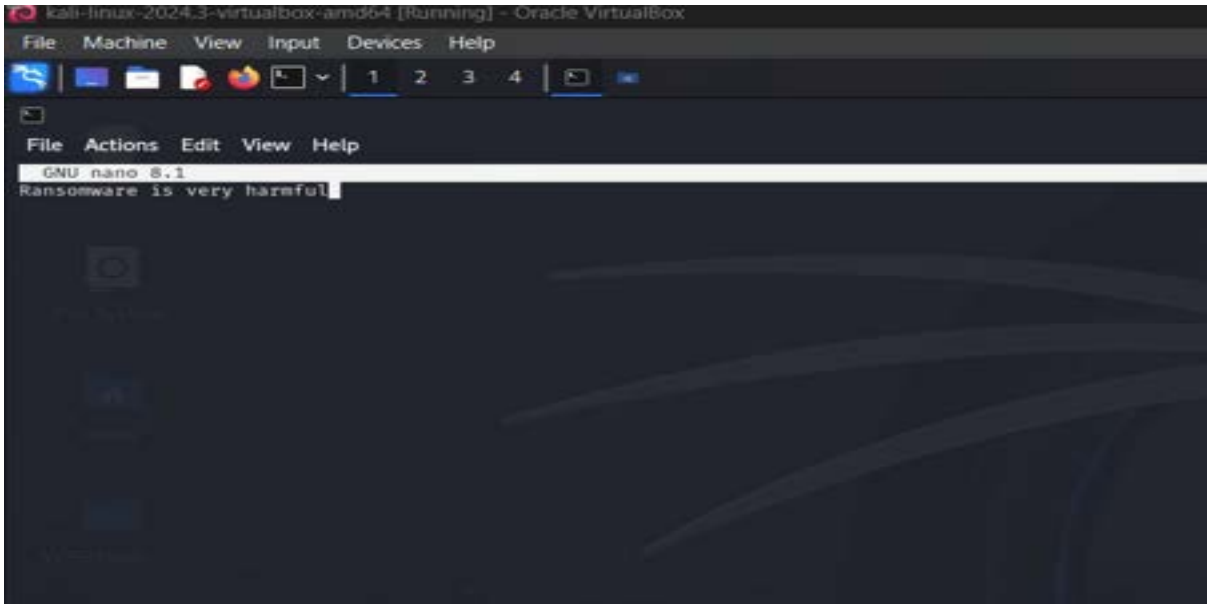


Step 3: Open command prompt and give a command to create text



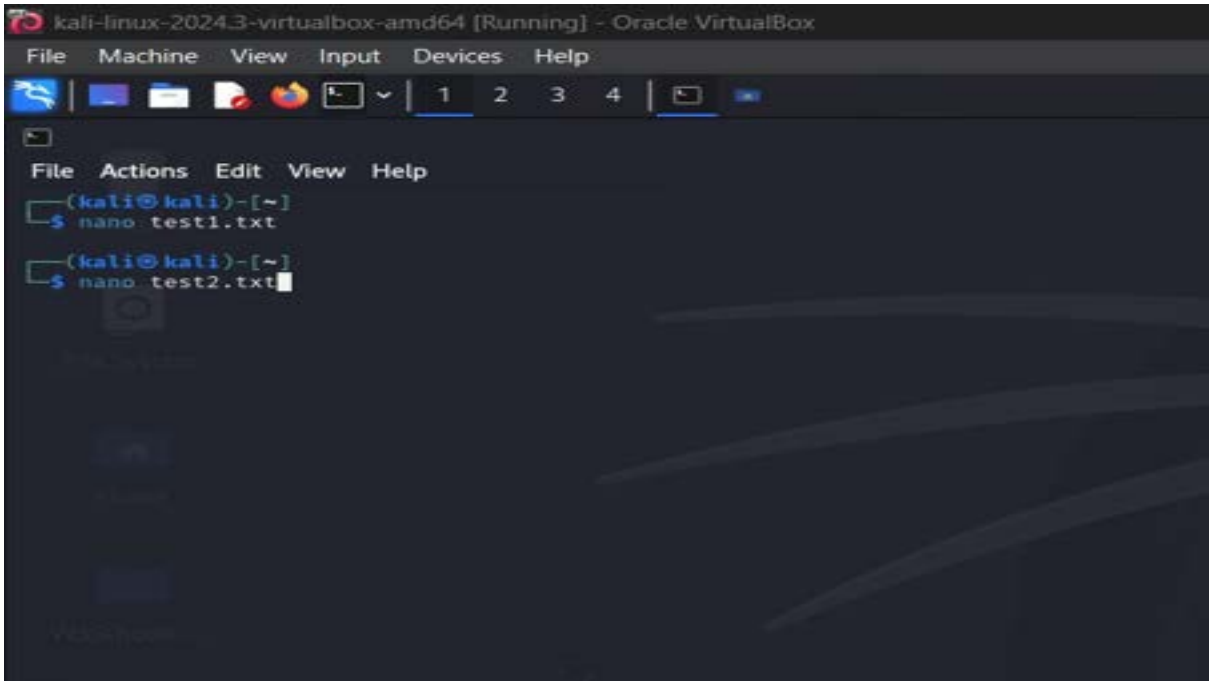
Step 4: click Enter

Enter some text



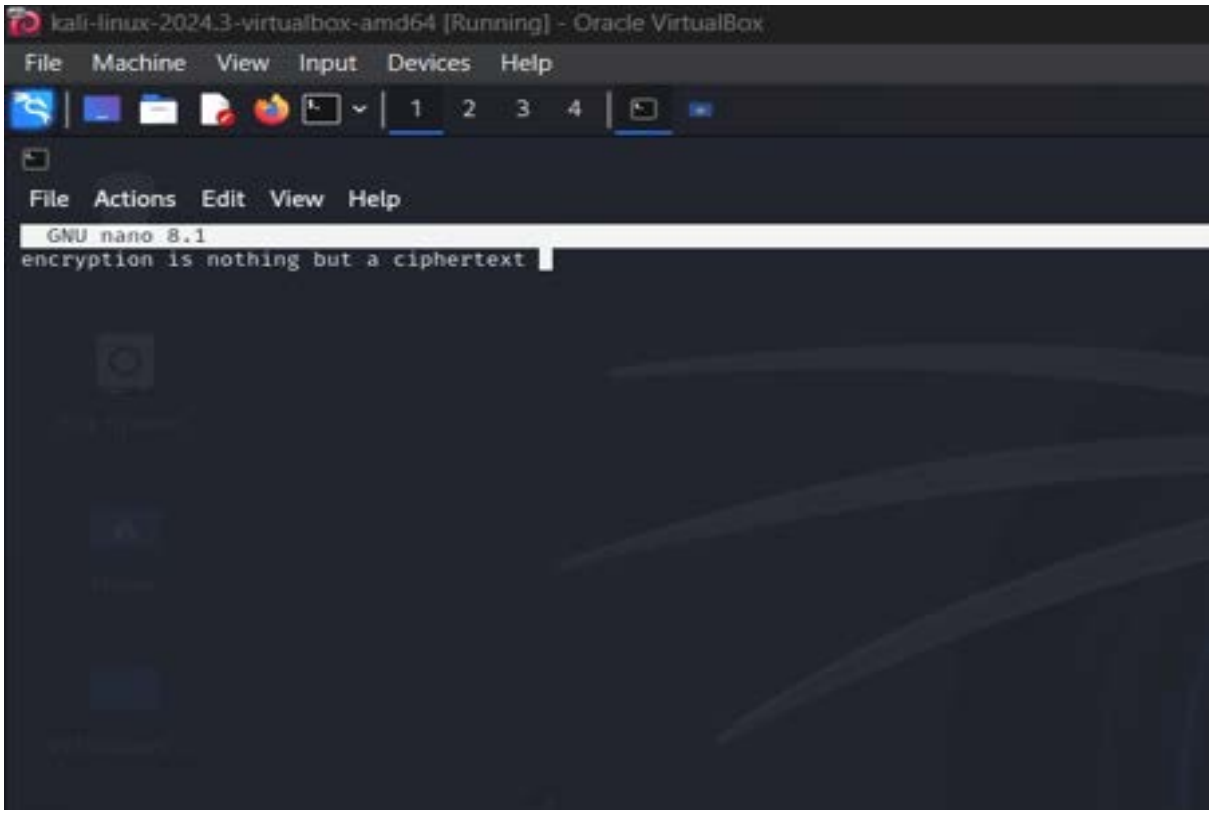
To save this click CTRL+X+Y+ENTER simultaneously, it redirected to command prompt.

Step 5: Giving command to create another text



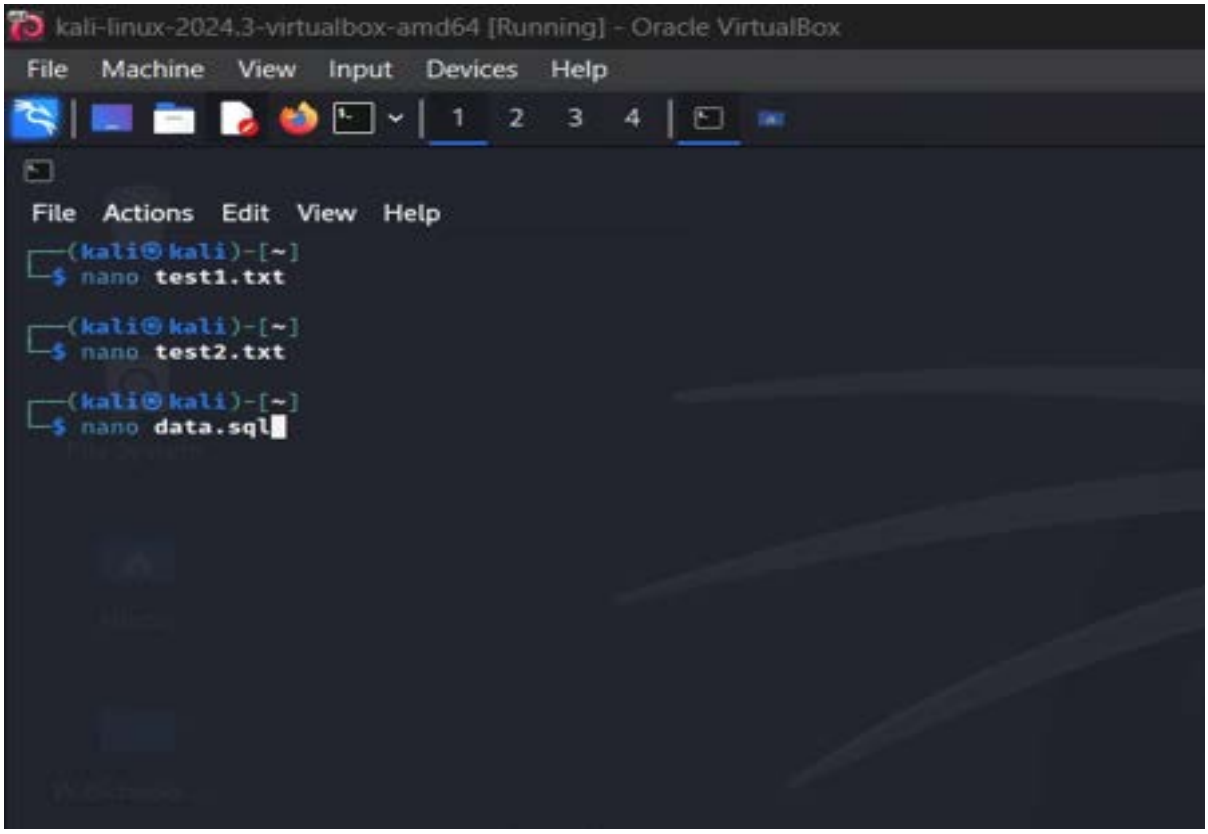
Step 6: click Enter

Again Enter some text

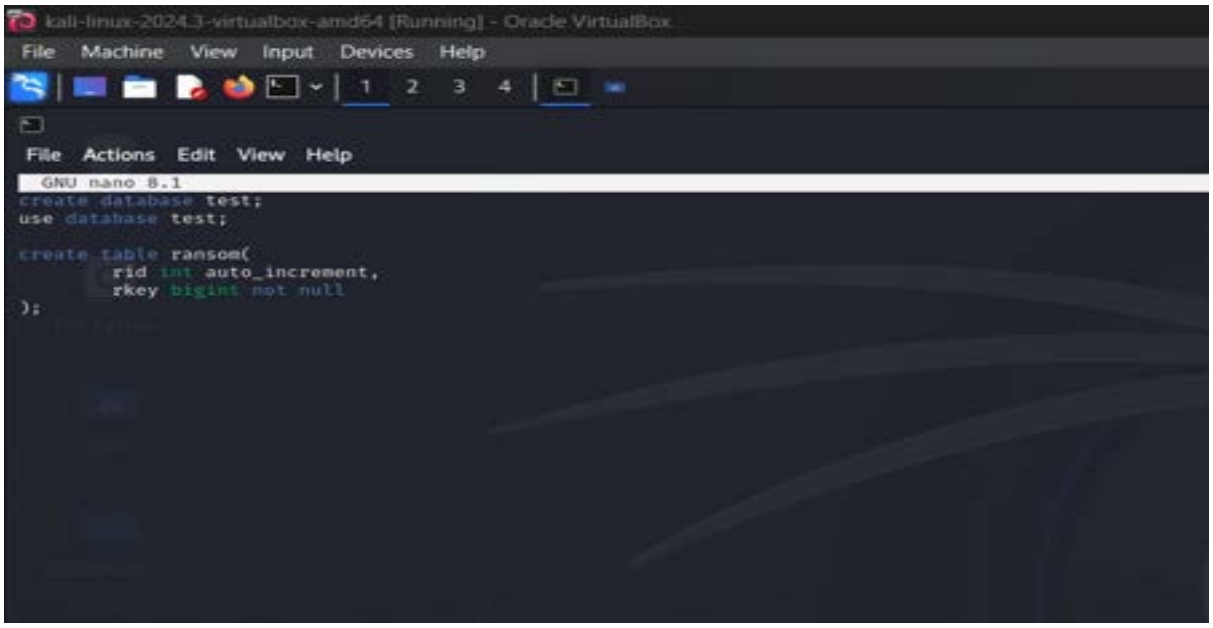


To save this click CTRL+X+Y+ENTER simultaneously, it redirected to command prompt

Step 7: Here, giving command to create Data SQL



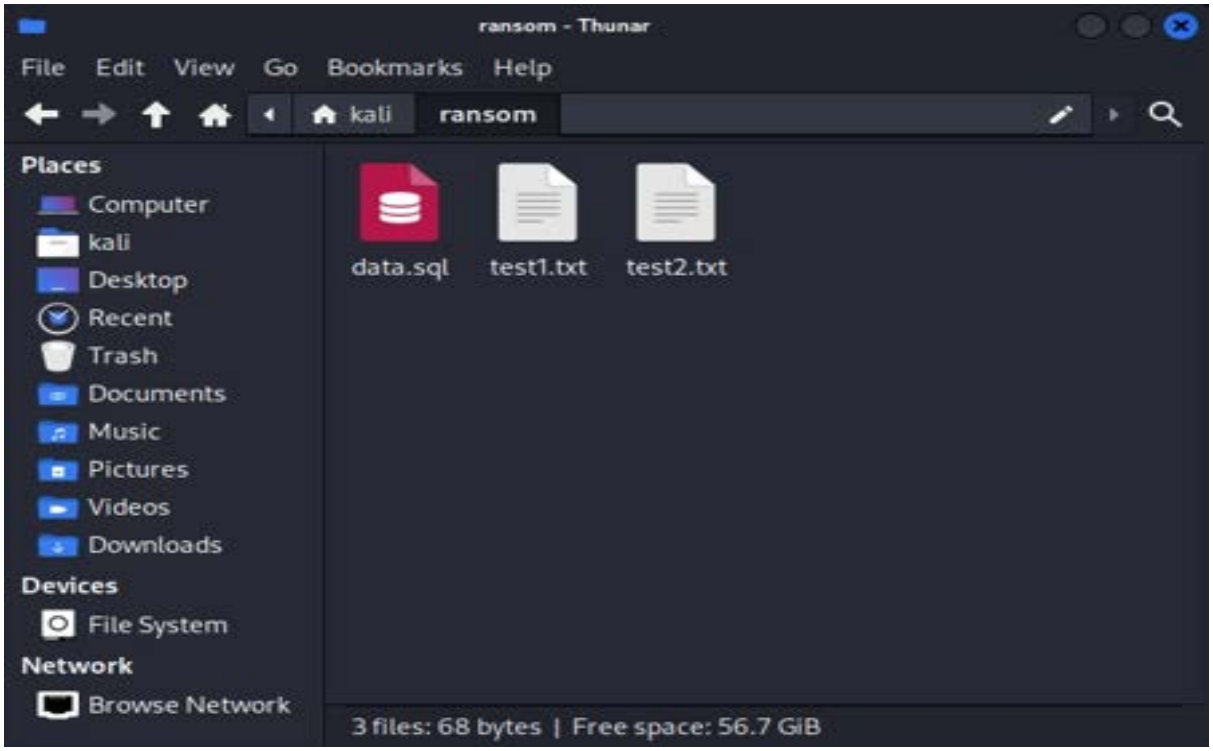
Step 8: Again click Enter
Giving database test



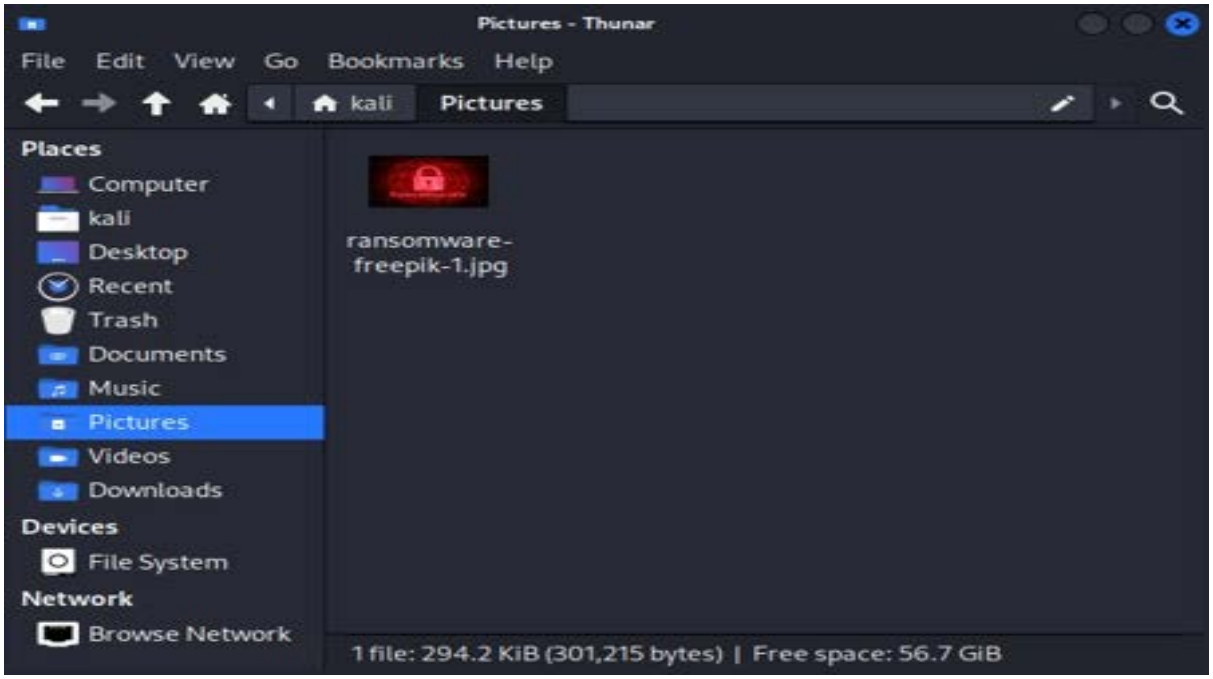
To save this click CTRL+X+Y+ENTER simultaneously, it redirected to command prompt

Step 9: We can see the saved files in kali

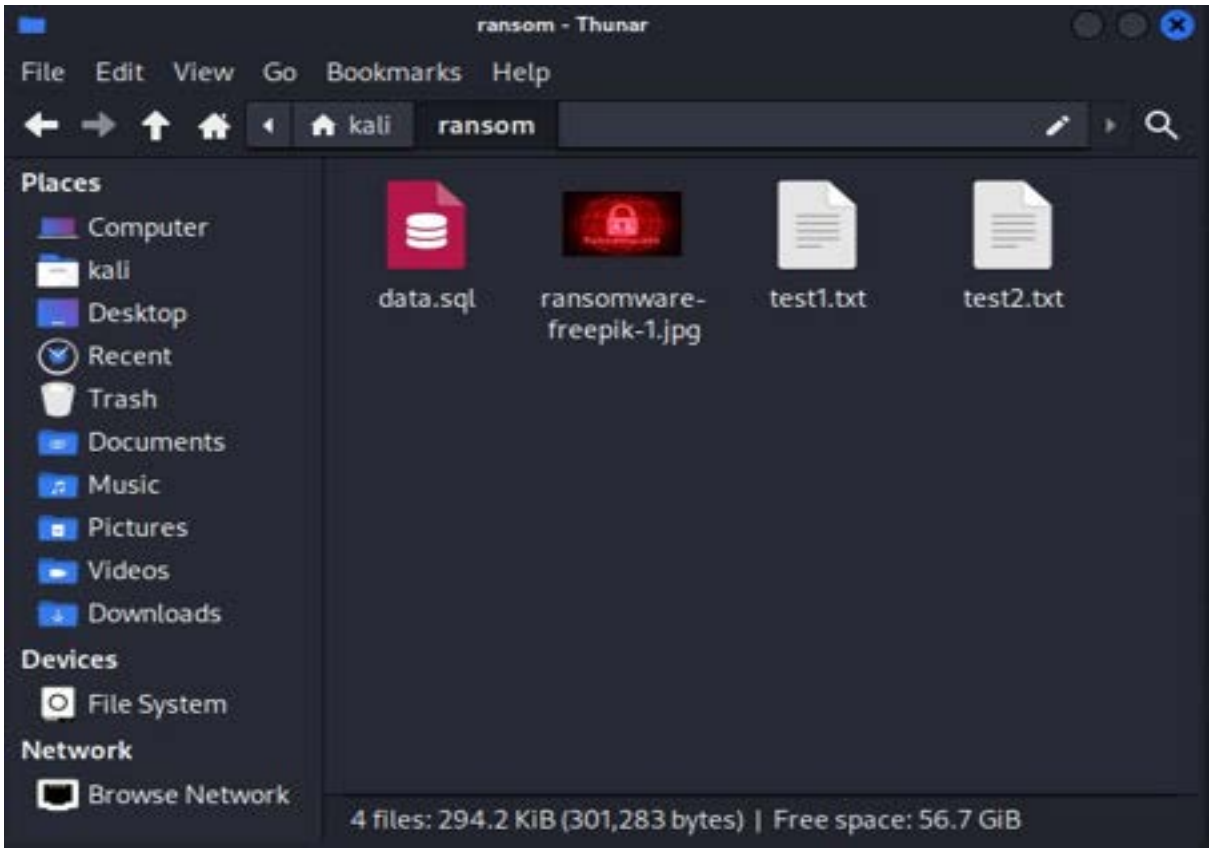
Step 10: Store all the three files in ransom folder



Step 11: Download some picture

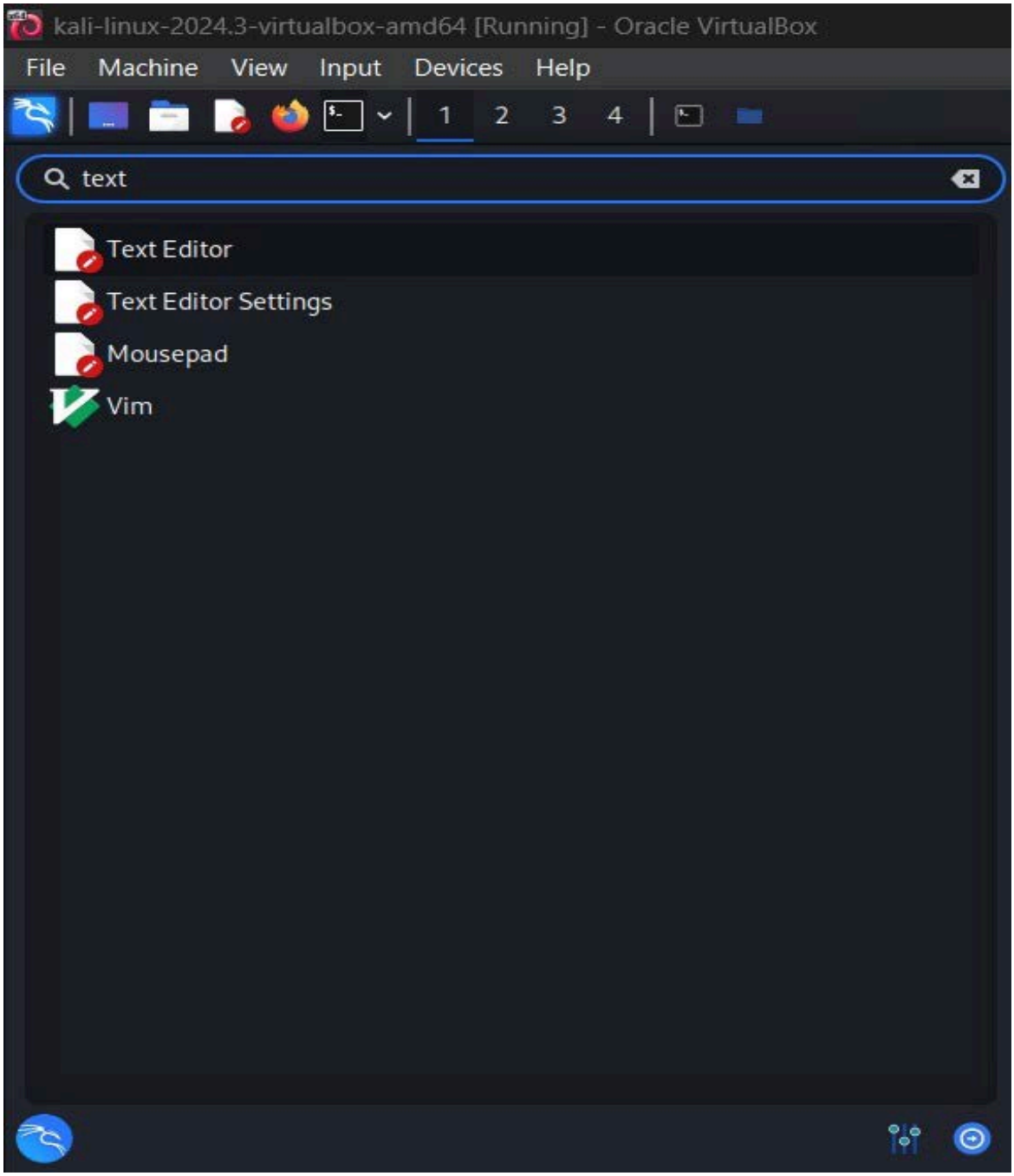


Step 12: Store that picture in ransom folder

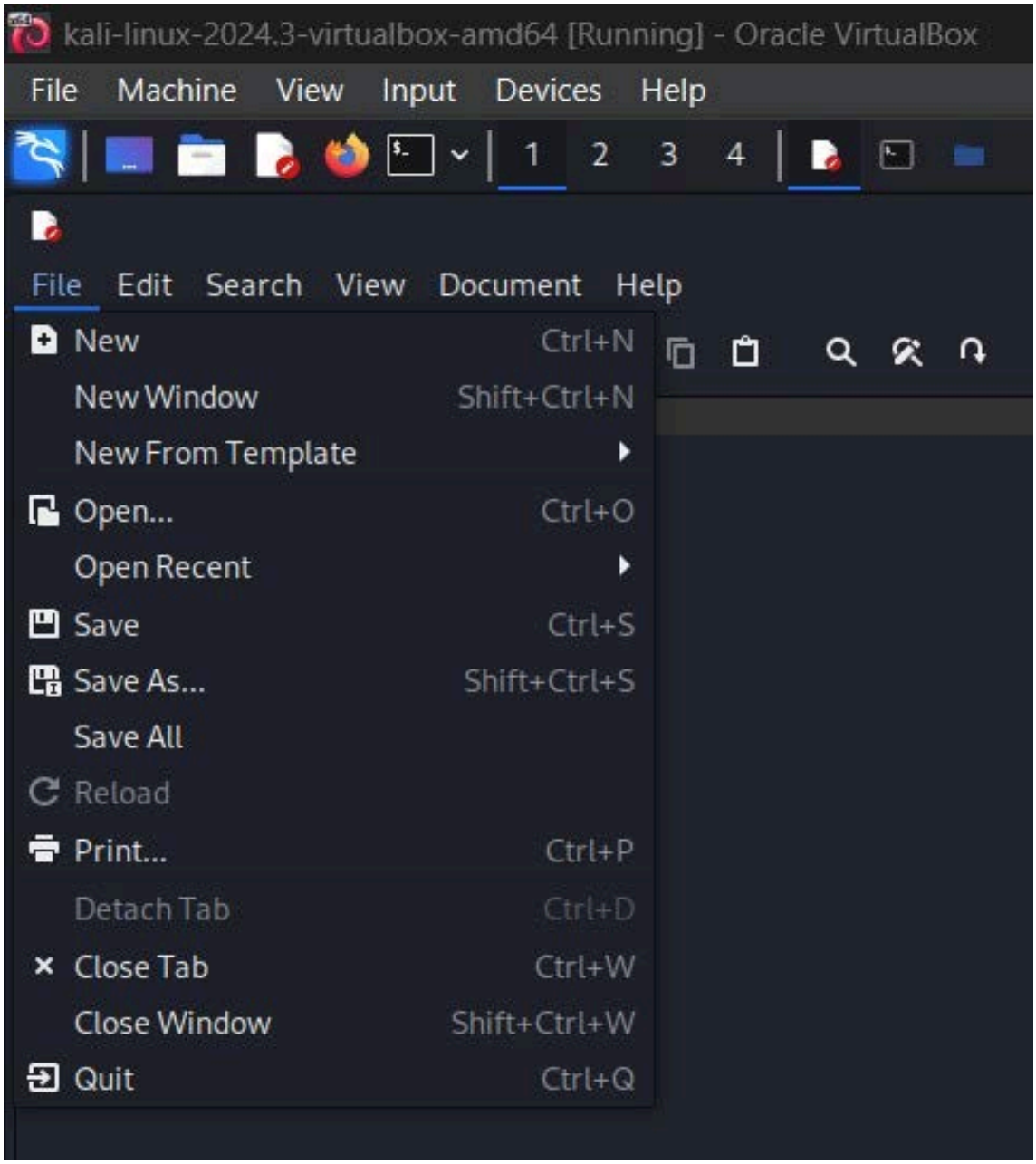


<u>ENCRYPTION</u>:

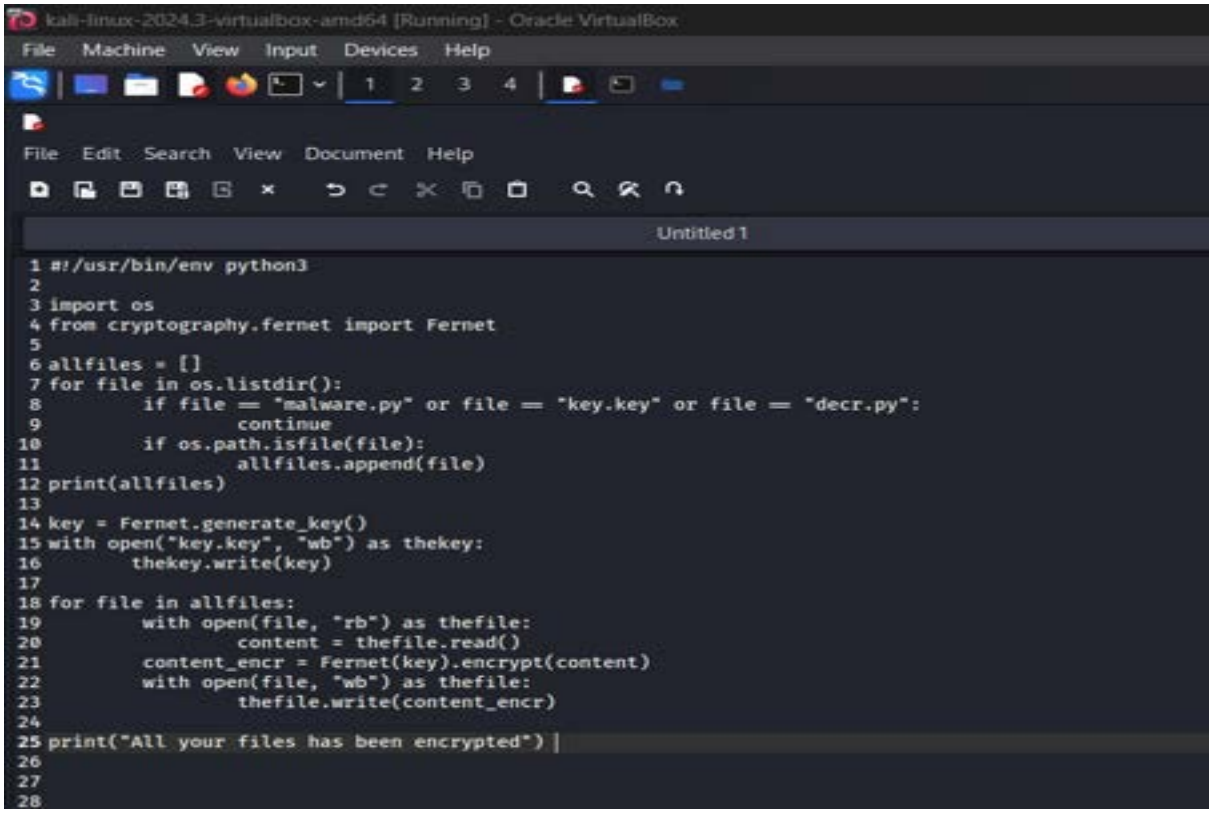
Step 13: Now, Go to text Editor



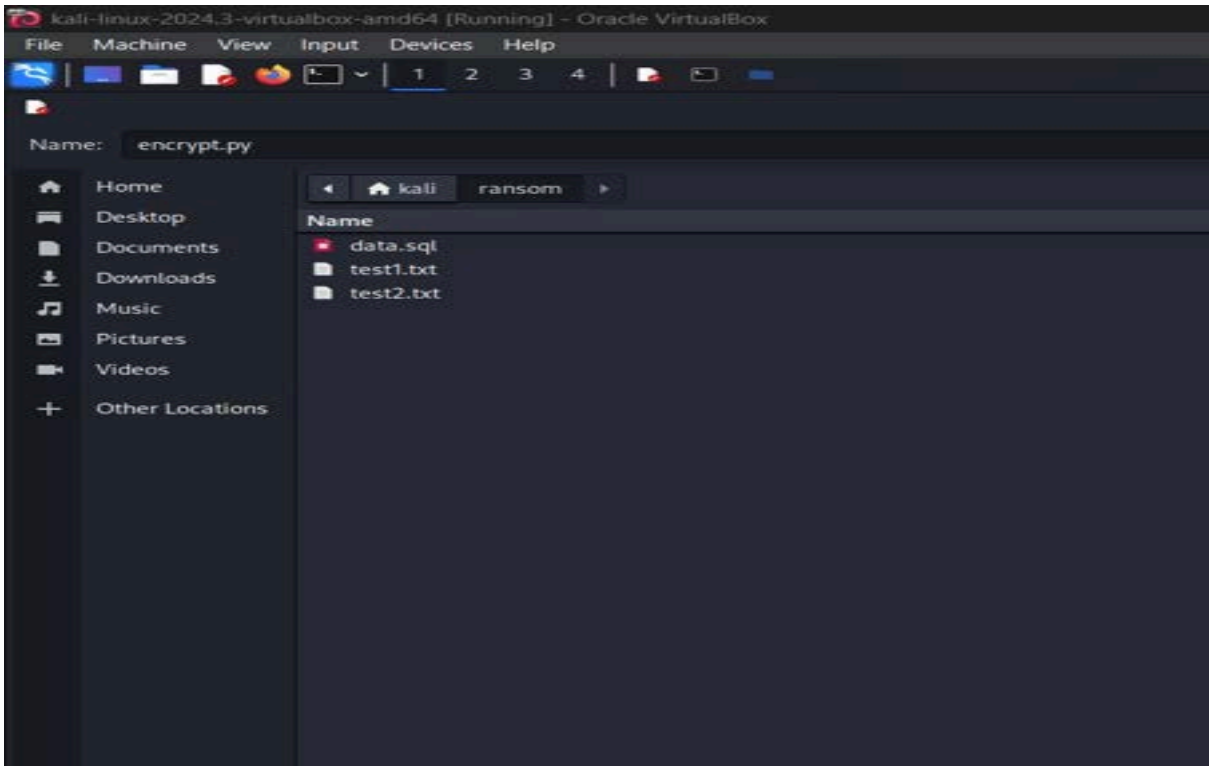
Step 14: Take a new file

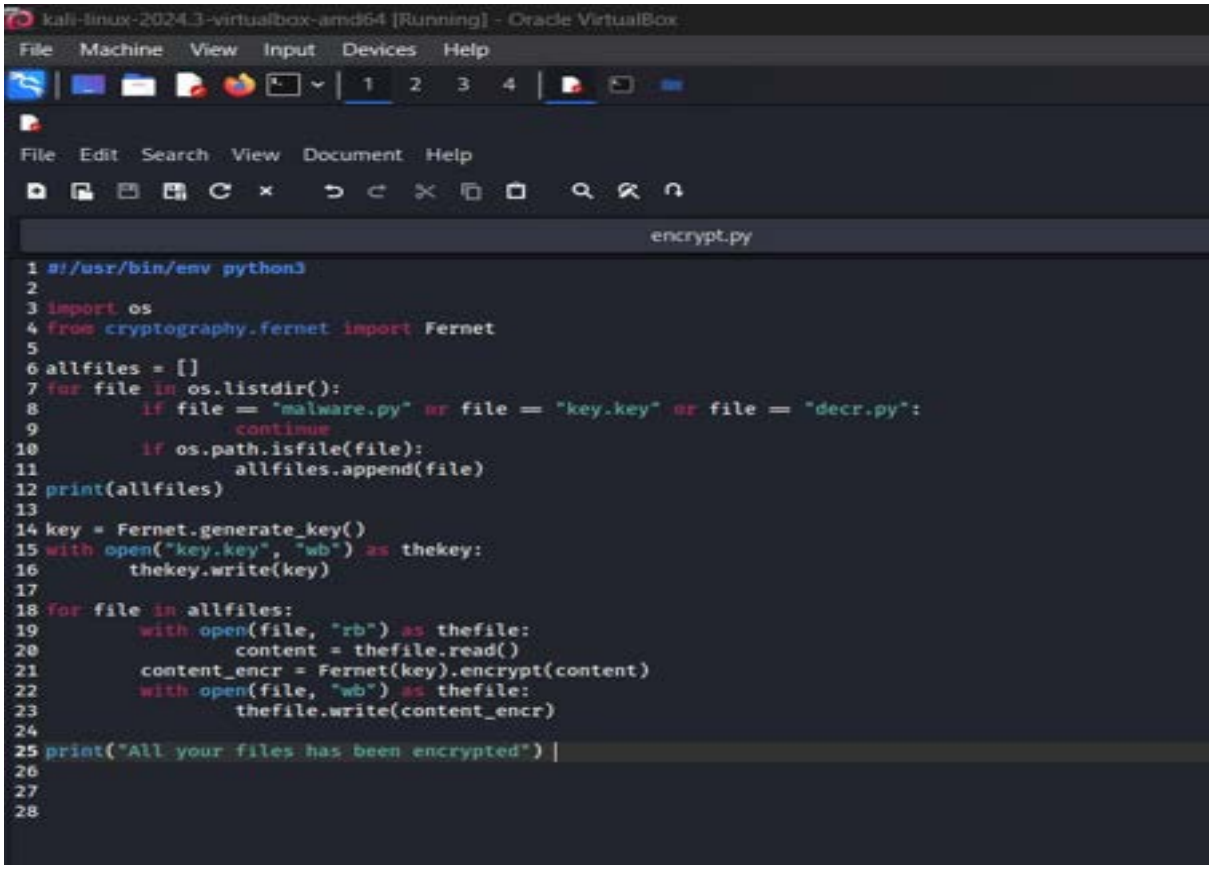


Step 15: Enter the Encrypt code

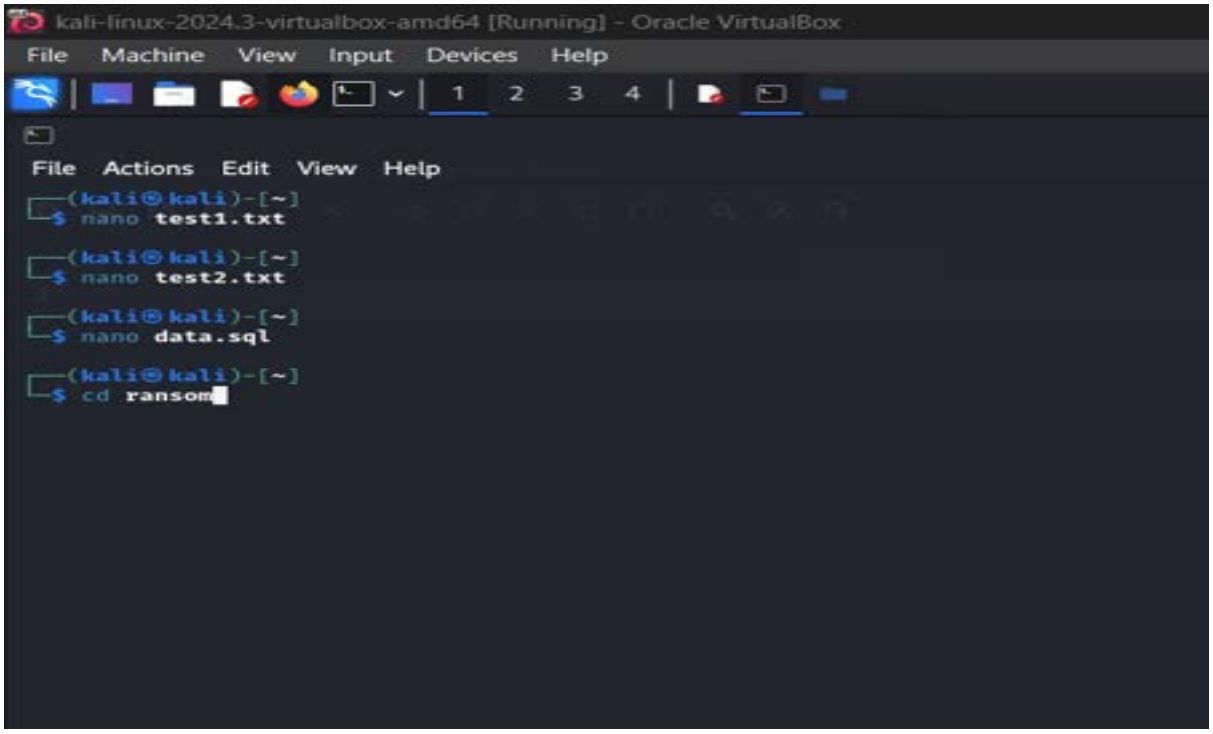


Step 16: Save it as encrypt.py

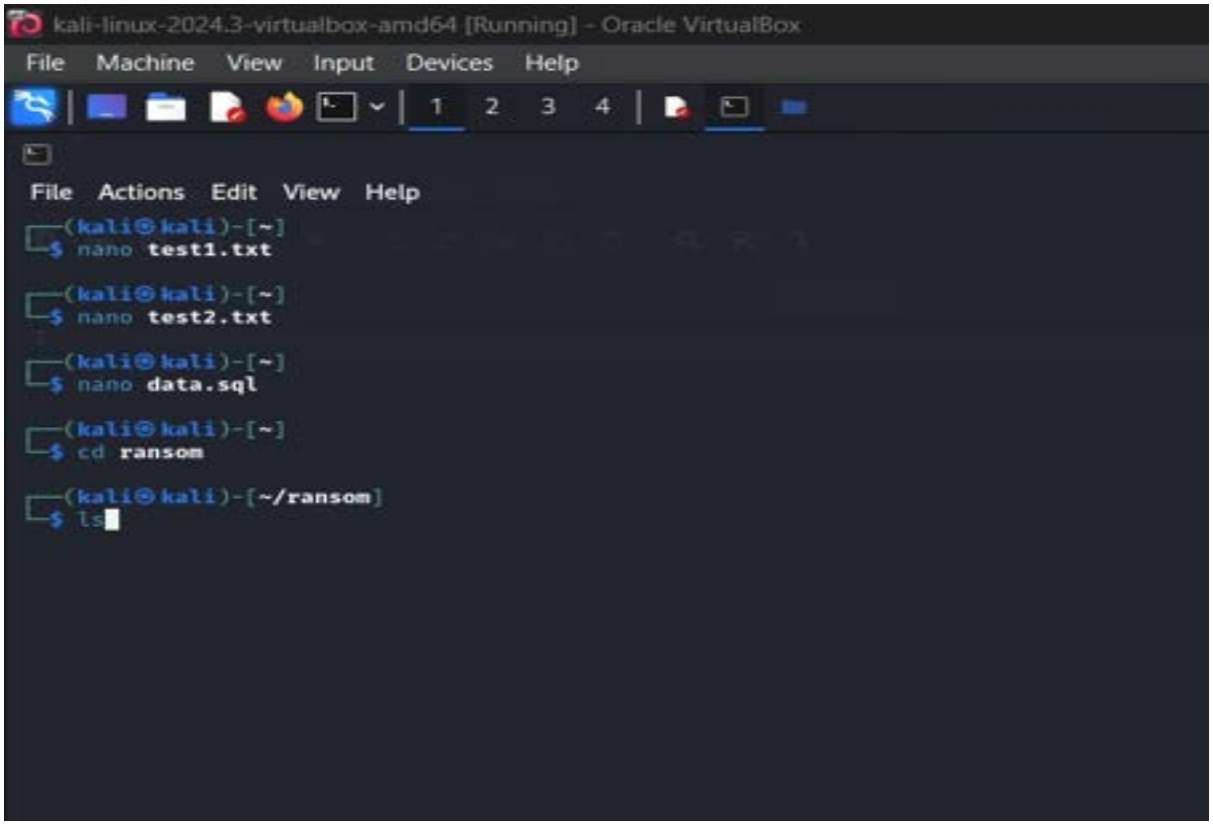




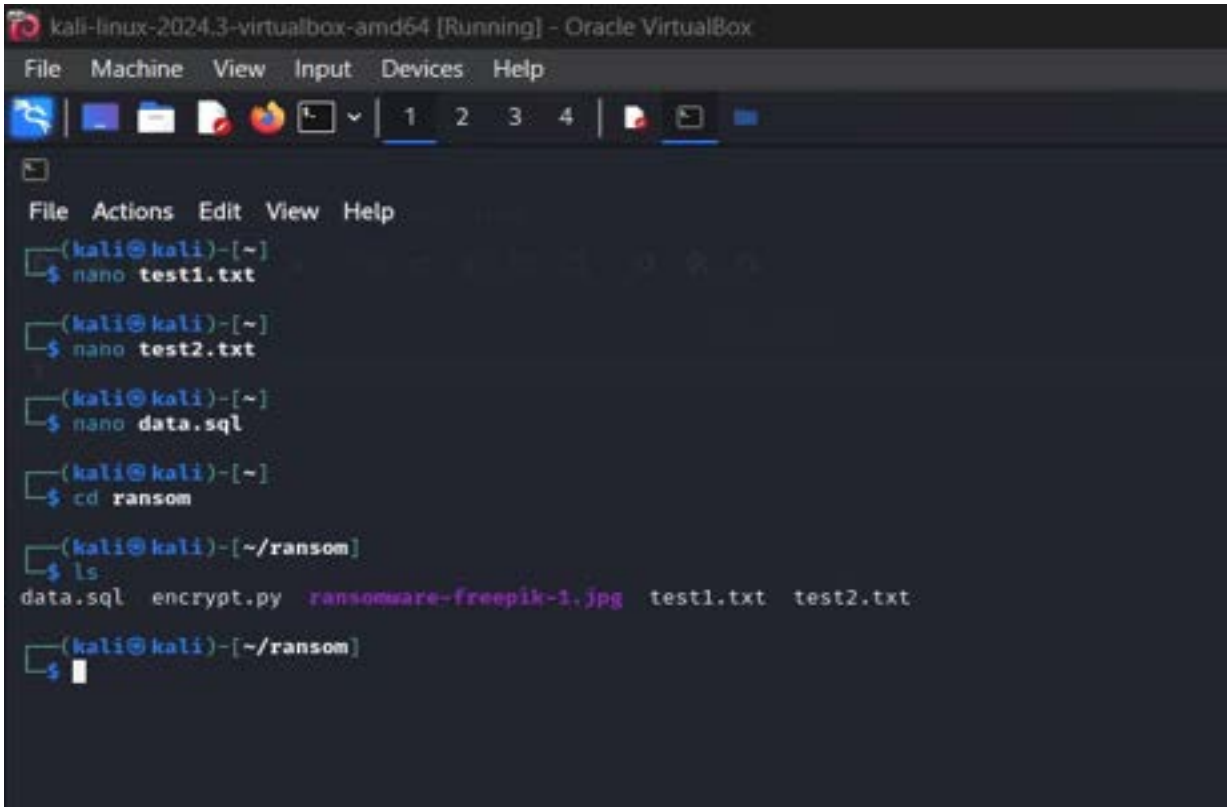
Step 17: Open command prompt and give the command ‘cd ransom’



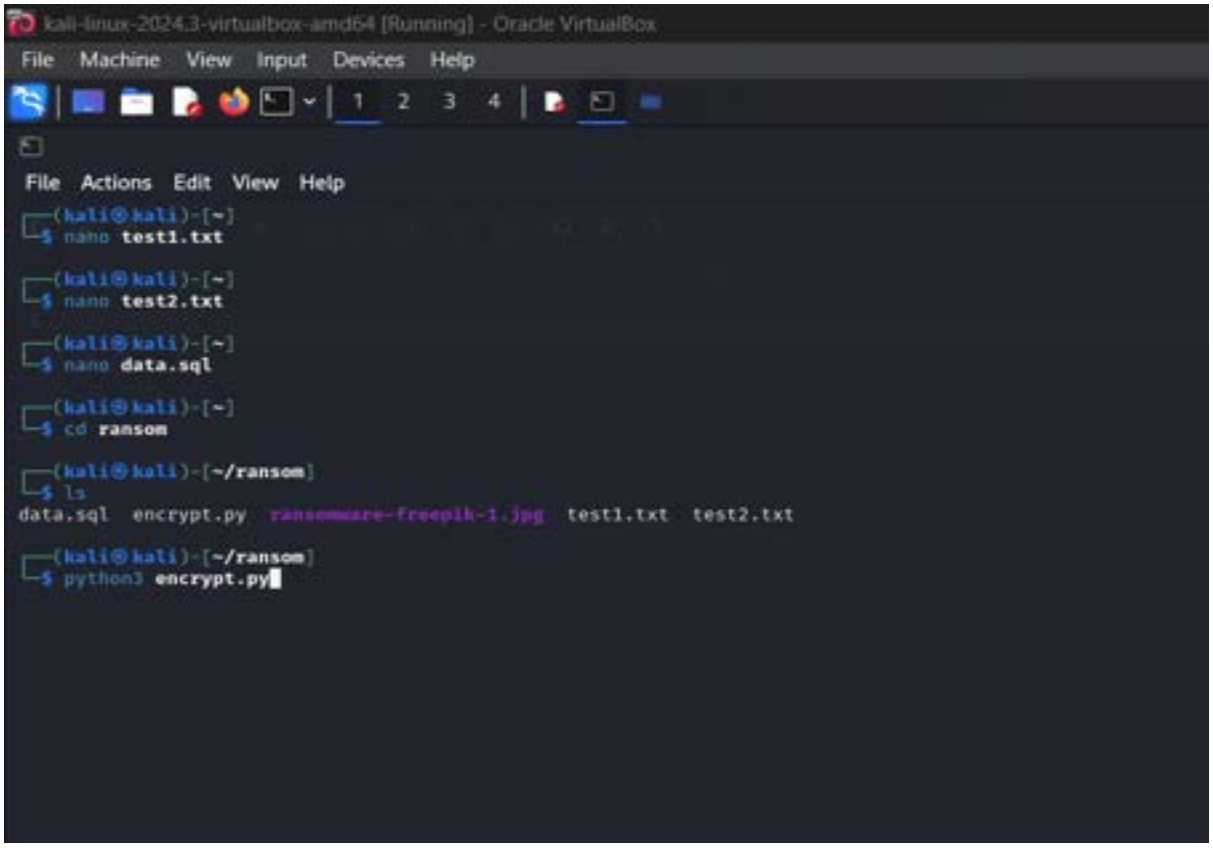
Step 18: Give ls and click Enter



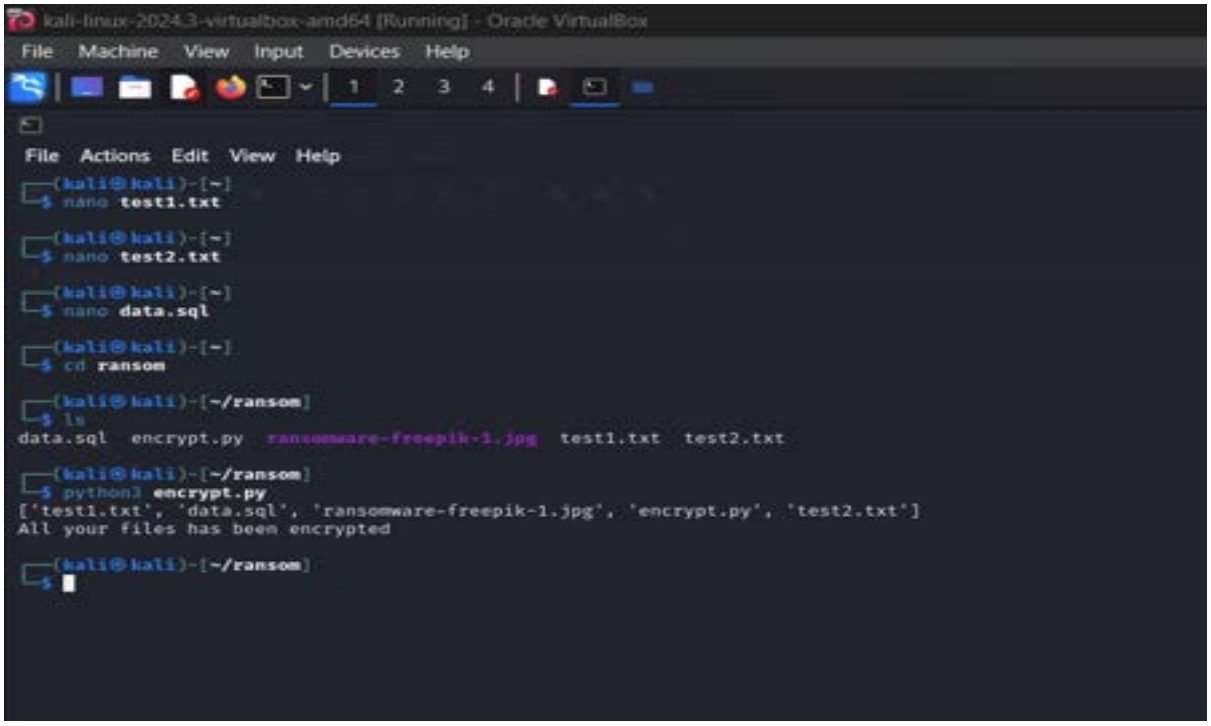
We can able to see the saved files which are in ransom folder



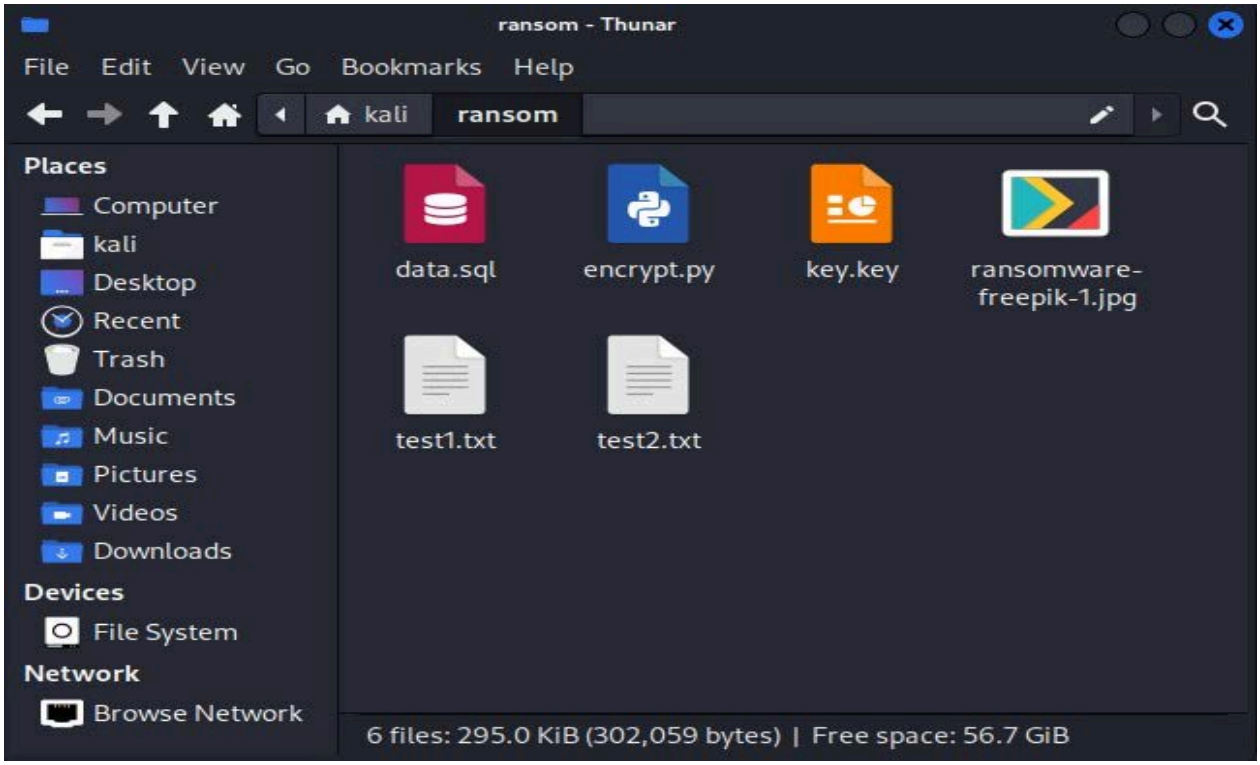
Step 19: Enter the saved file(encrypt.py)

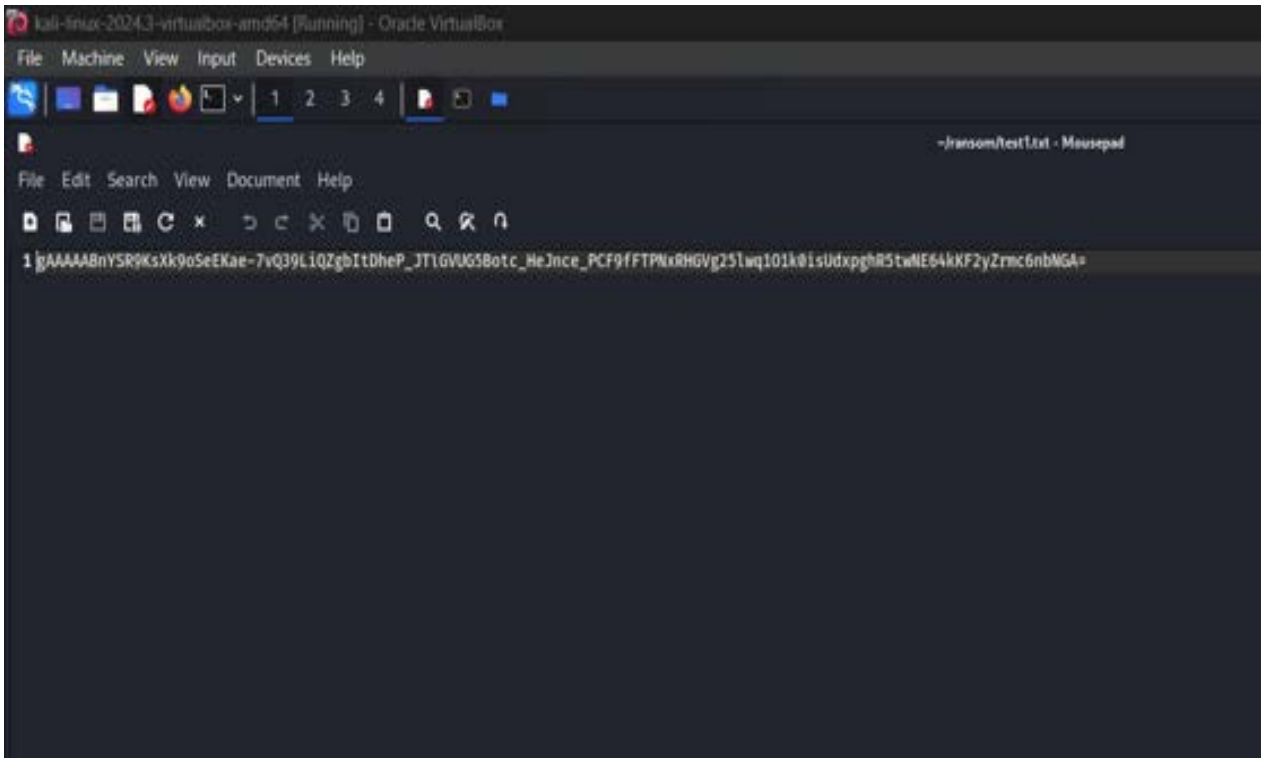


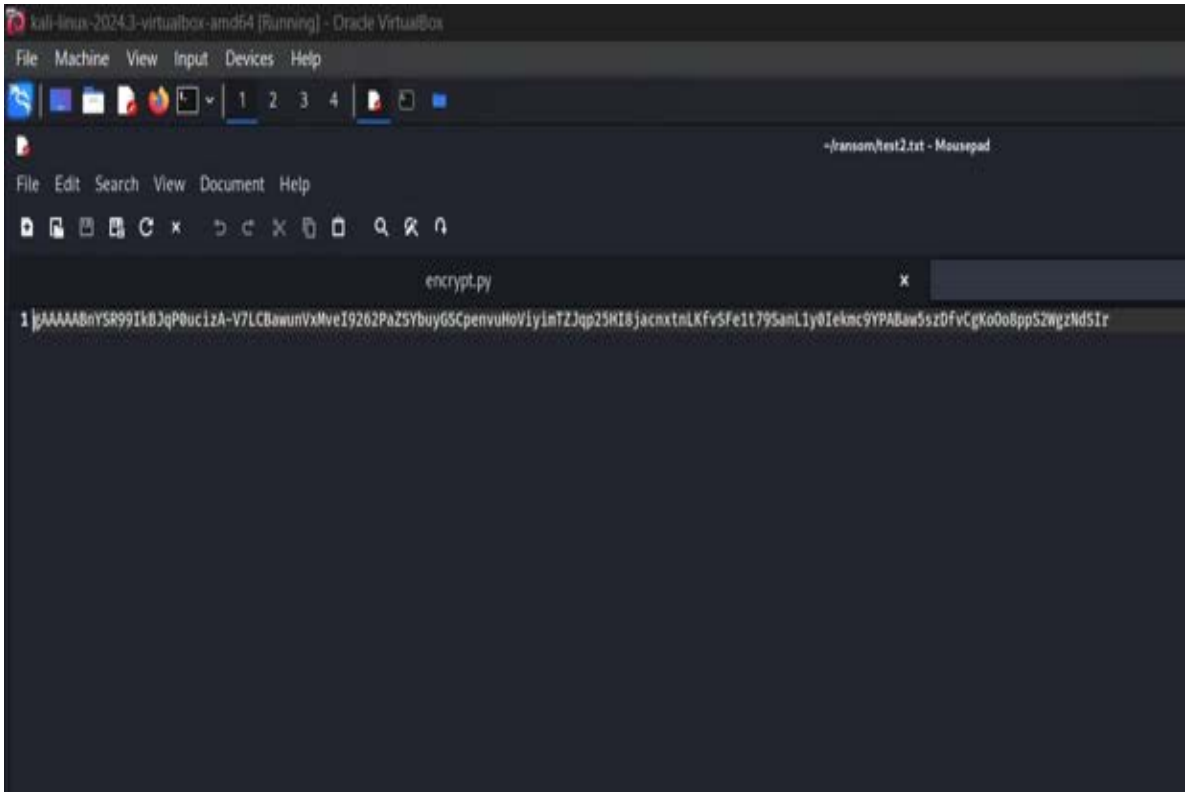
Step 20: Here, we can see all the files are encrypted

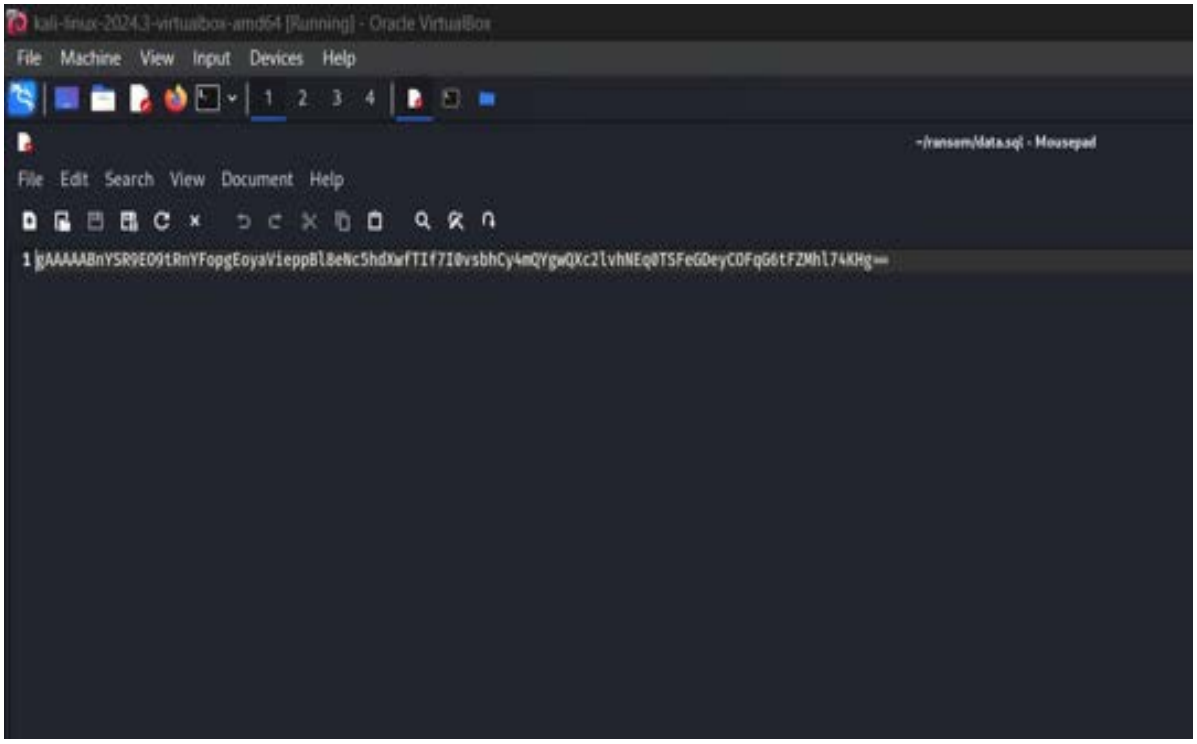


Encrypted files:





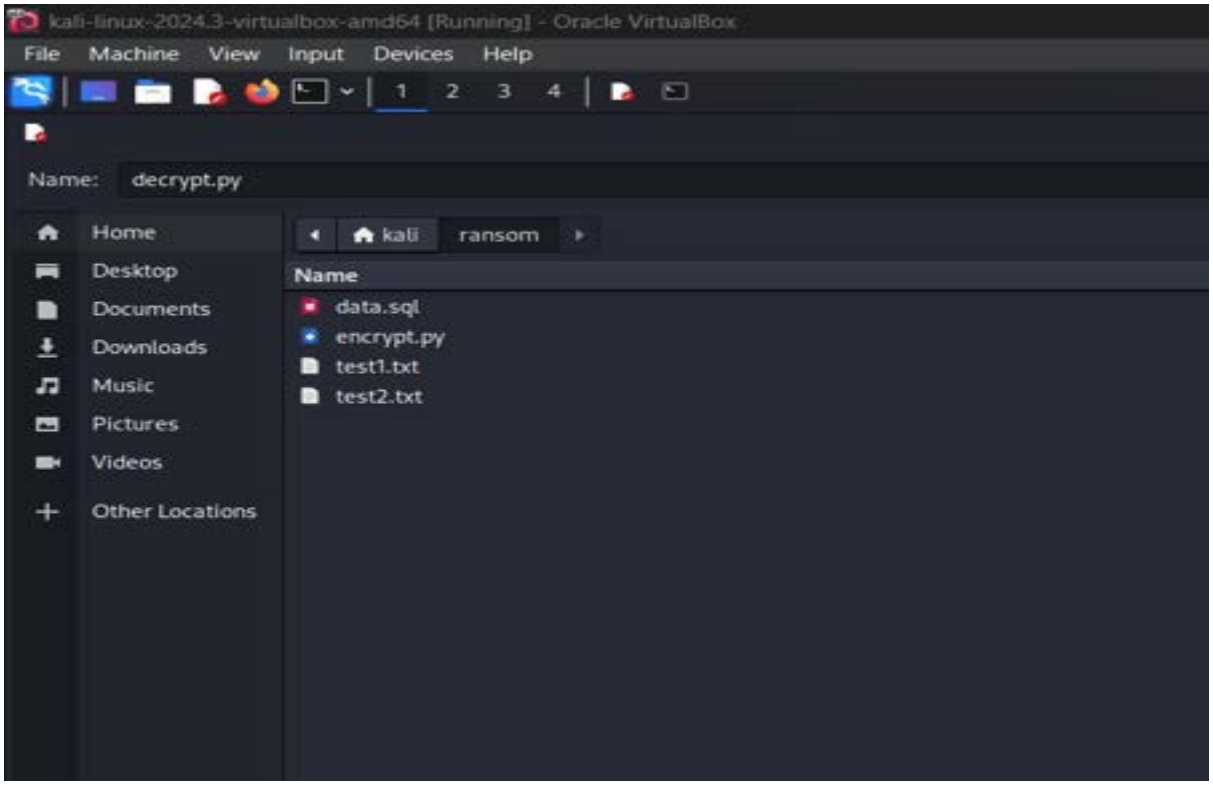

kali-linux-2024.3-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
~/ransom/test2.txt - Mousepad
File Edit Search View Document Help
encrypt.py
1 gAAAAABnYSR99IkBJqP0ucizA-V7LCBawunVxMveI9262PaZSYbuyG5CpenvuHoViyimTZJqp25KI8jacnxtnLKfvSfe1t795anL1y0IekmcSYPABaw5szDfvCgKoOo8ppS2WgzNdSIr


kali-linux-2024.3-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
~/ransom/data.sql - Mousepad
File Edit Search View Document Help
1 gAAAAABnYSR9EO9tRnYFopgEoyaVieppBl8eNc5hdXwfTIf7I0vsbhCy4mQYgwQXc2lvhNEq0TSFeGDeyCOFqG6tFZMhl74KHg==

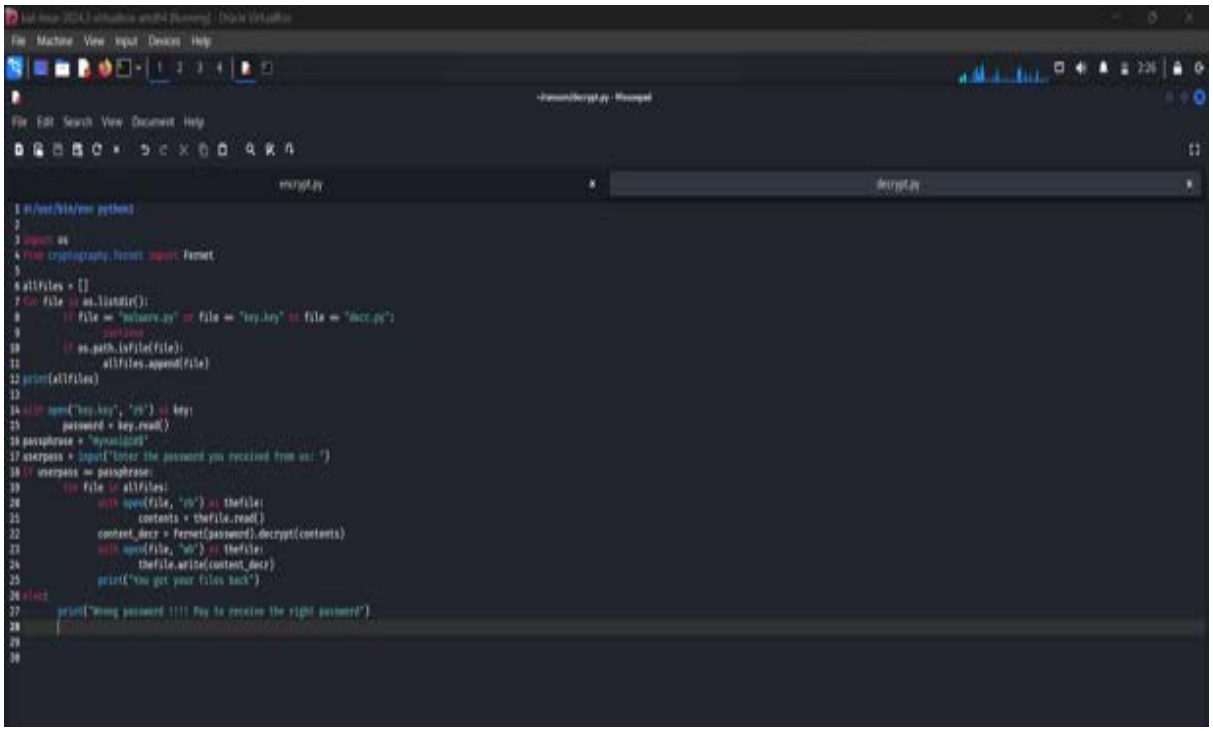
ALL THE FILES ARE ENCRYPTED

DECRYPTION:

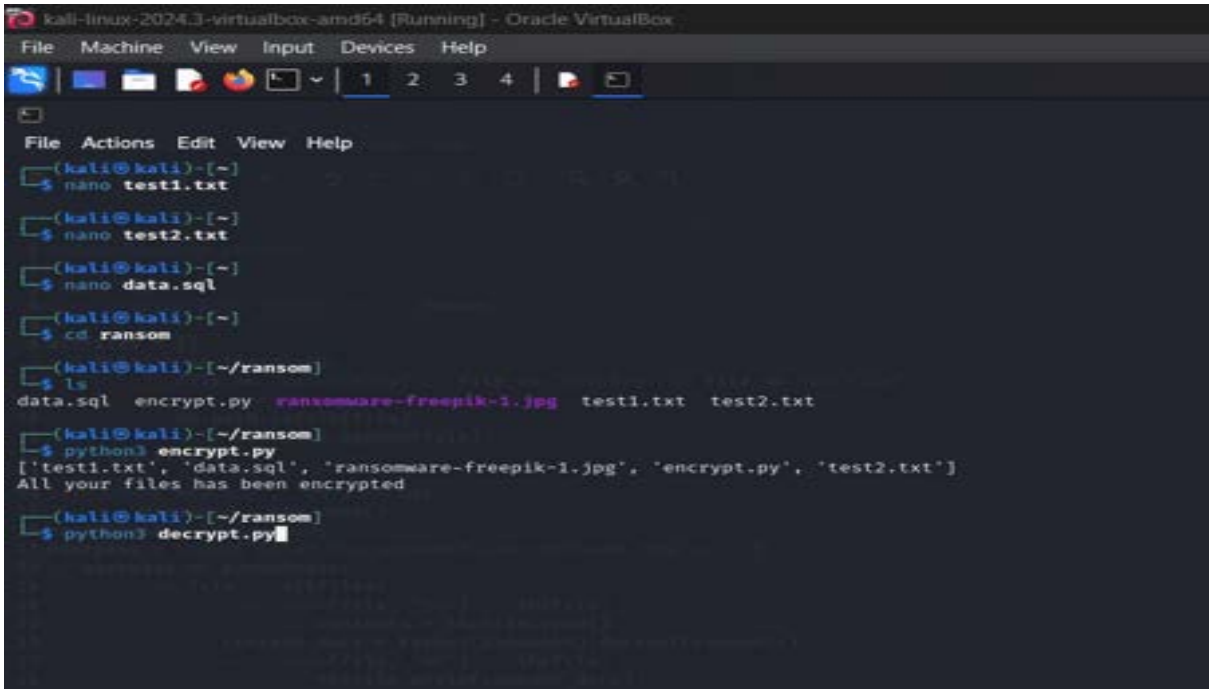
Step 21: Now, take a new file and save it as decrypt.py



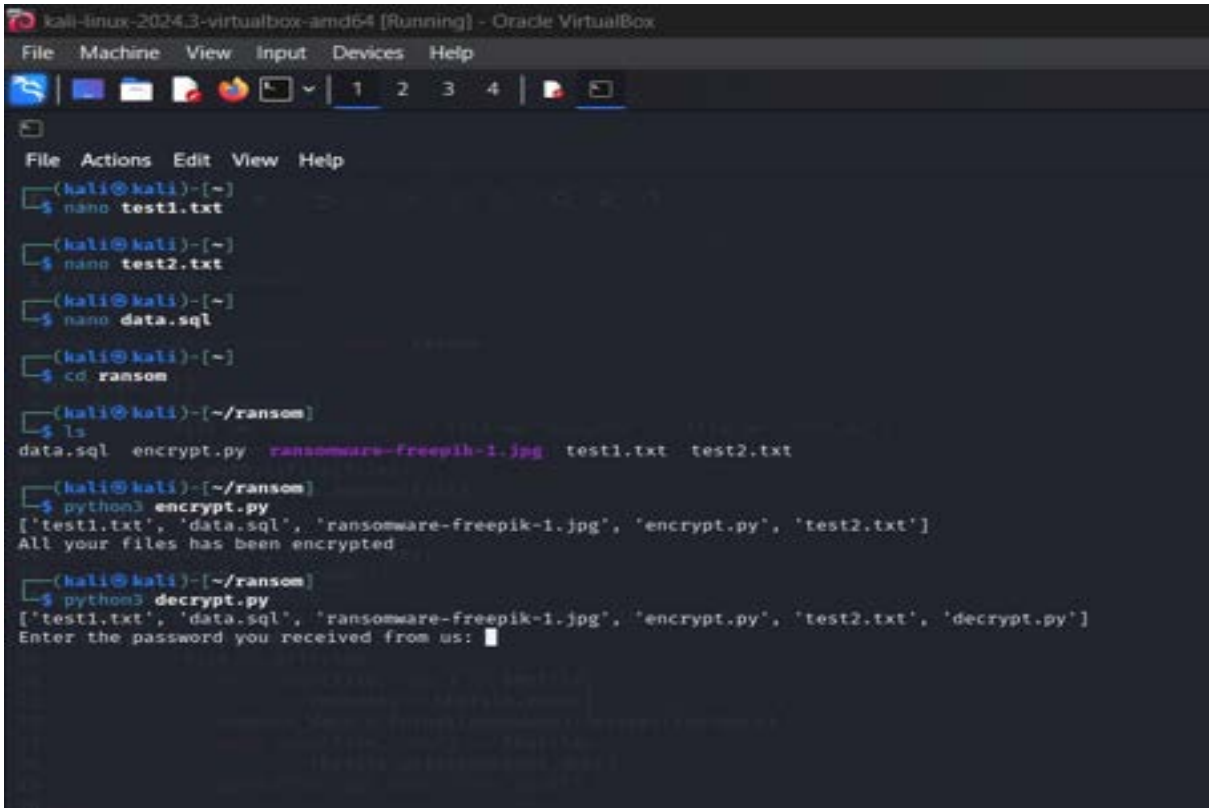
Step 22: Enter the decrypt code



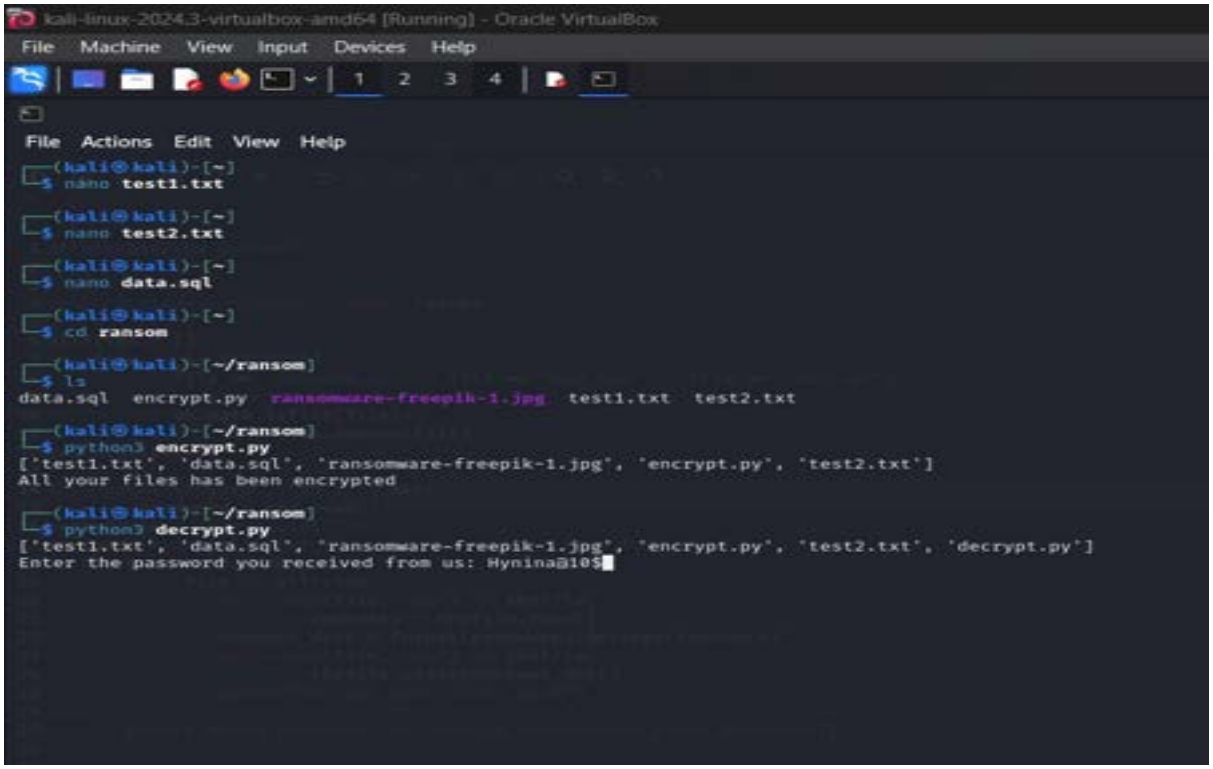
Step 23: Open command prompt and type decrypt.py



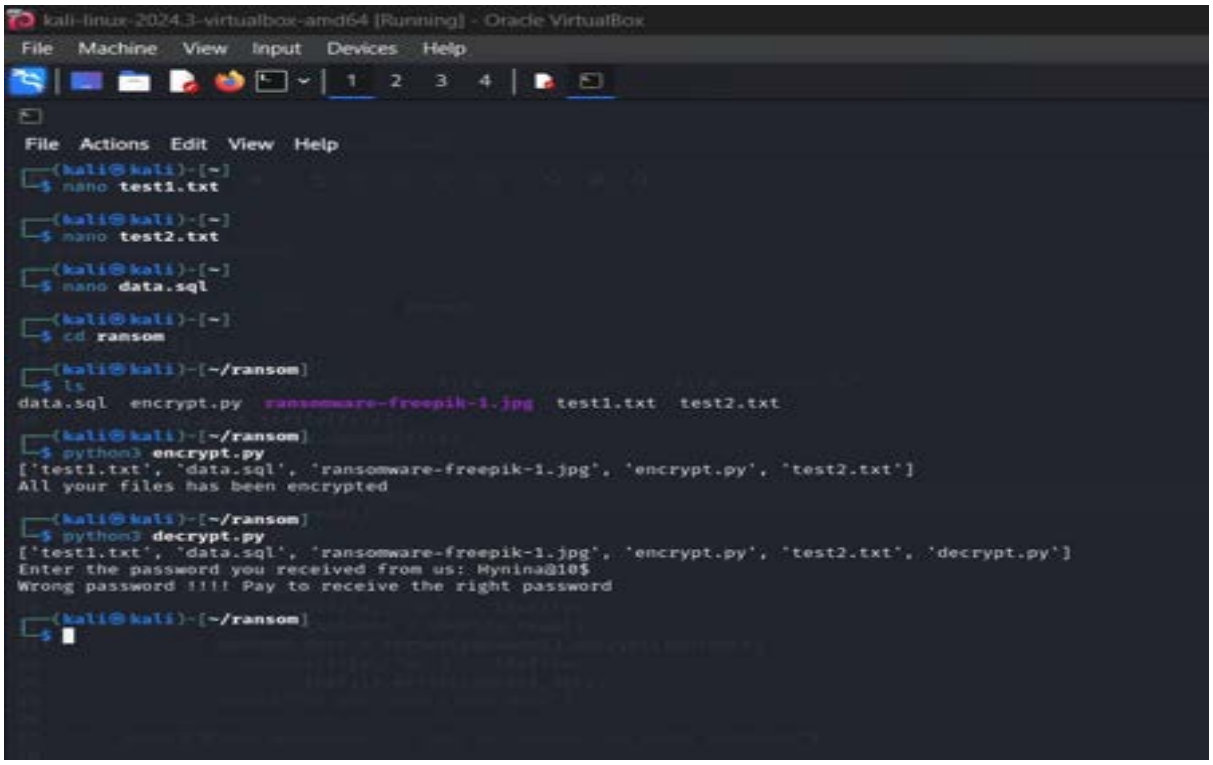
Step 24: Now, it shows us all the saved files which are in ransom folder & and gives us a command



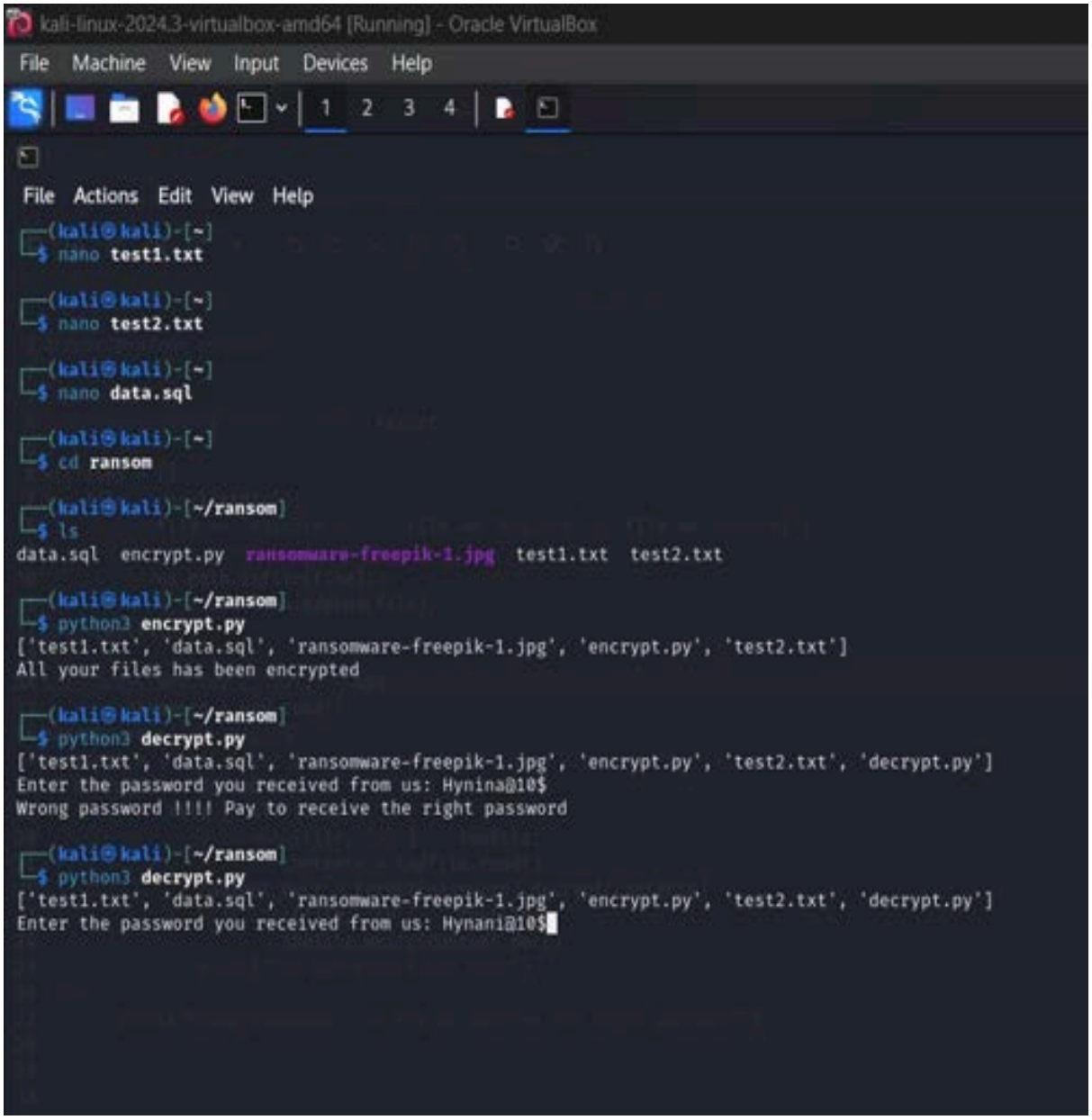
Step 25: Enter the password



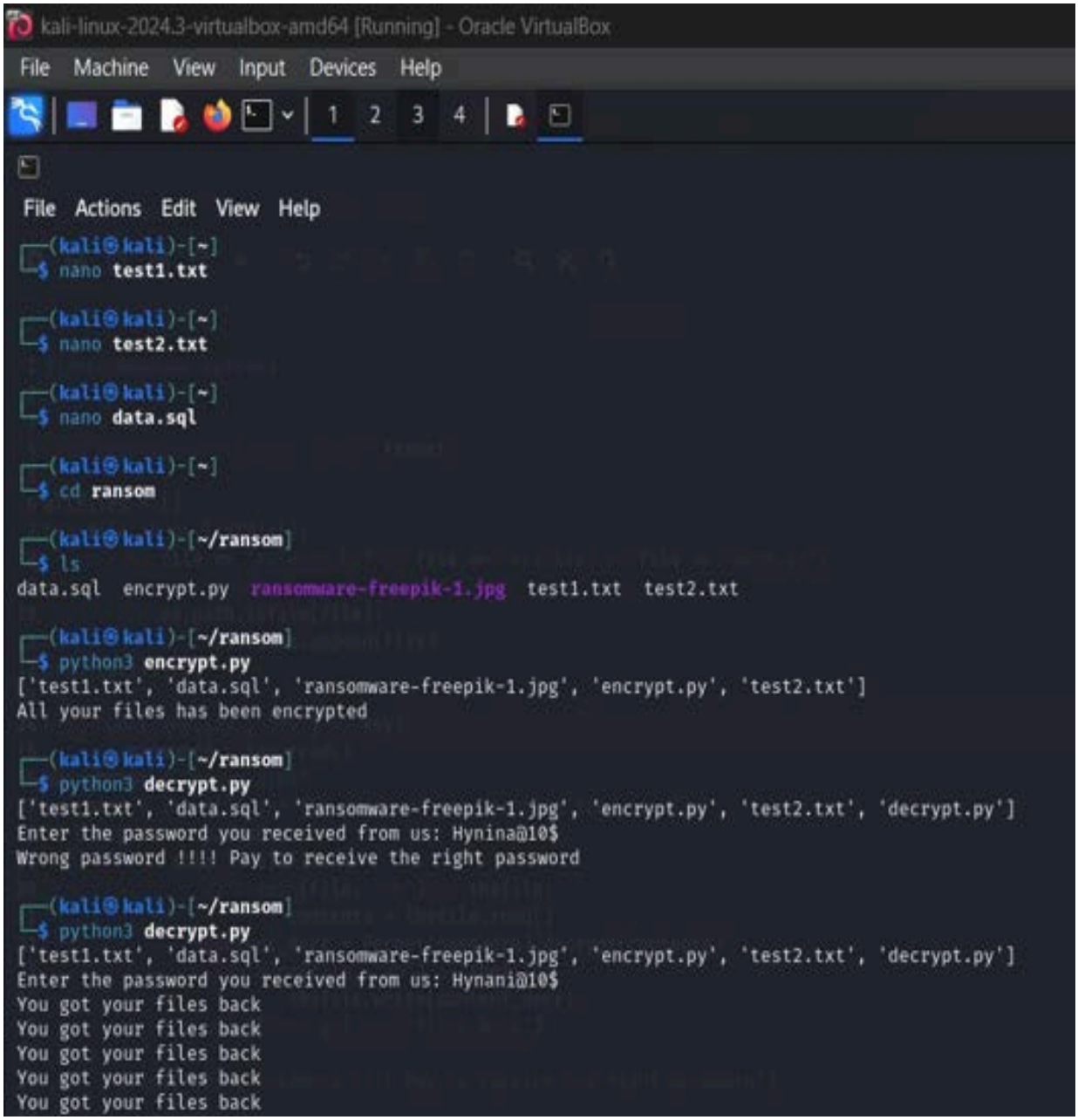
Step 26: If we enter the wrong password



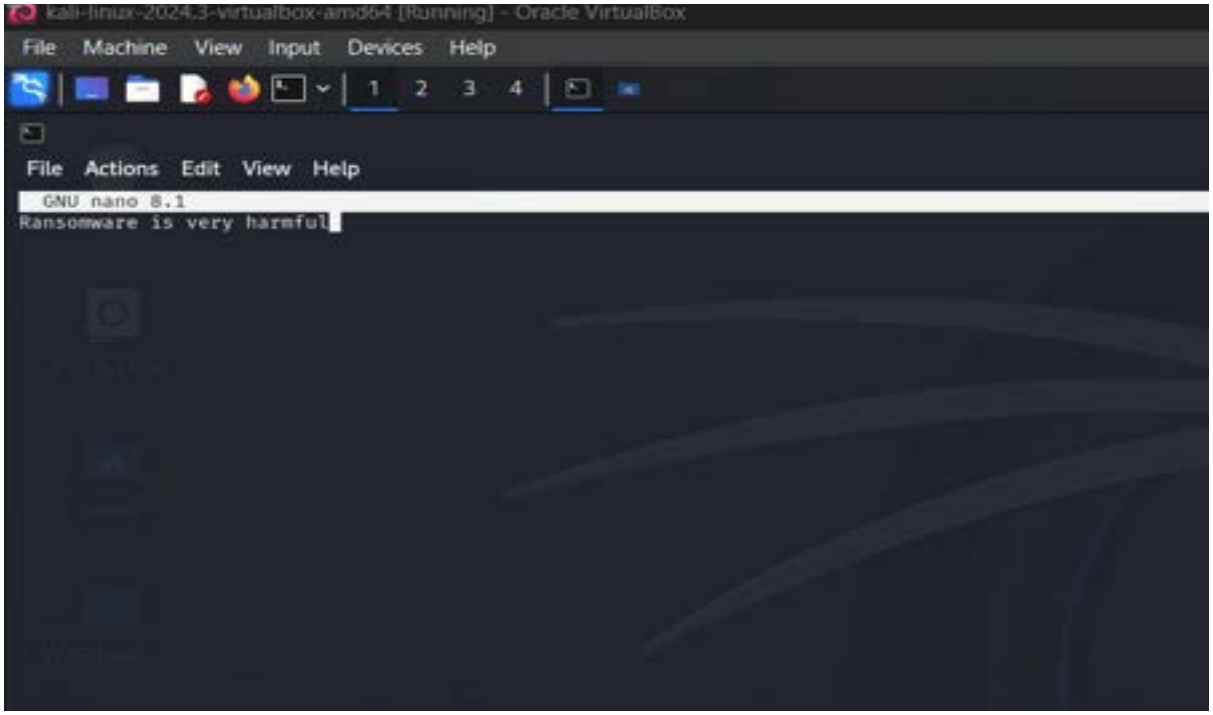
Step 27: After enter the correct password

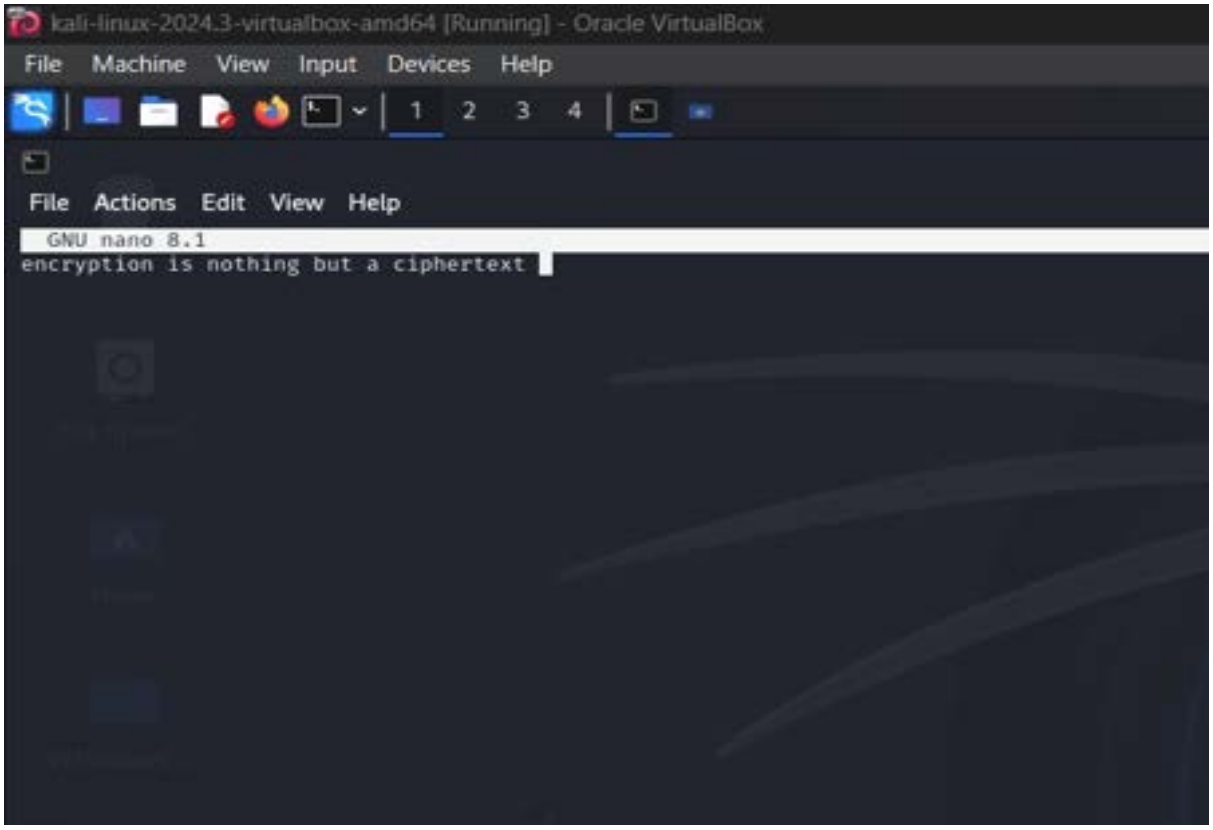


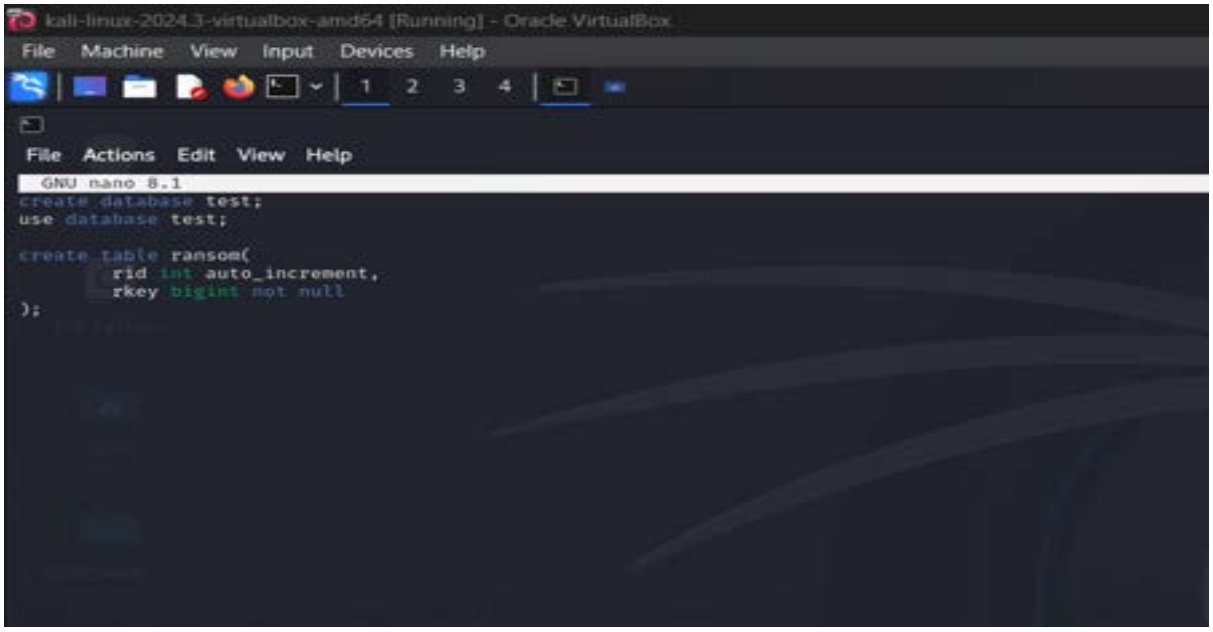
Step 28: Then, we got our files back



Decrypted Files:

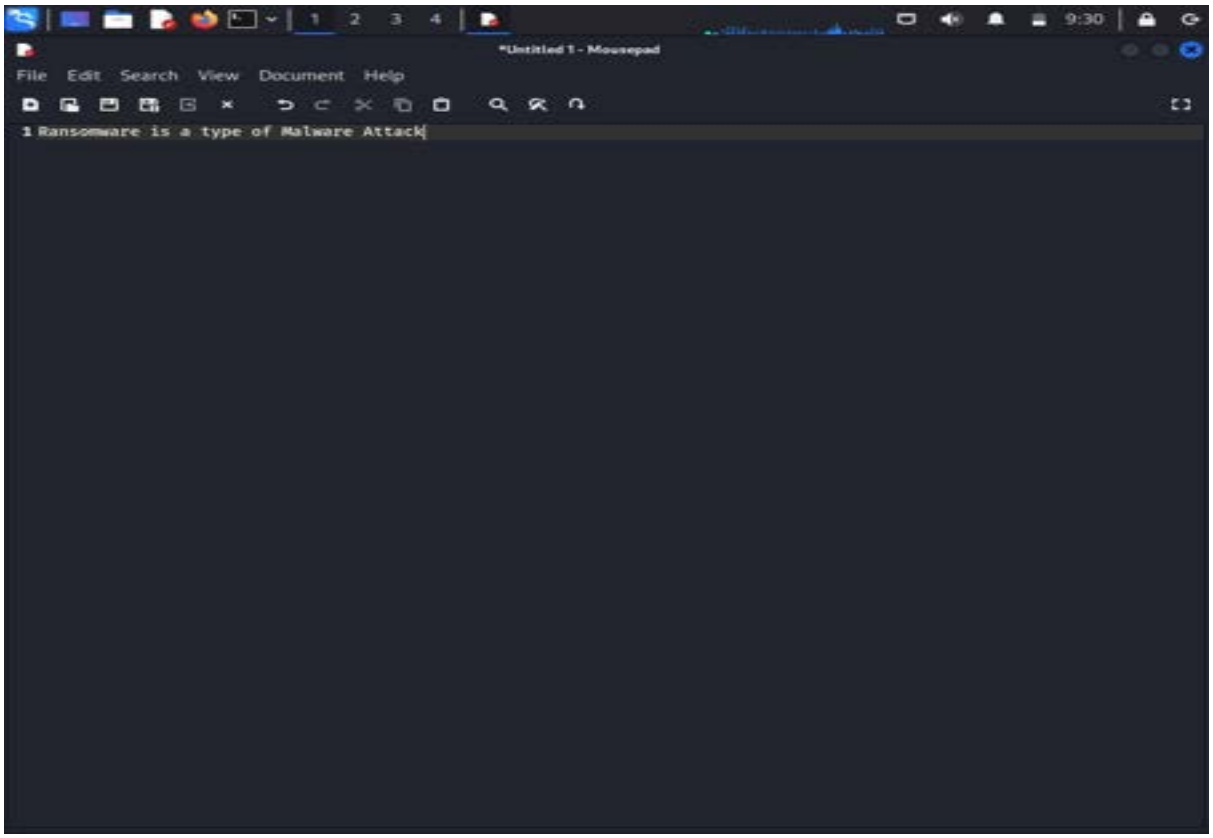

kali-linux-2024.3-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
File Actions Edit View Help
GNU nano 8.1
Ransomware is very harmful


kali-linux-2024.3-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
1 2 3 4
File Actions Edit View Help
GNU nano 8.1
encryption is nothing but a ciphertext

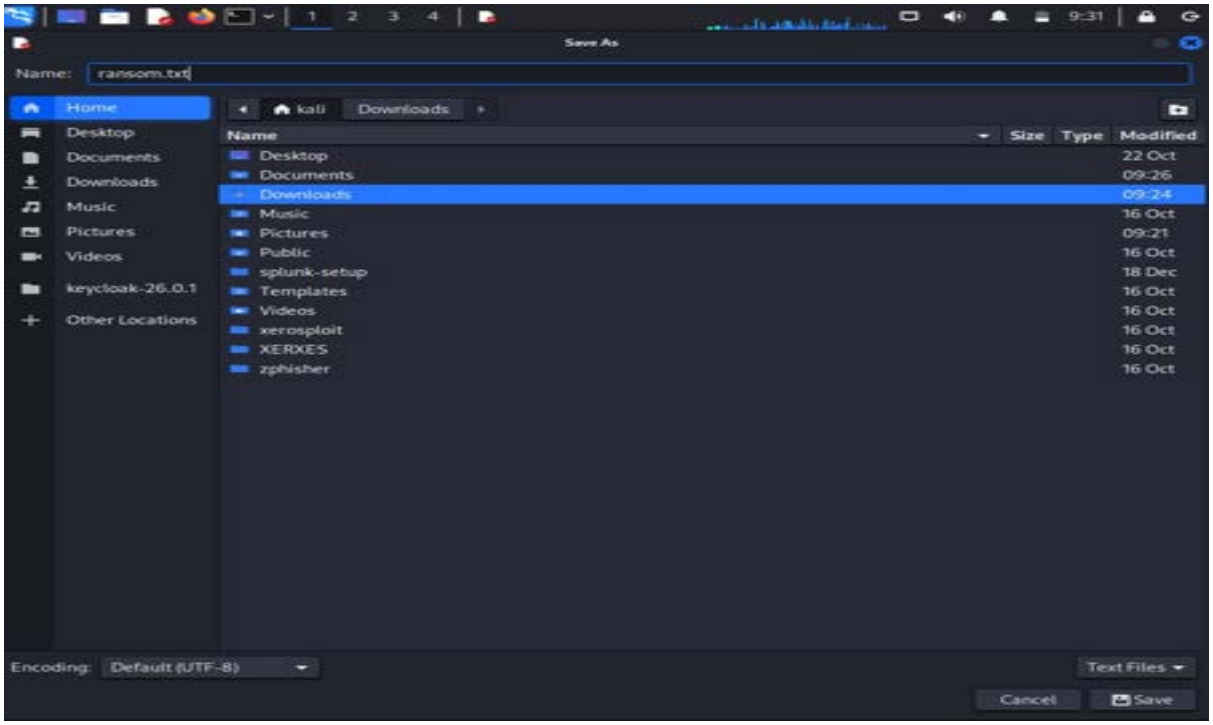


2.

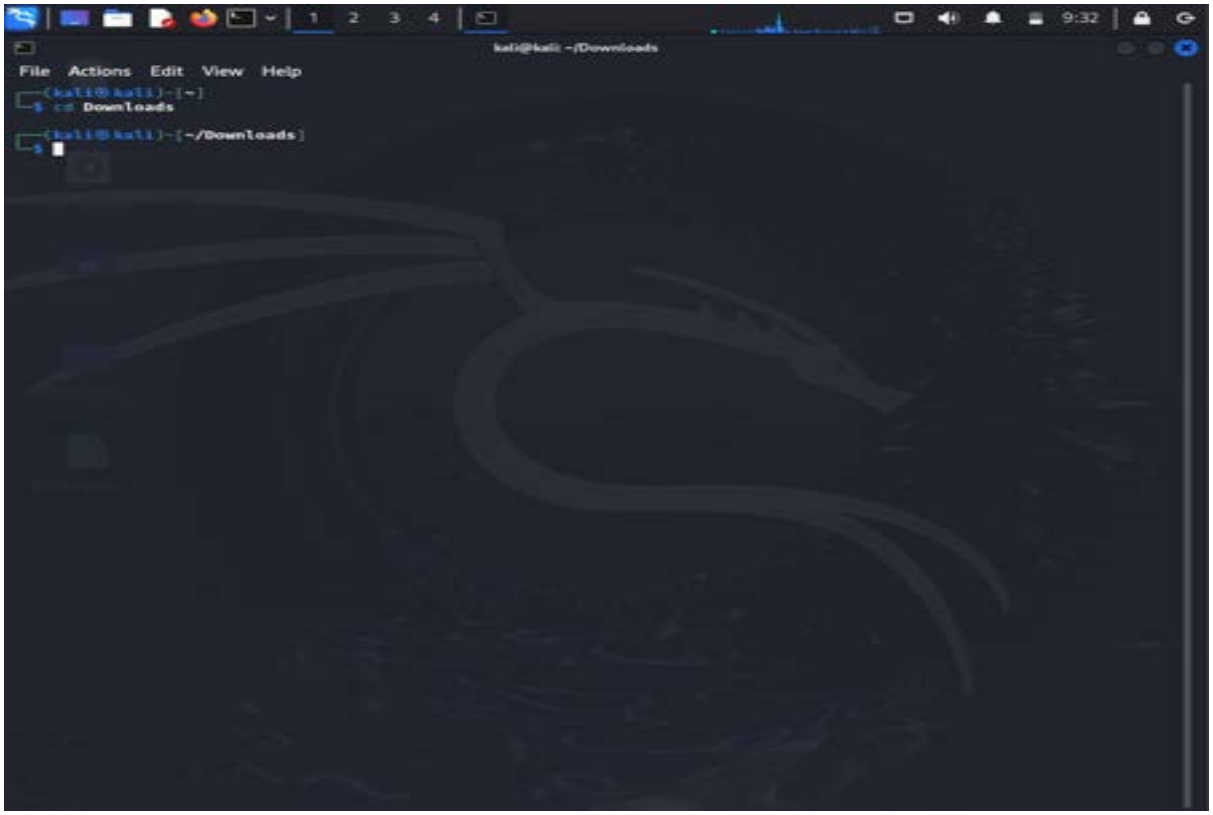
Step1: Enter atext intext editor



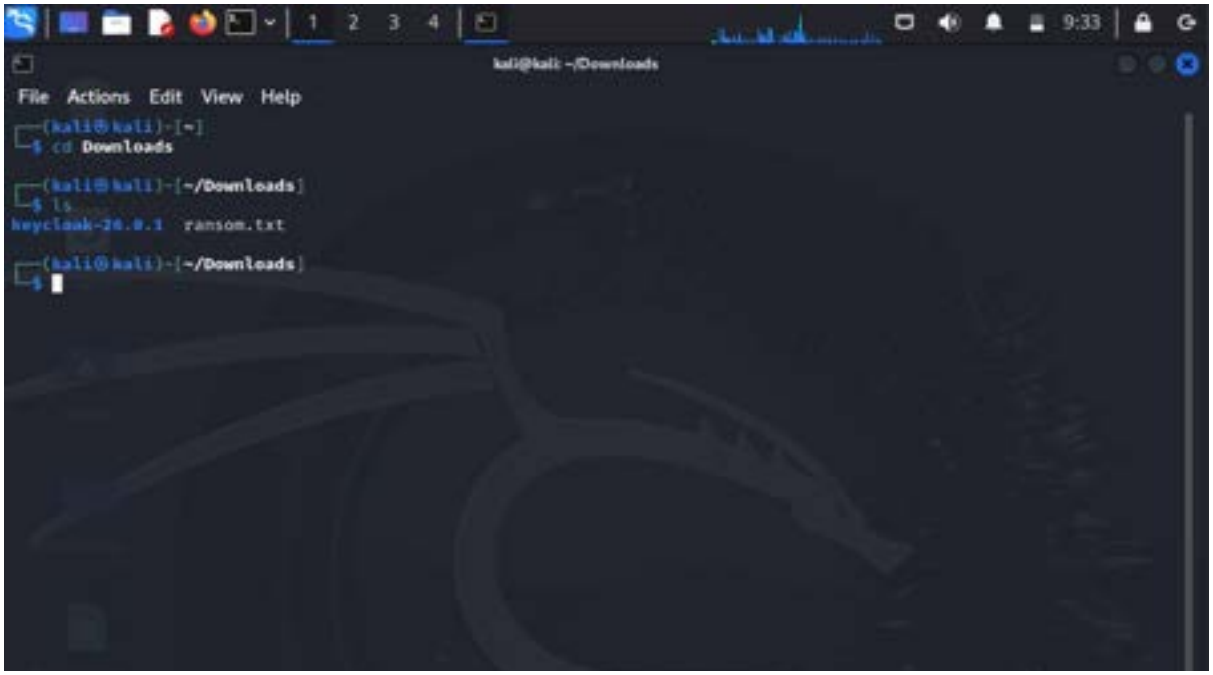
Step 2: Save it as ransom.txt in downloads



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

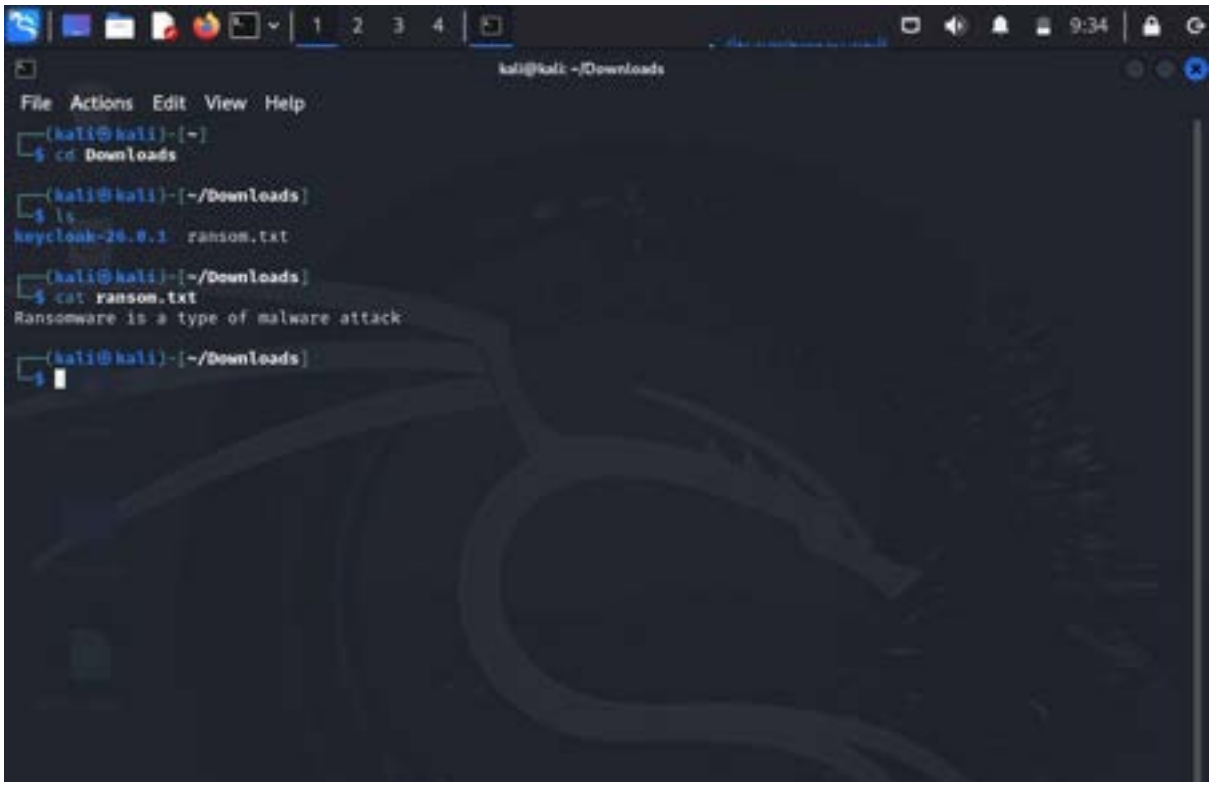


Step 4: Give the command ls



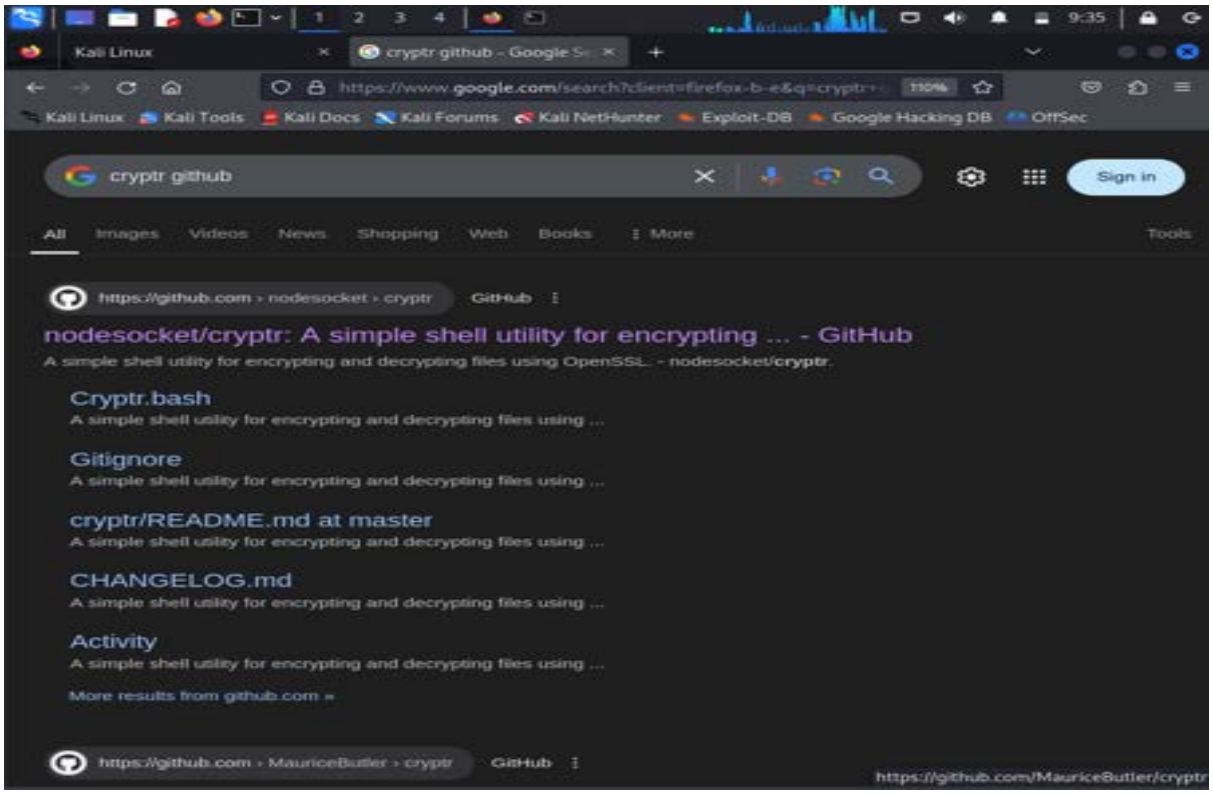
Step 5: Enter “cat ransom.txt”

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

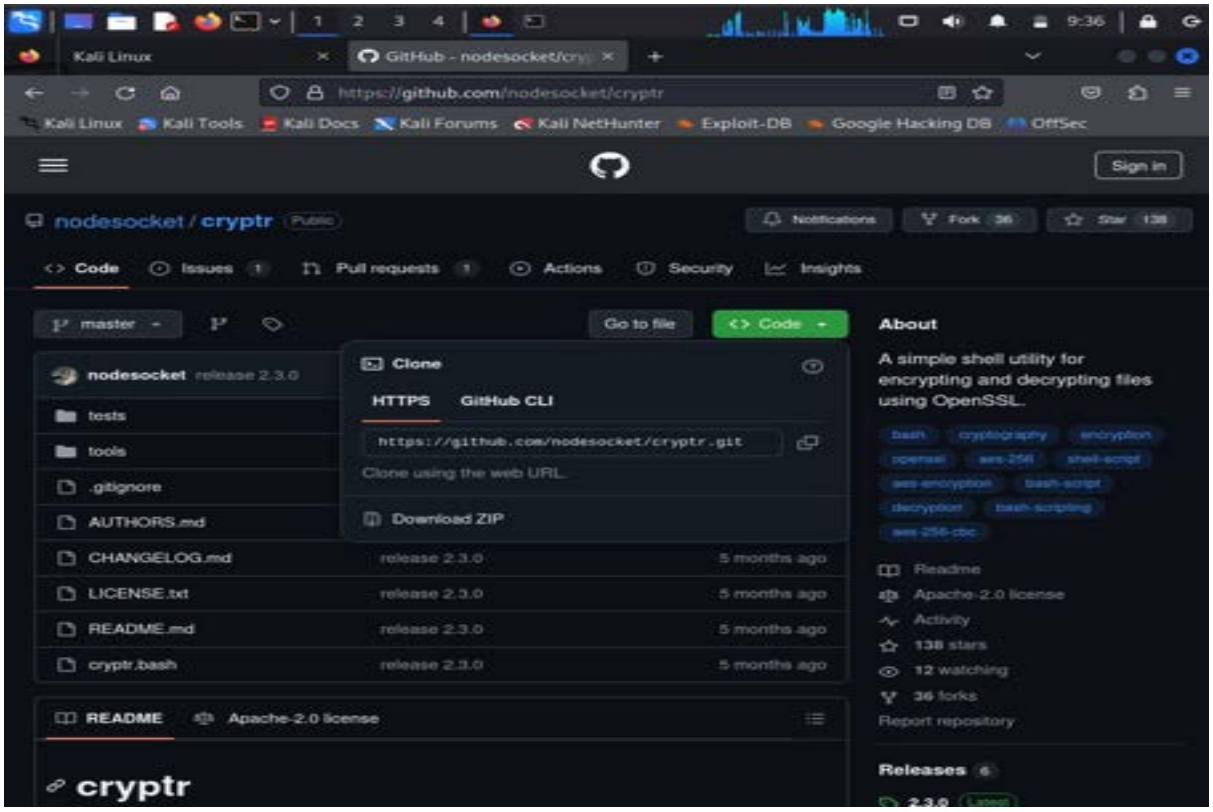


Step 6: open Firefox and search “Cyptr GitHub”

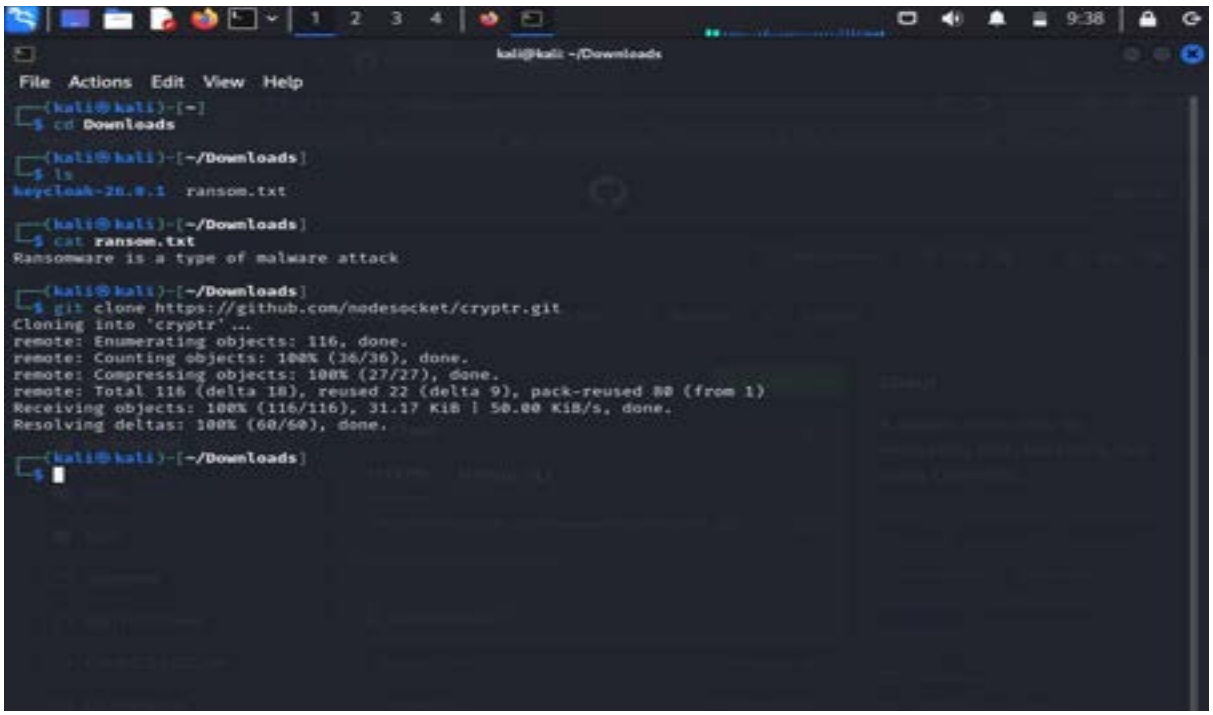
Step 7: Select first link



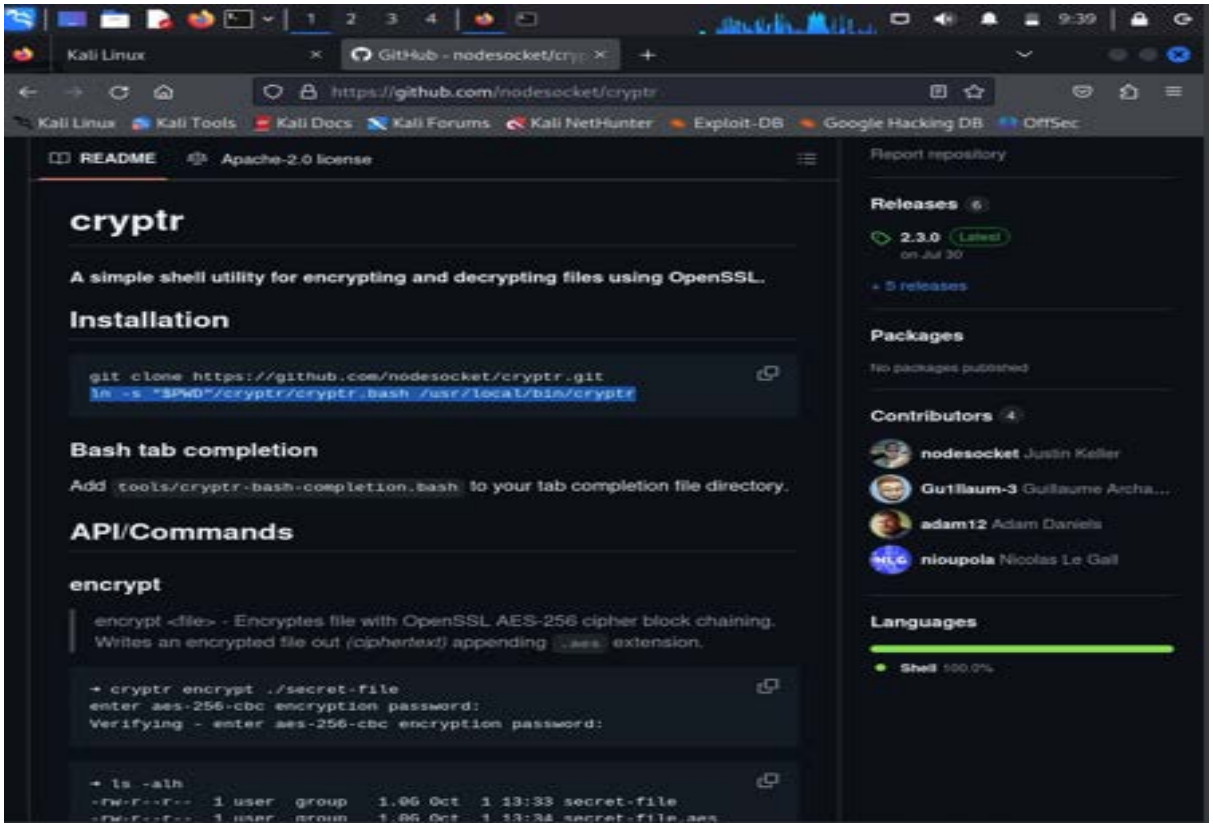
Step 8: Copy the HTTPS link in code



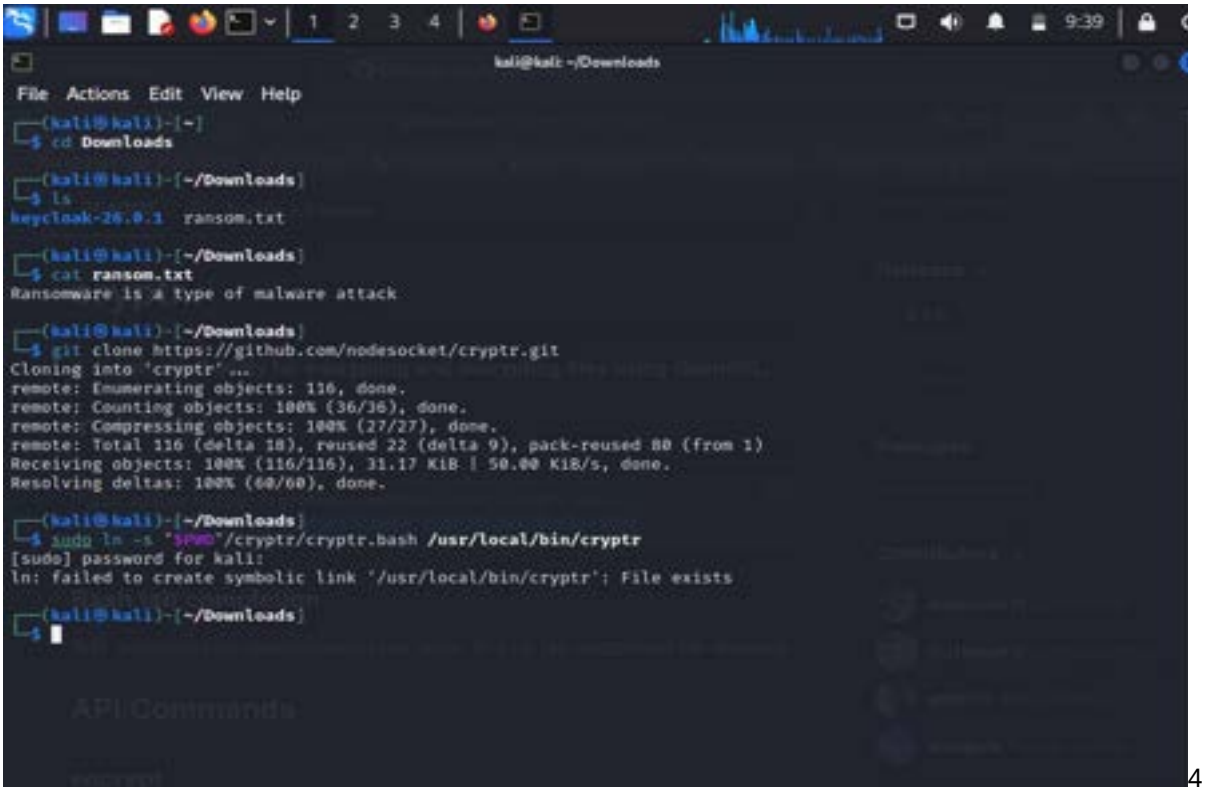
Step 9: Then go back to the terminal and type git clone and paste the HTTPS link



Step 10: copy the second link in installation at GitHub



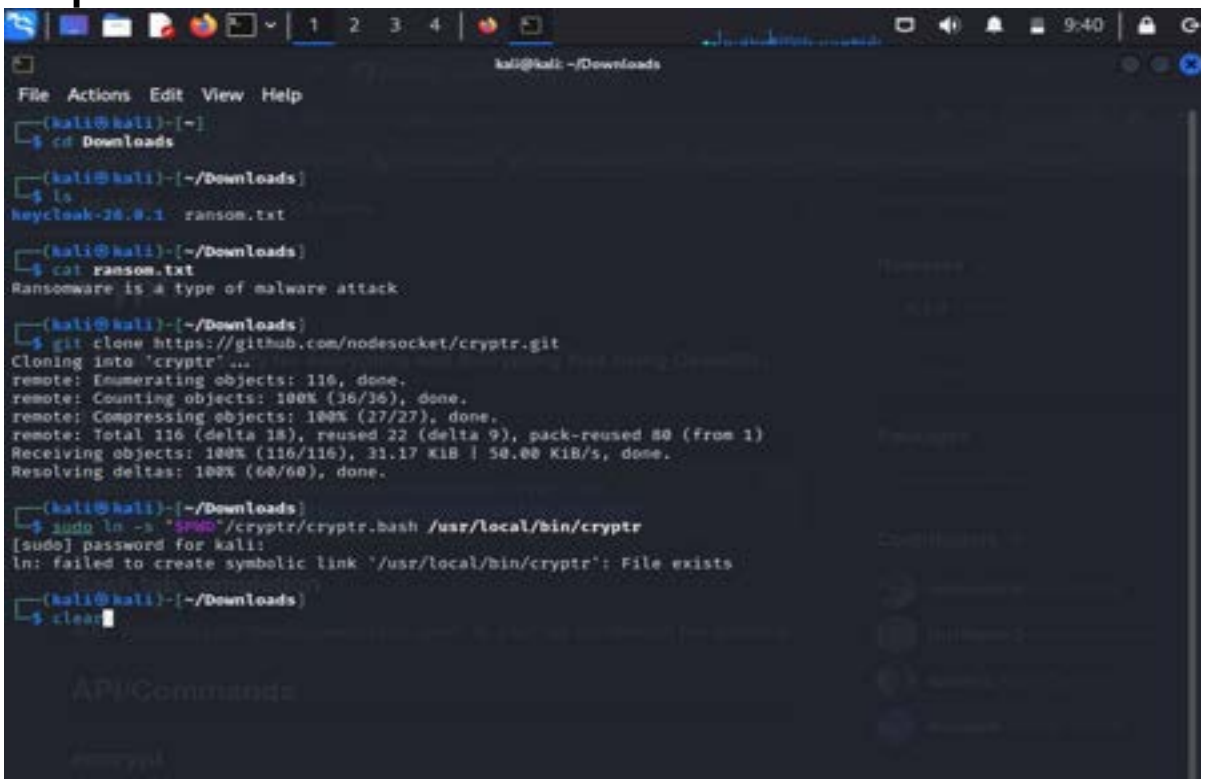
Step 11: Type sudo and paste the link



4

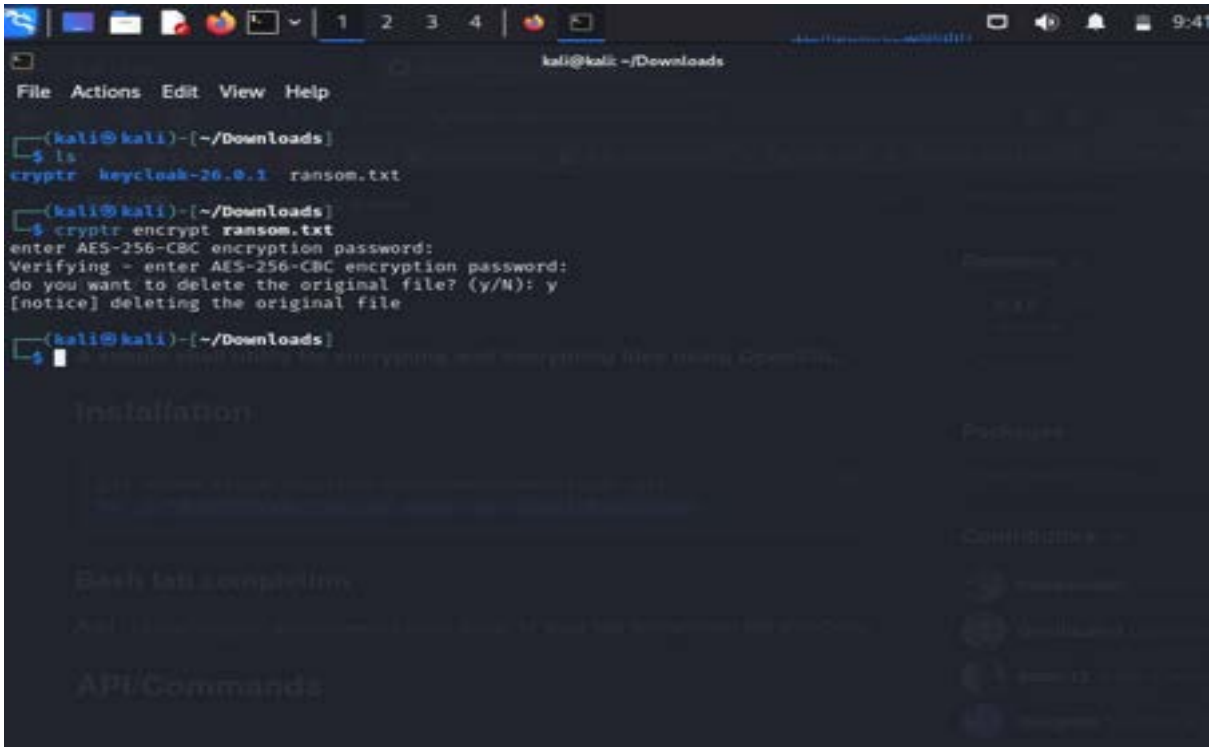
1

Step 12: clear

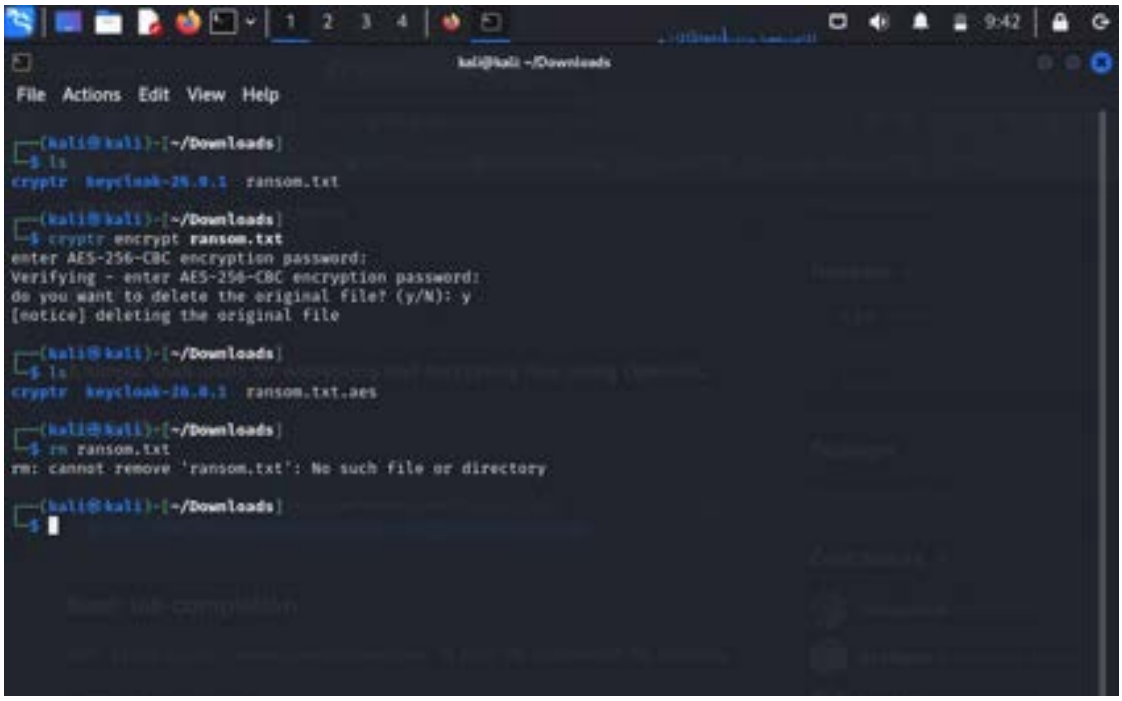


Step 13: To encrypt the text

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

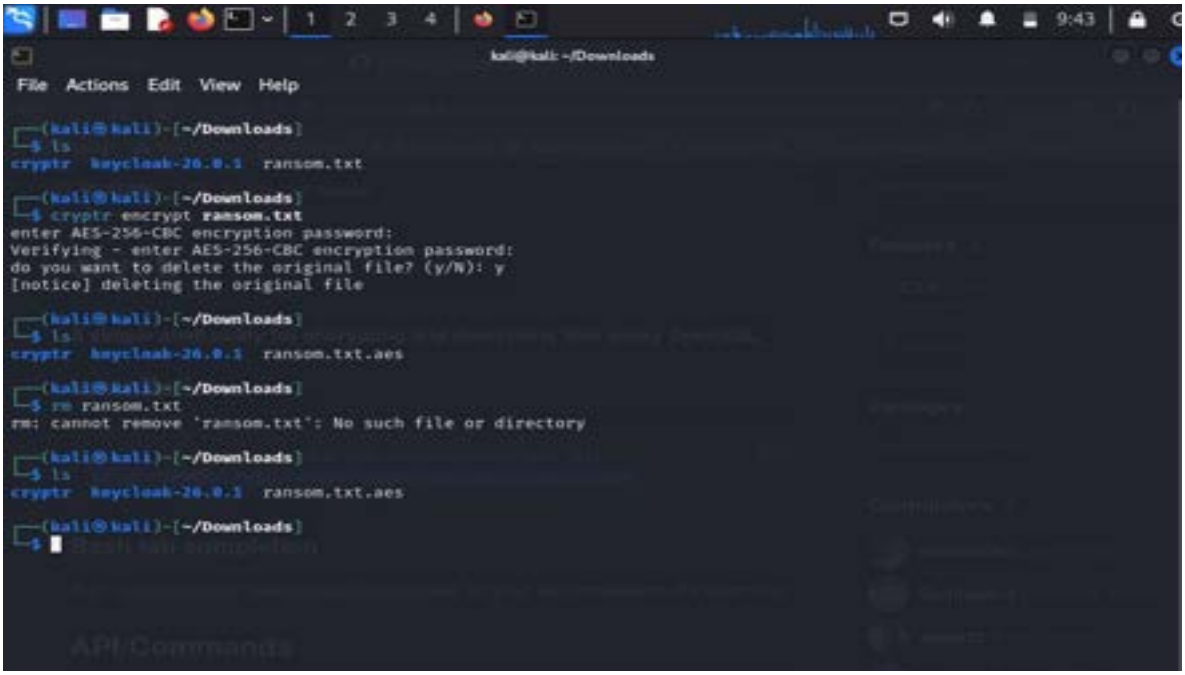


Step 14: Give ls and click enter then, “rm ransom.txt”

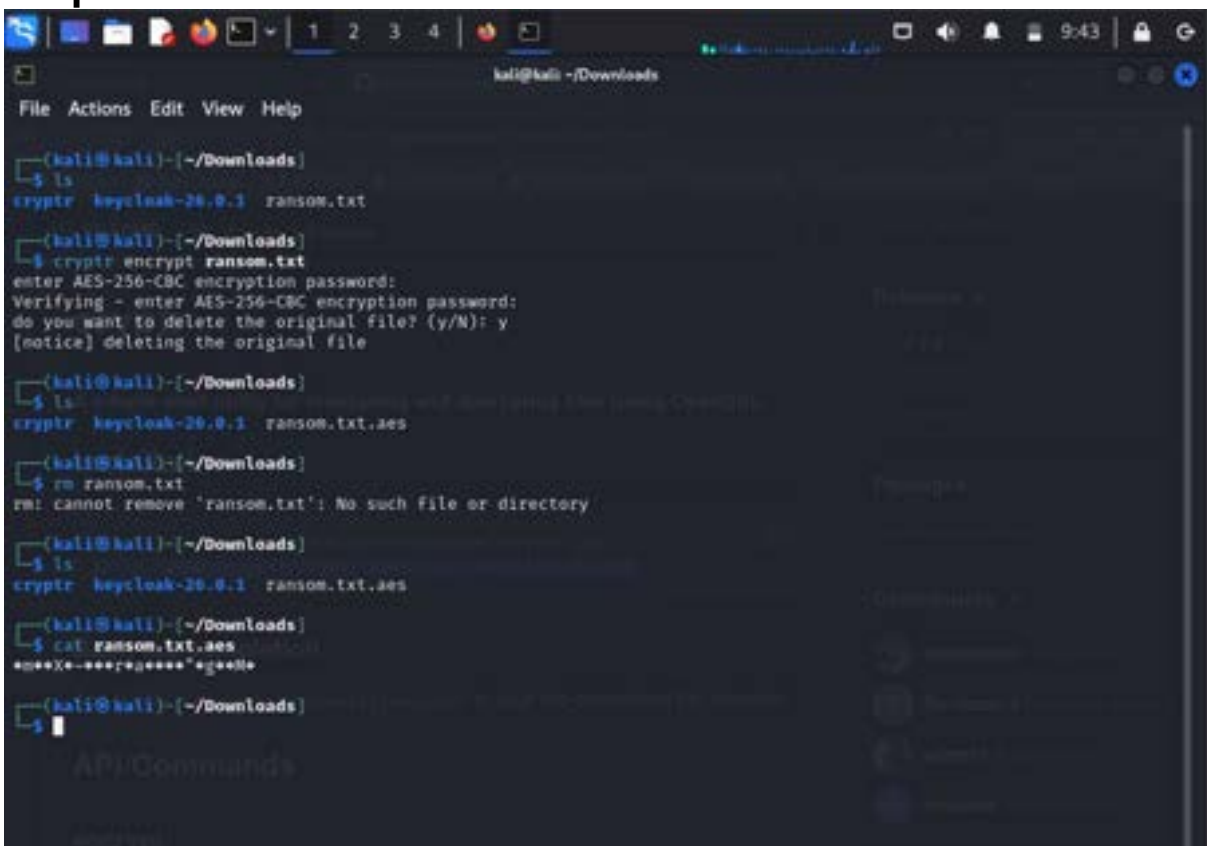


Step 15: Type ls

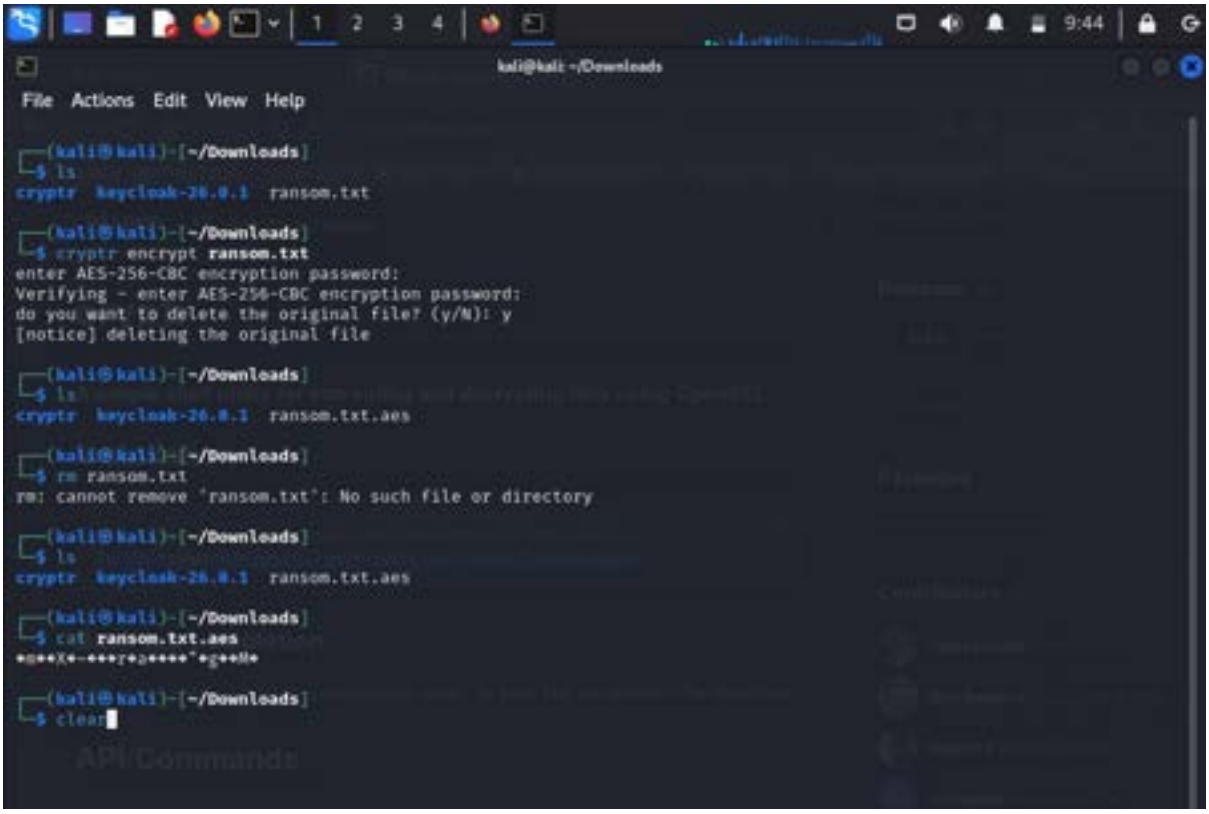
we can see the saved file here



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

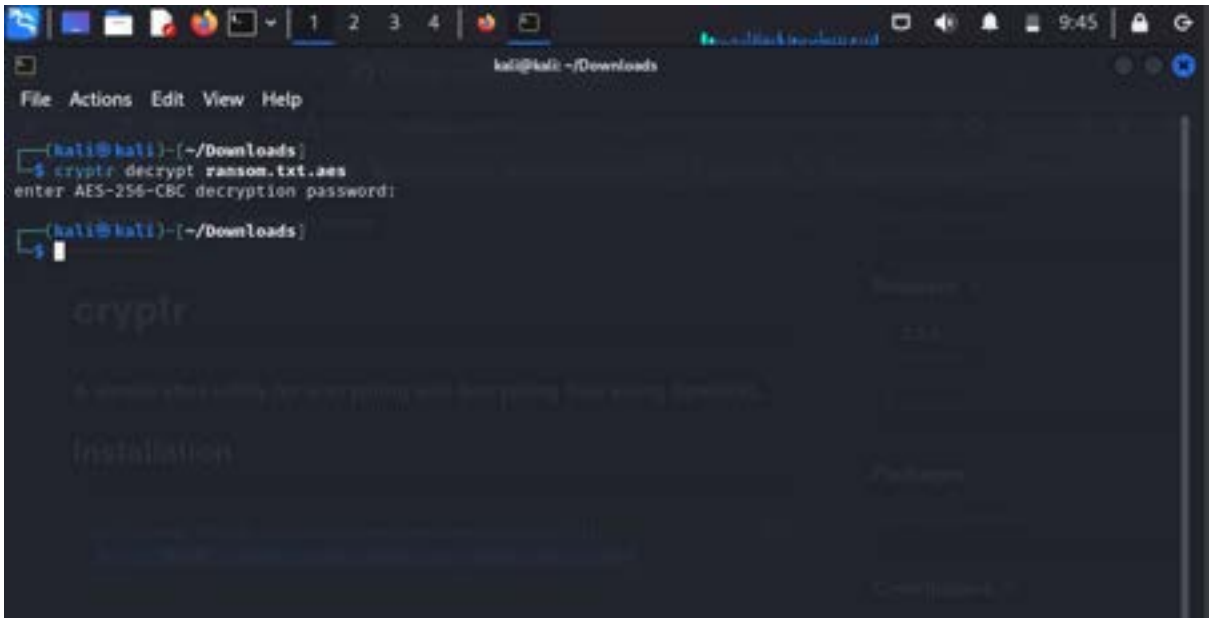


Step 17: clear



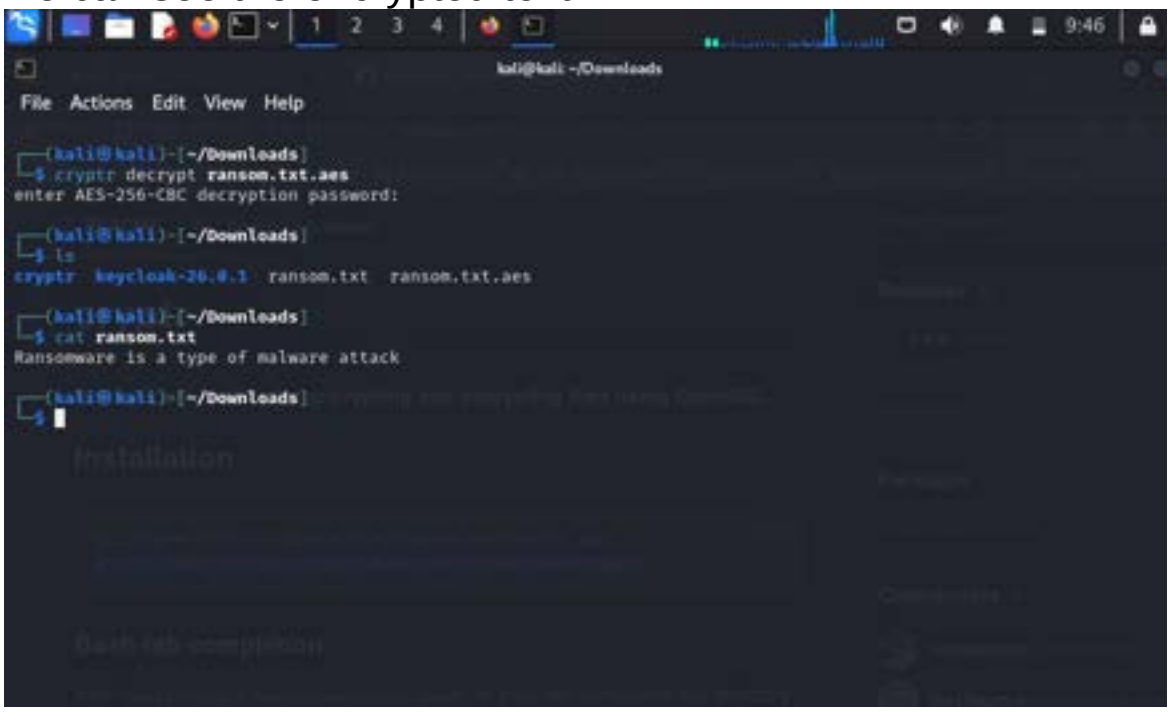
Step 18: To decrypt the text

Give the command “crypt decrypt ransom.txt.aes”



Step 19: By giving “cat ransom.txt”

we can see the encrypted text

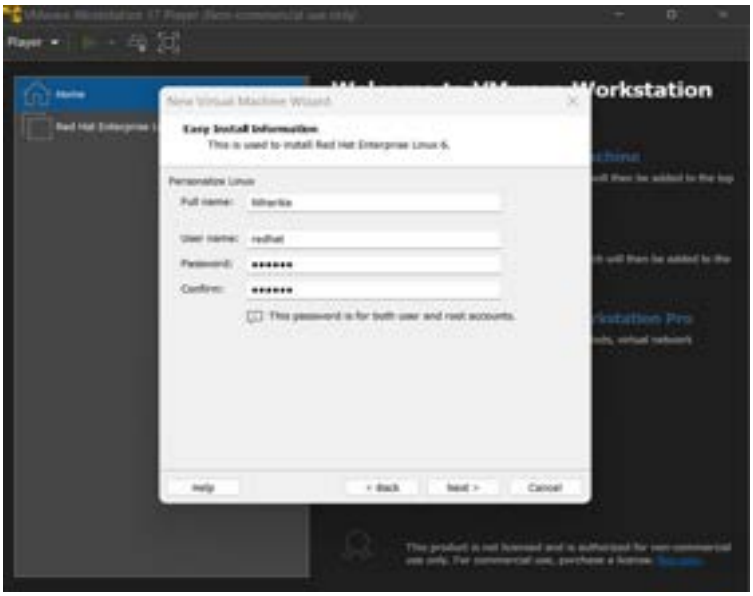


Linux ISO Image using VMWARE

Step 1: To install RedhatinVMware,give

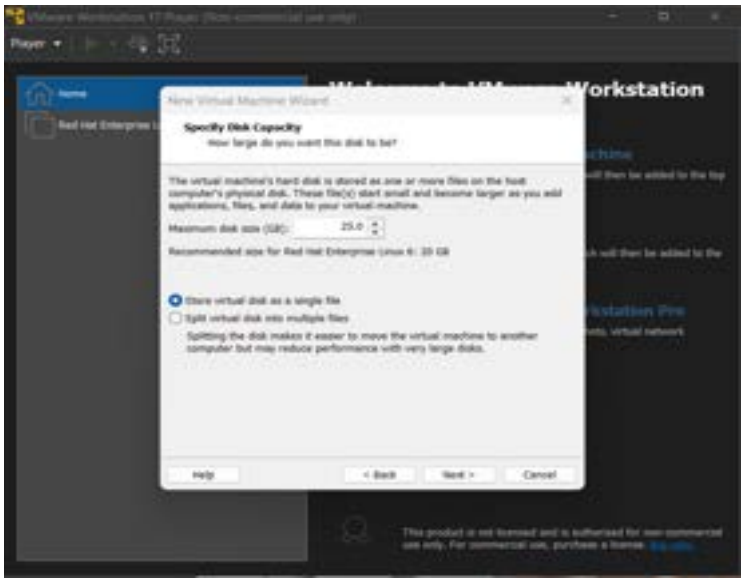
Username: redhat

Password :redhat



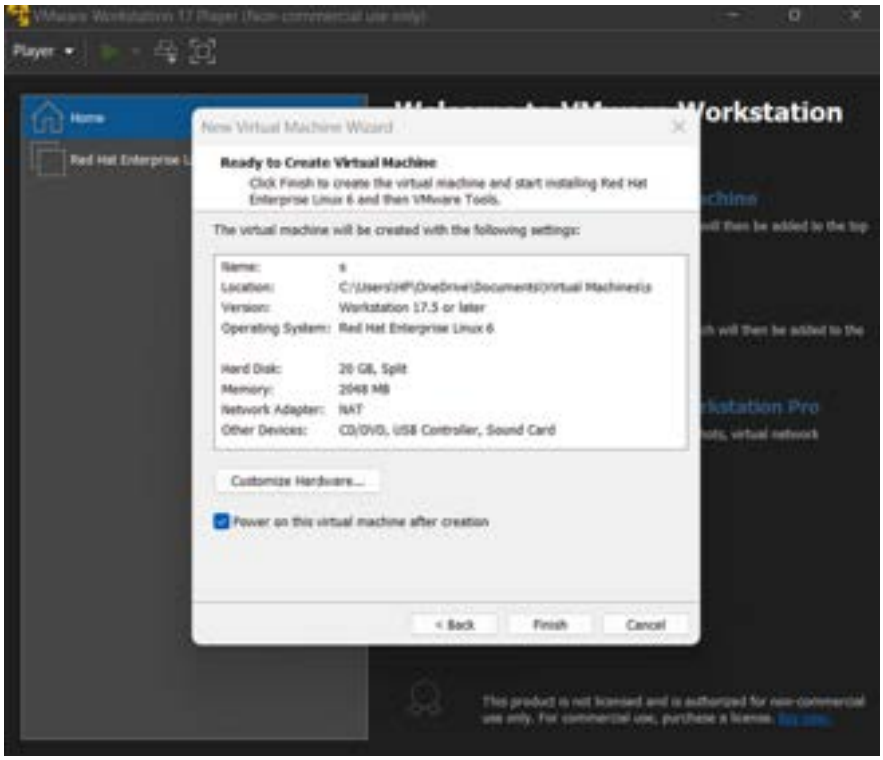
Step 2: Here we have to set the disk size upto:25.0

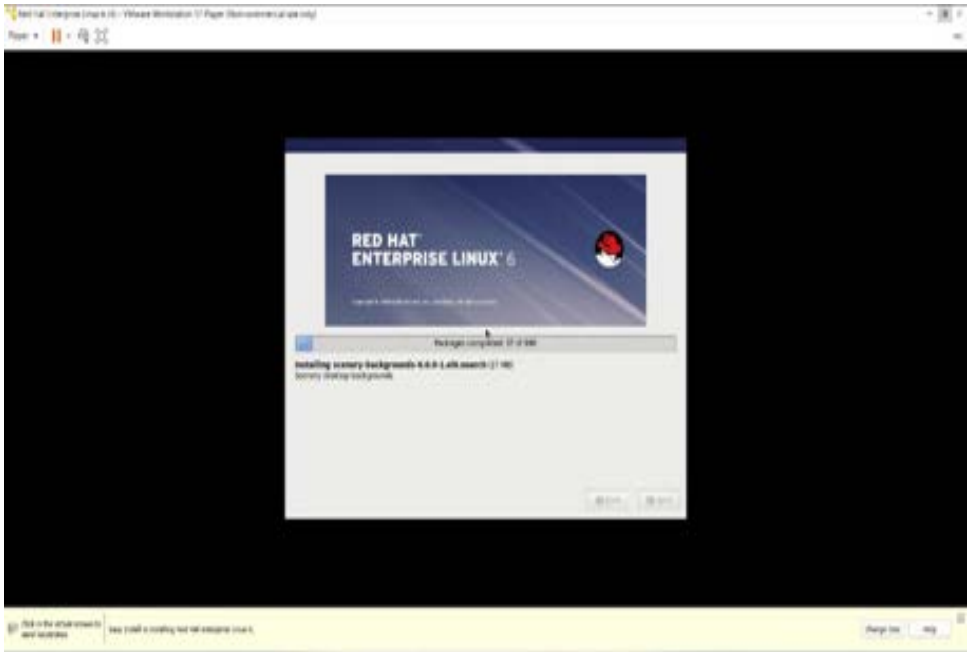
And select store virtual disk as a single file.



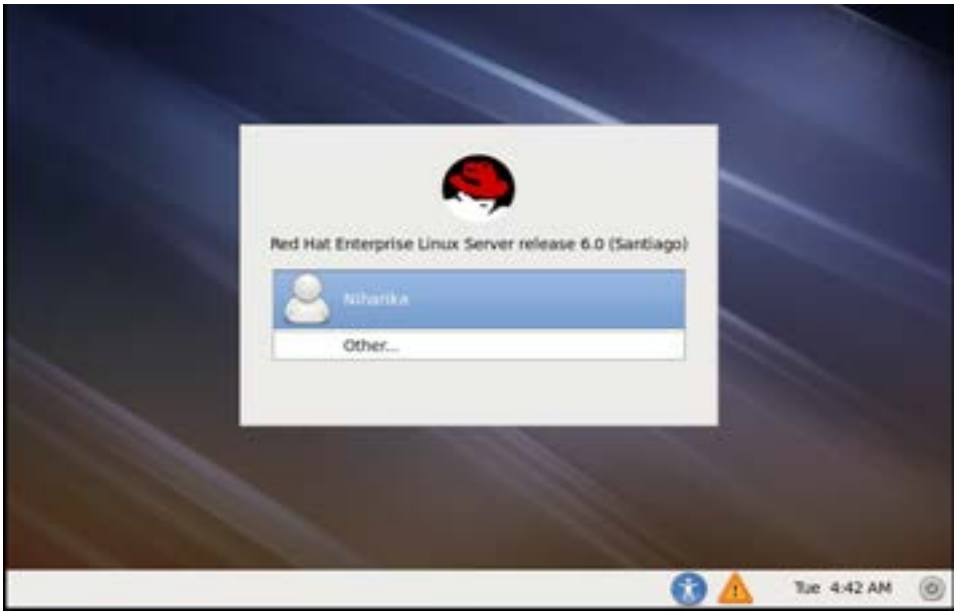
46

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



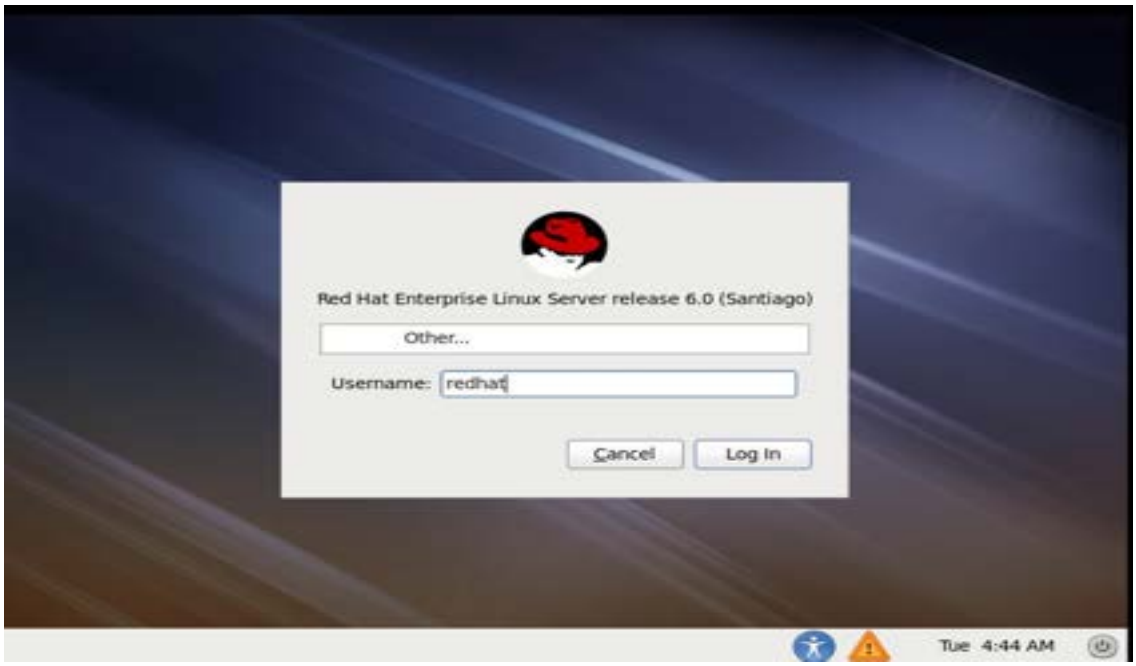


Step 4: Here the user which we created in the VMware is available here.

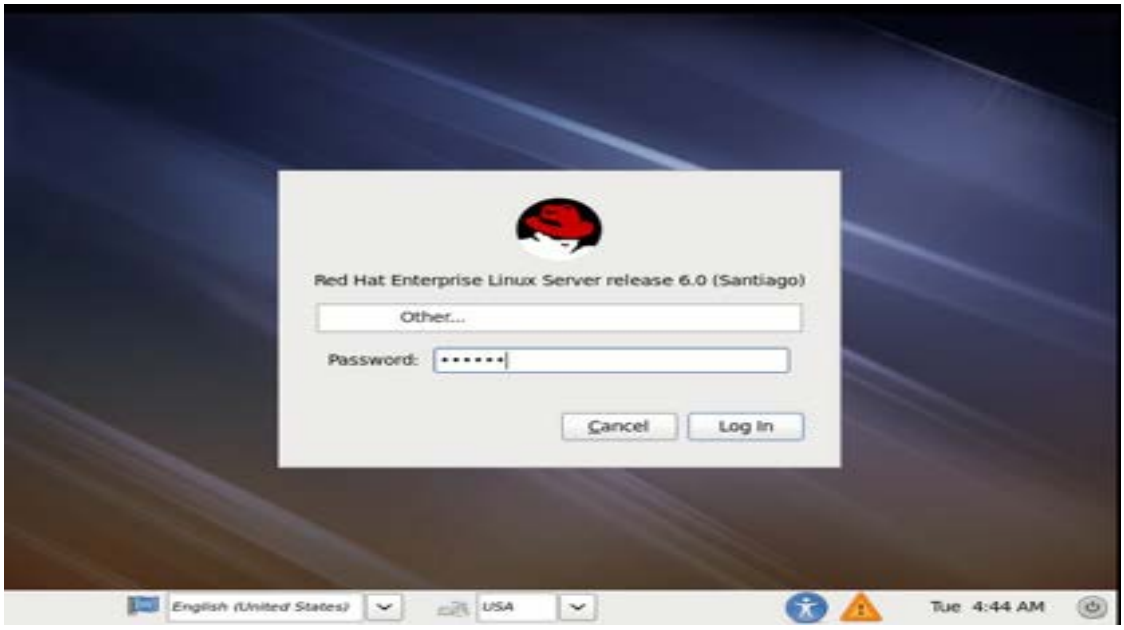


Step 5: we have to click other then, give the

Username: redhat



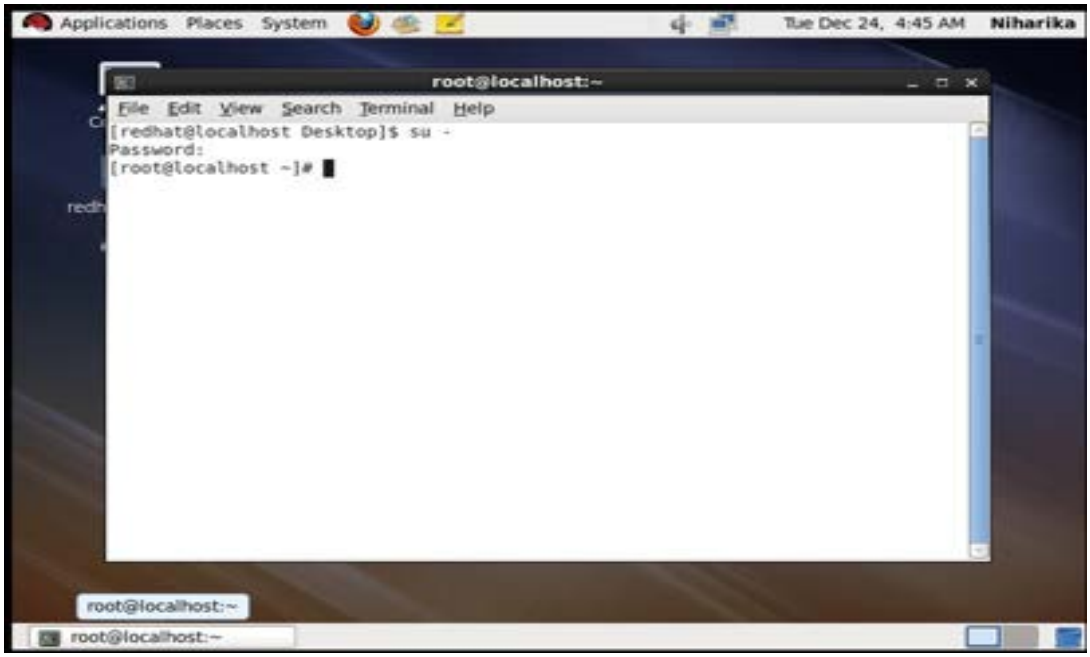
Password:redhat



Open the terminal and give the commands

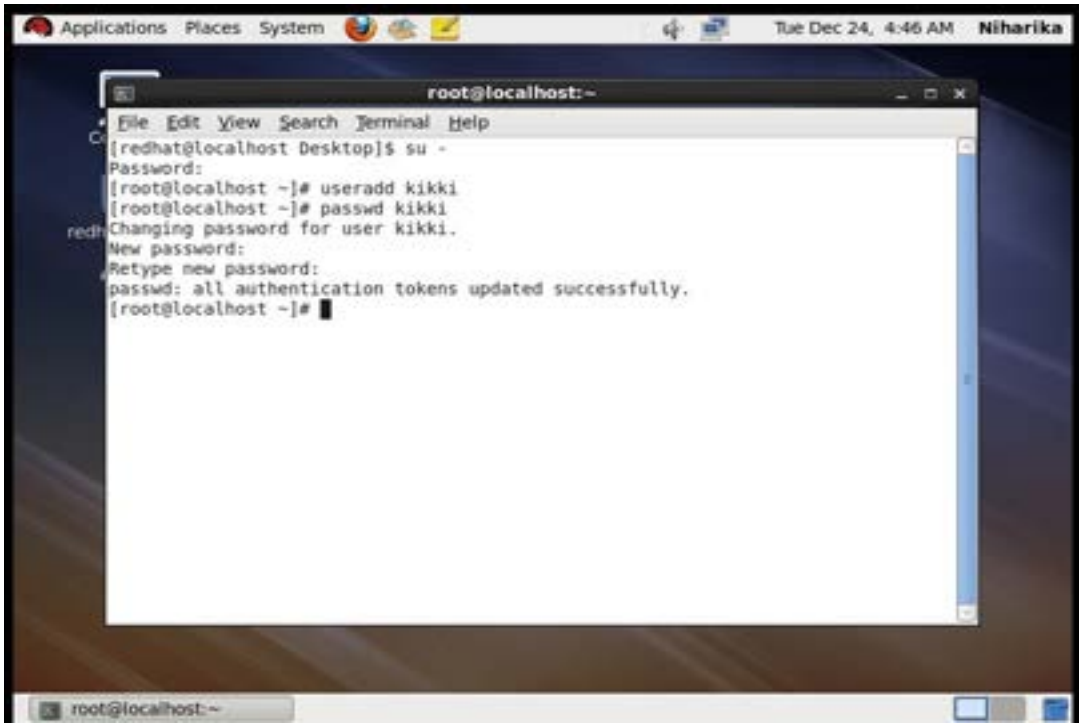
Command 1: su –

Enter the password

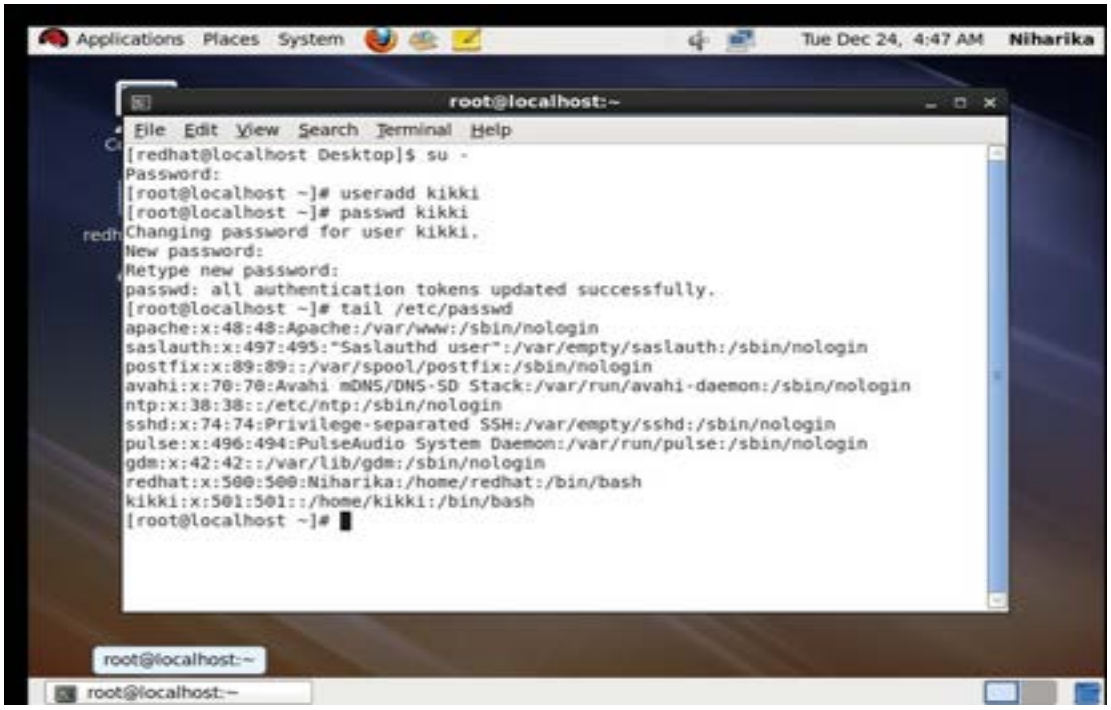


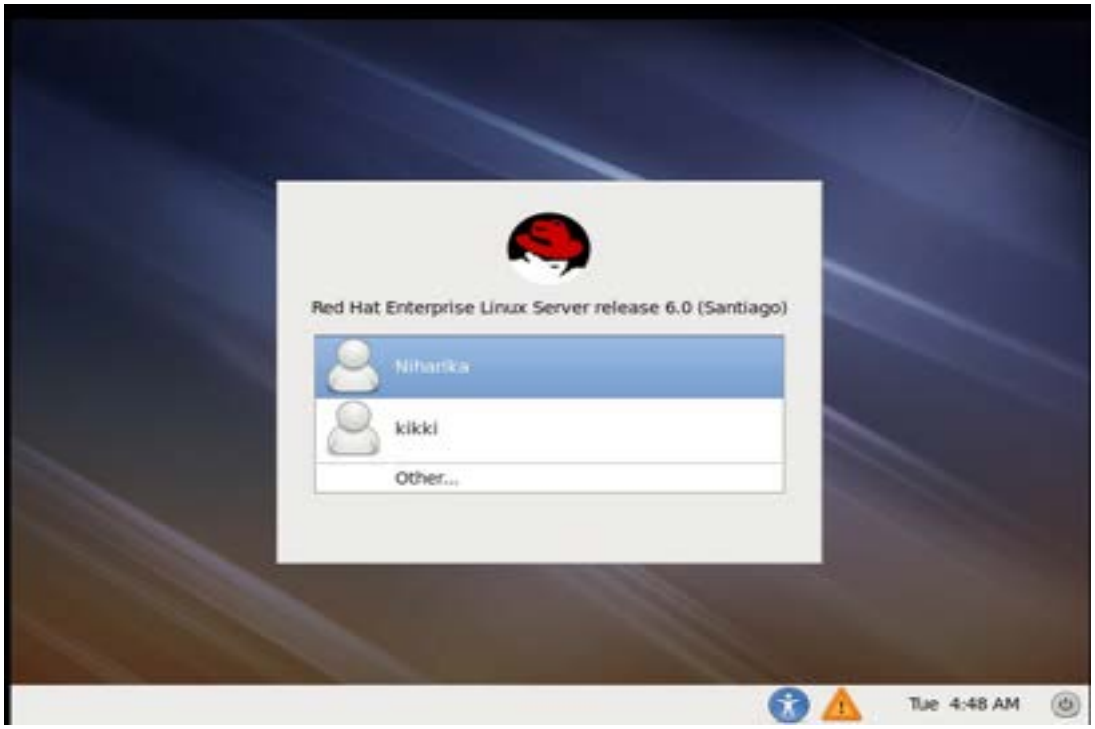
Command 2:Useradd kikki

Command 3:Passwd kikki



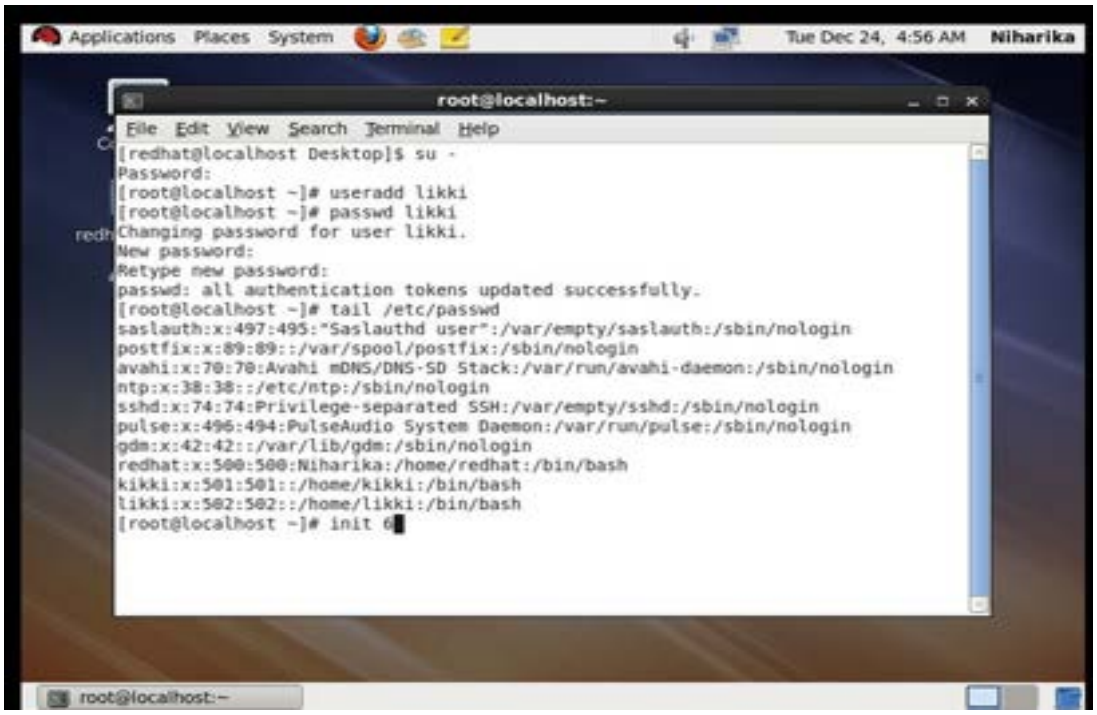
command 4: tail /etc/passwd

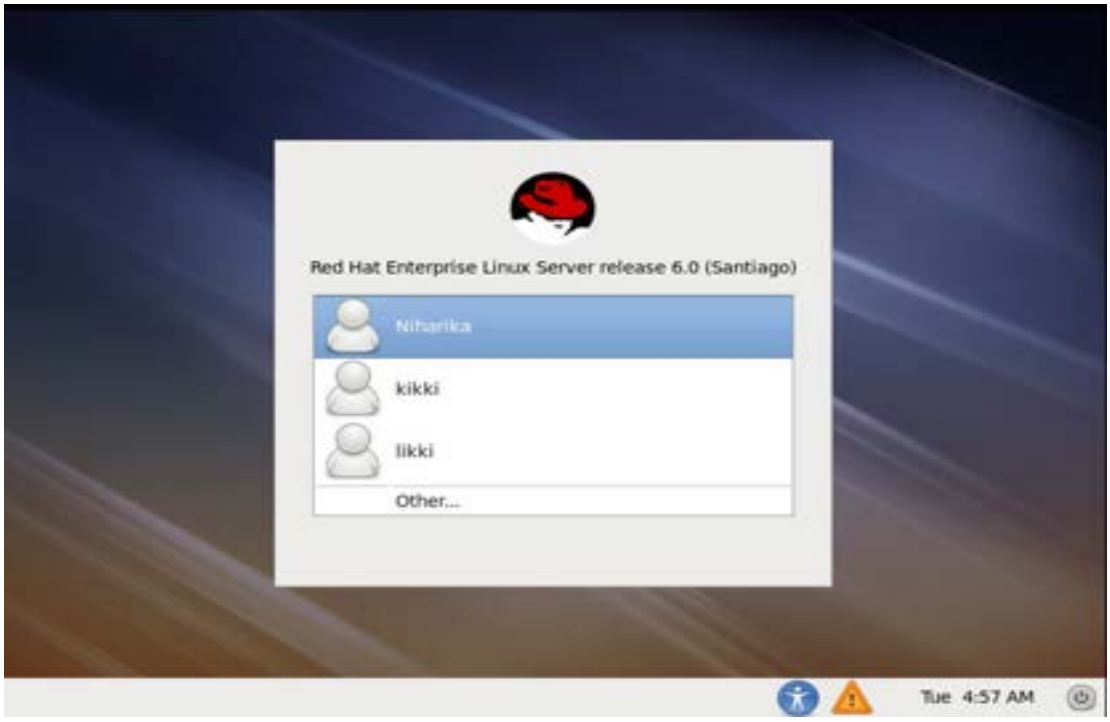




Now, the user is created.

Step 5: Similarly we create another user





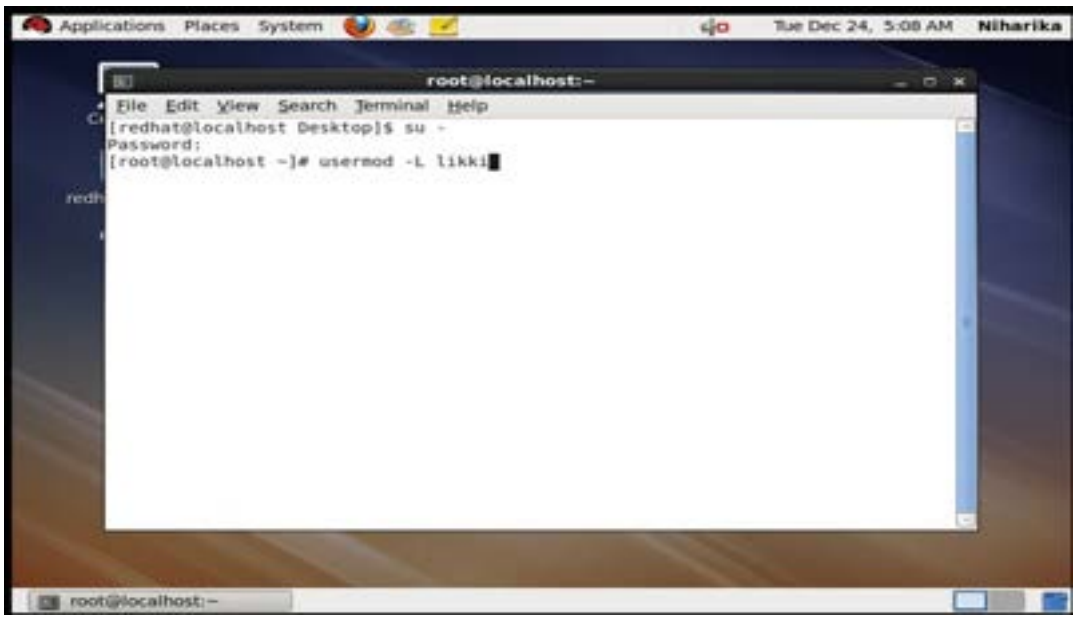
Another user is created as likki

Step 6: To lock the user by using the commands

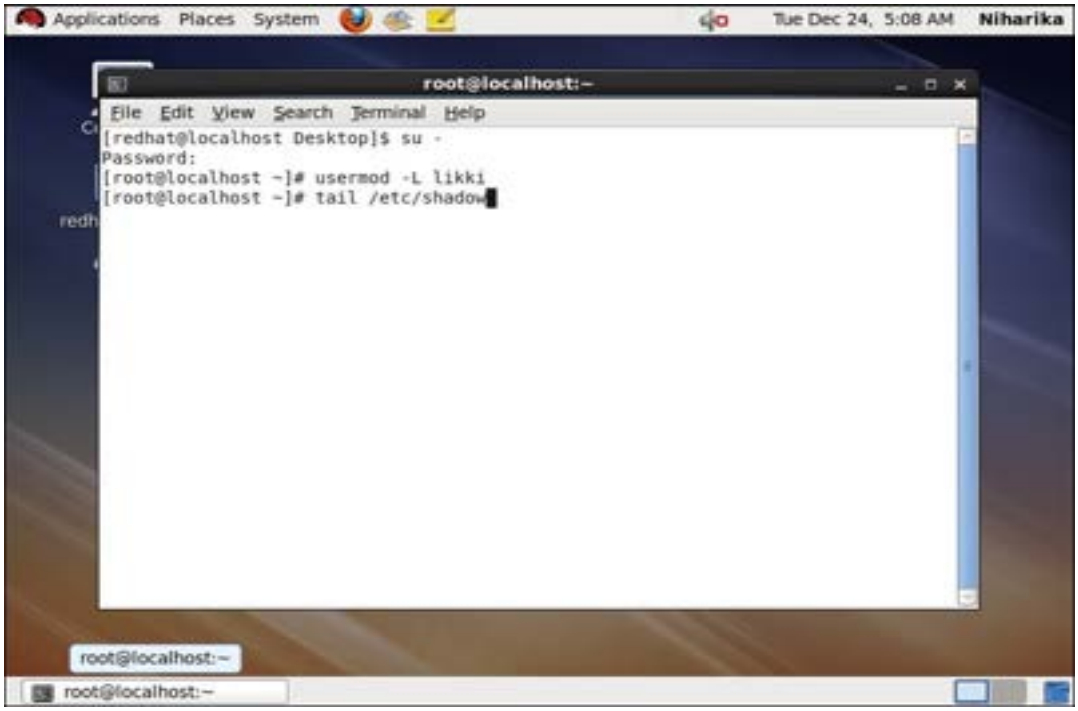
Command 1: su-

Enter the password

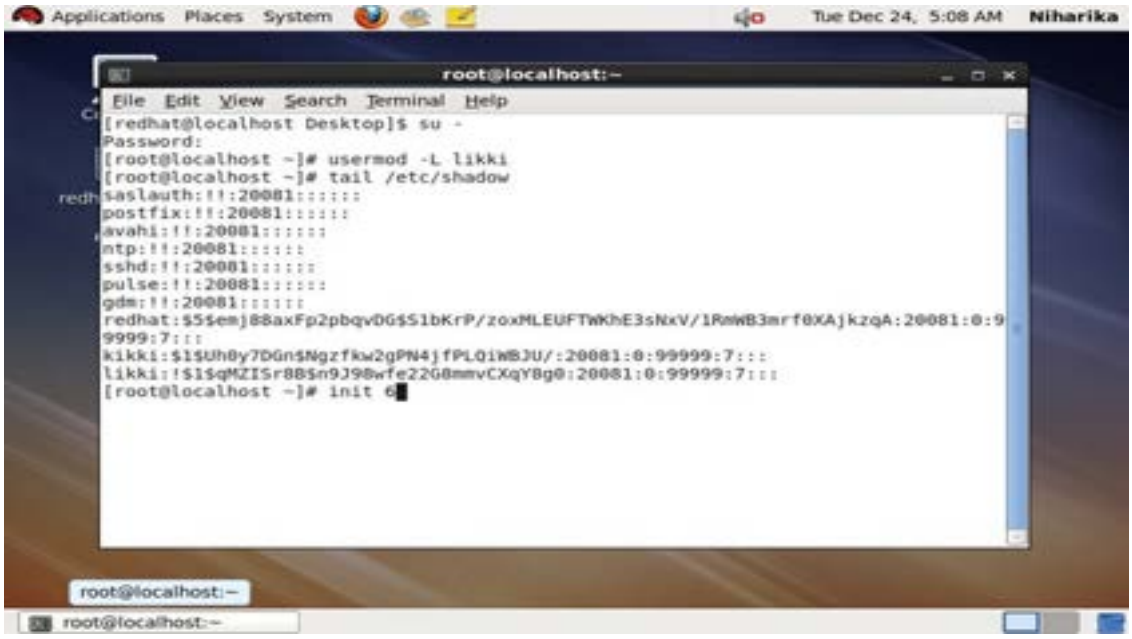
Command 2: usermod –L likki



Command 3: tail /etc/shadow



Command 4: init 6



We locked the user

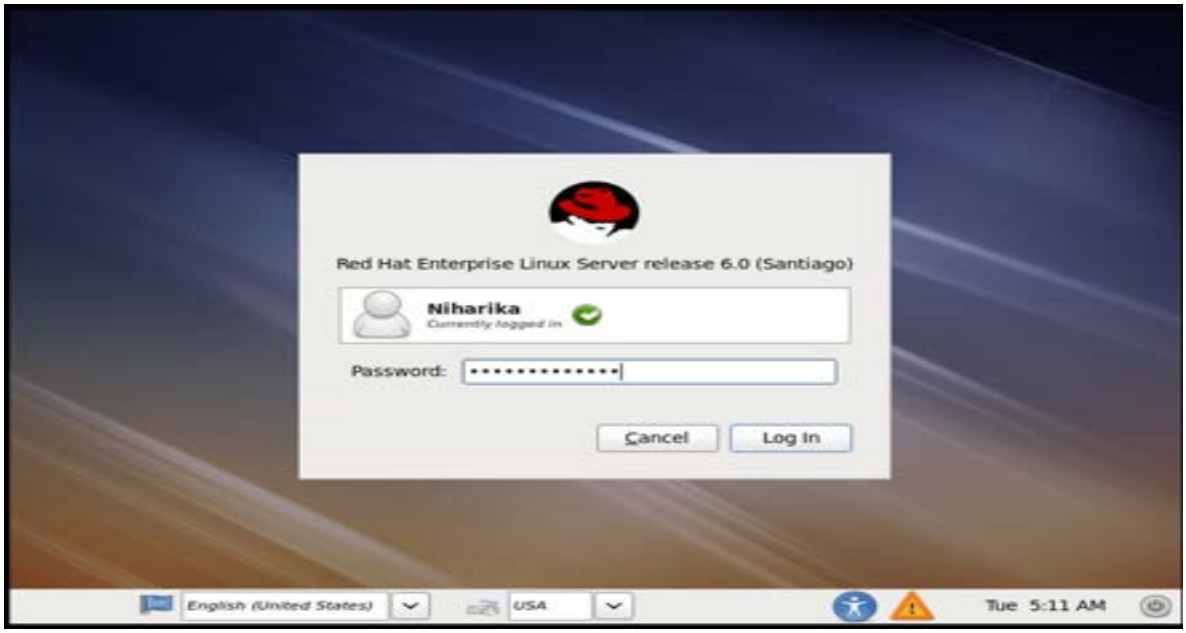
Step 7: Let us see whether the user is opening or not

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 ……

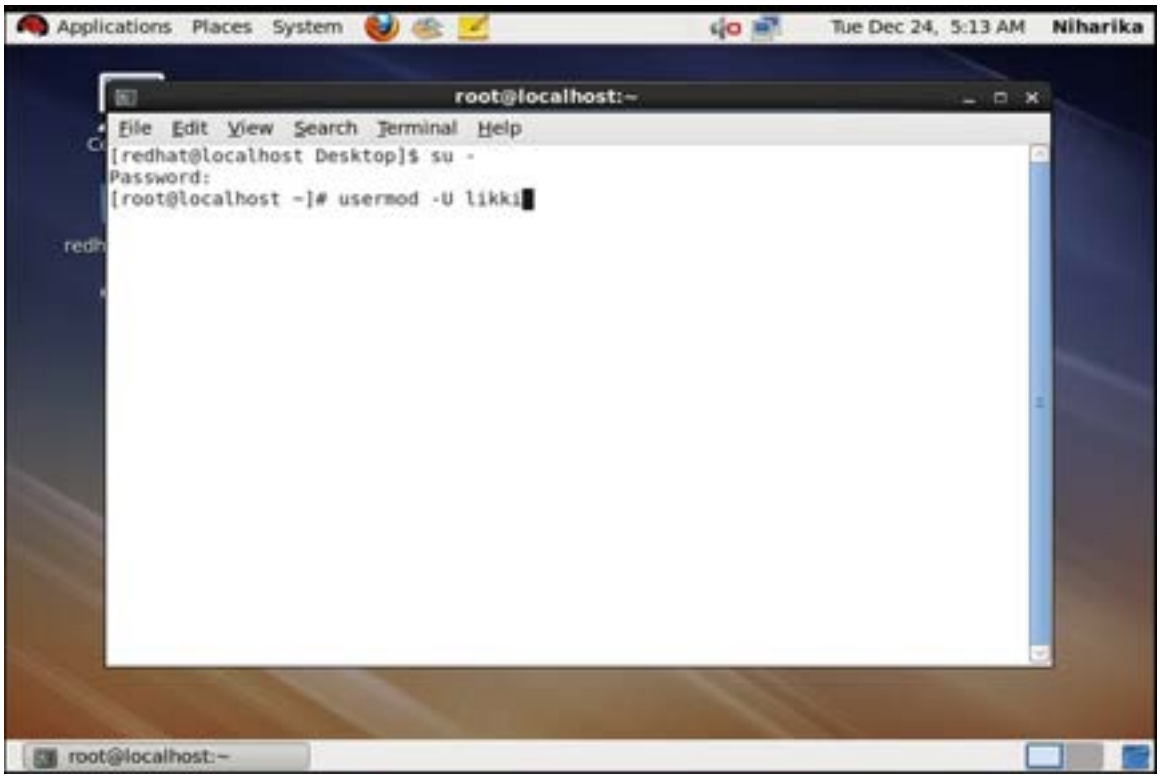


Now give the commands as

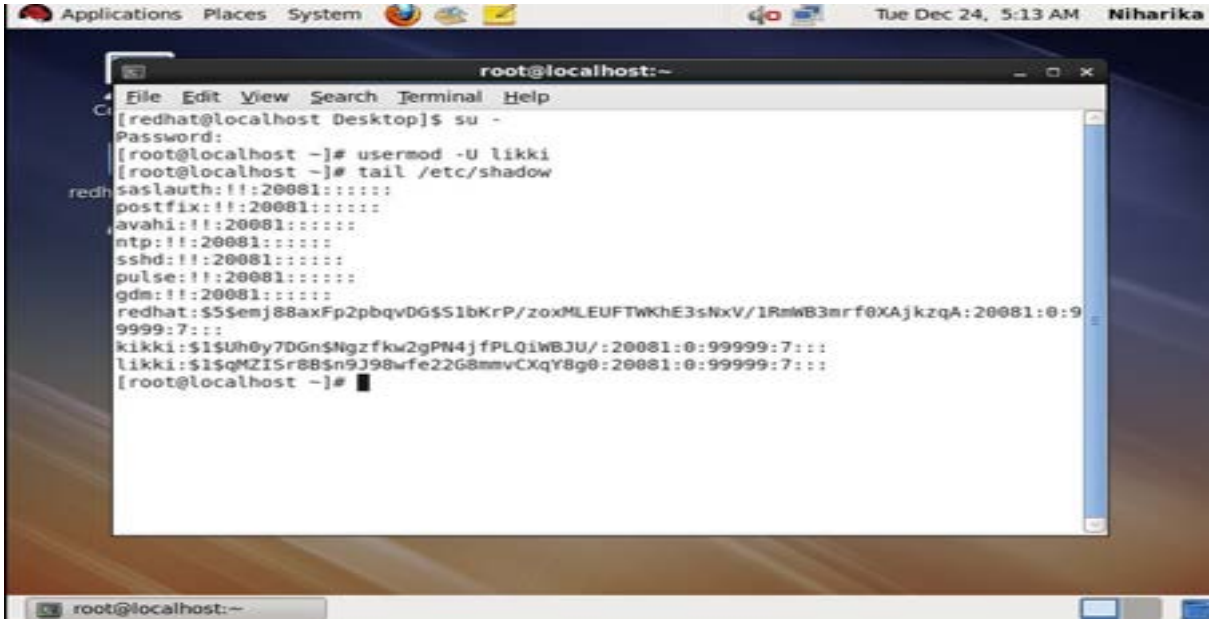
Command 1: su –

Enter the password

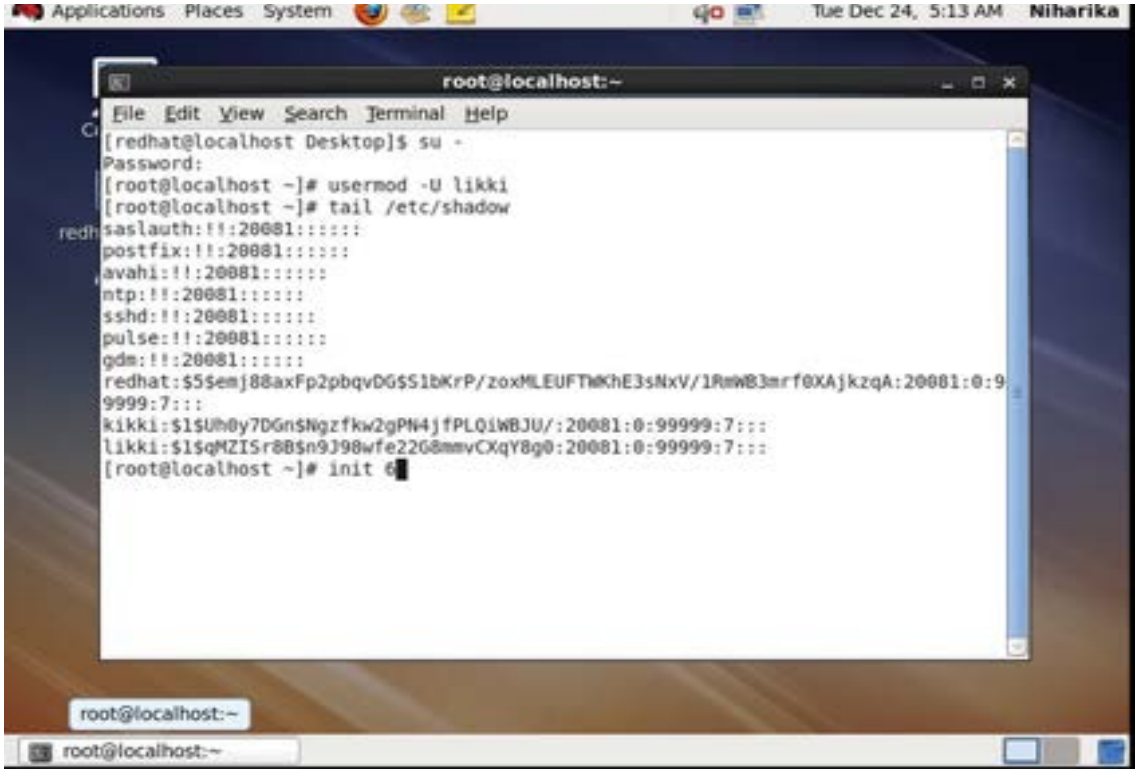
Command 2: usermod –U likki



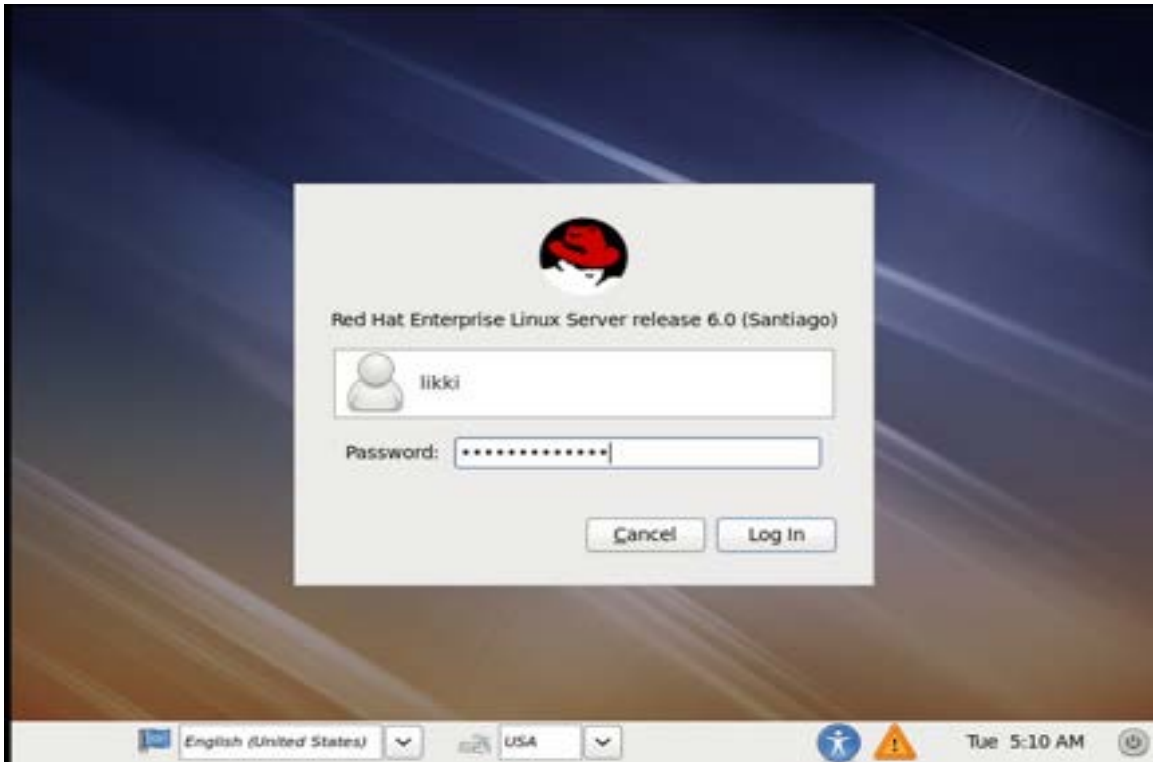
Command 3: tail /etc/shadow

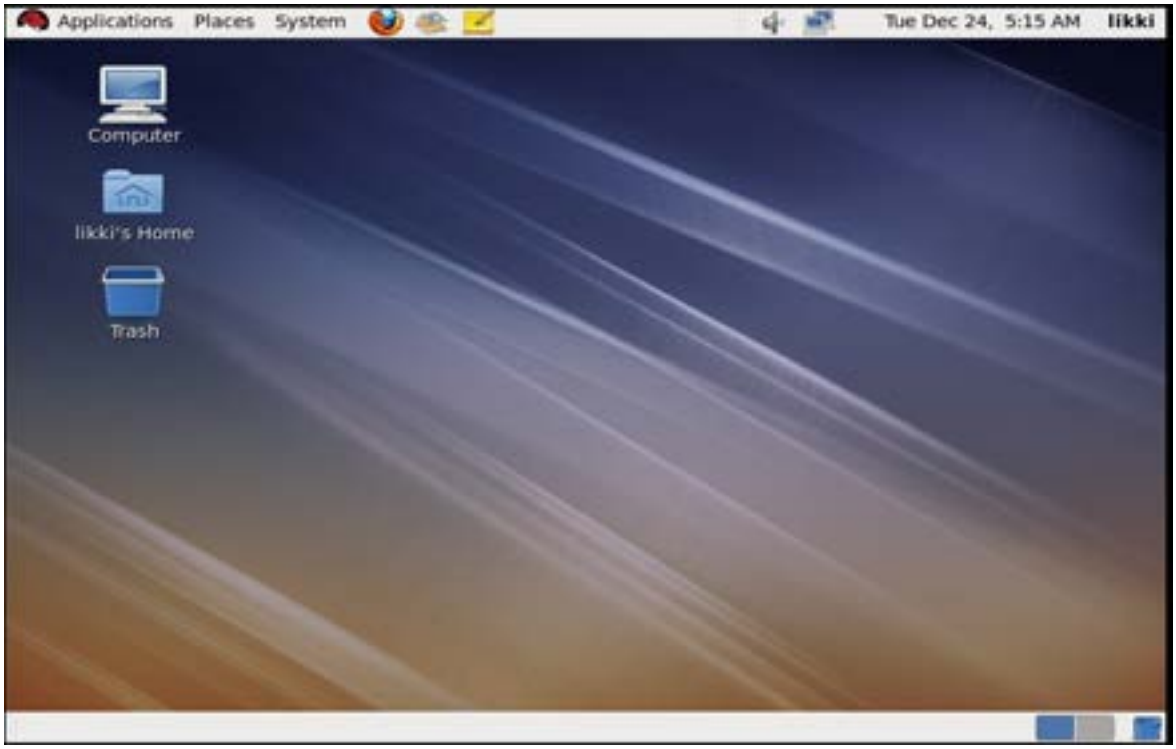


Command 4: init 6



Step 9: Enter the password to see the user





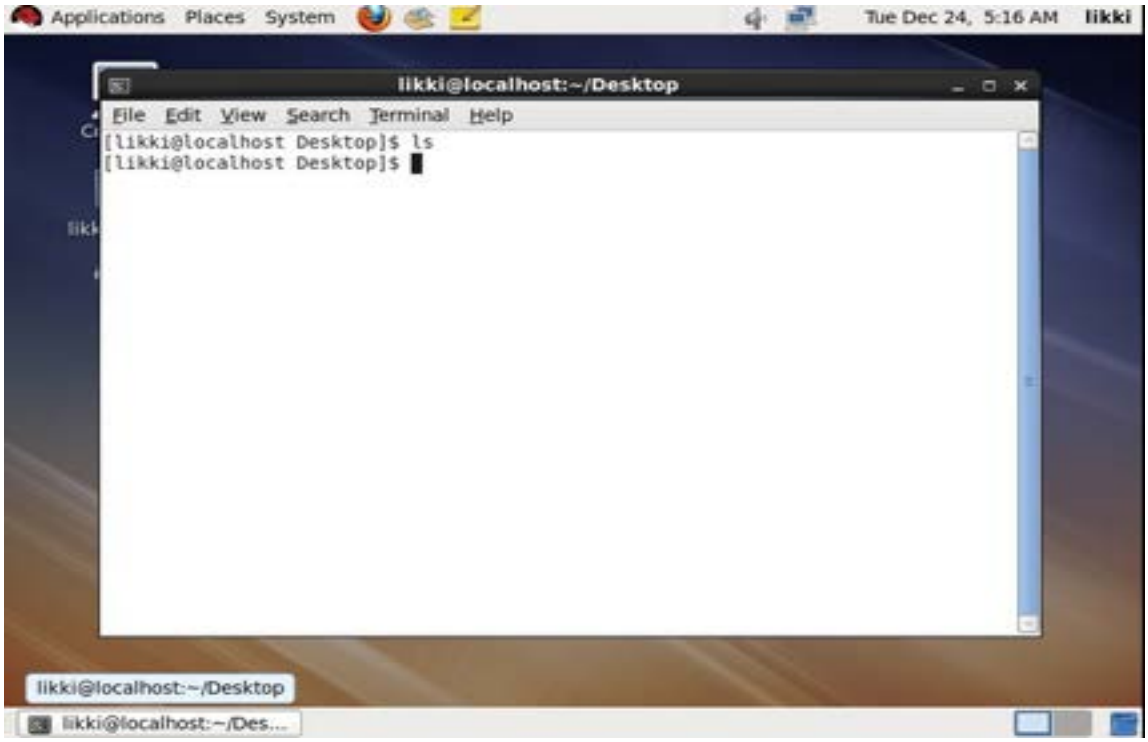
Step 10: Creating a file in folder

First select the user

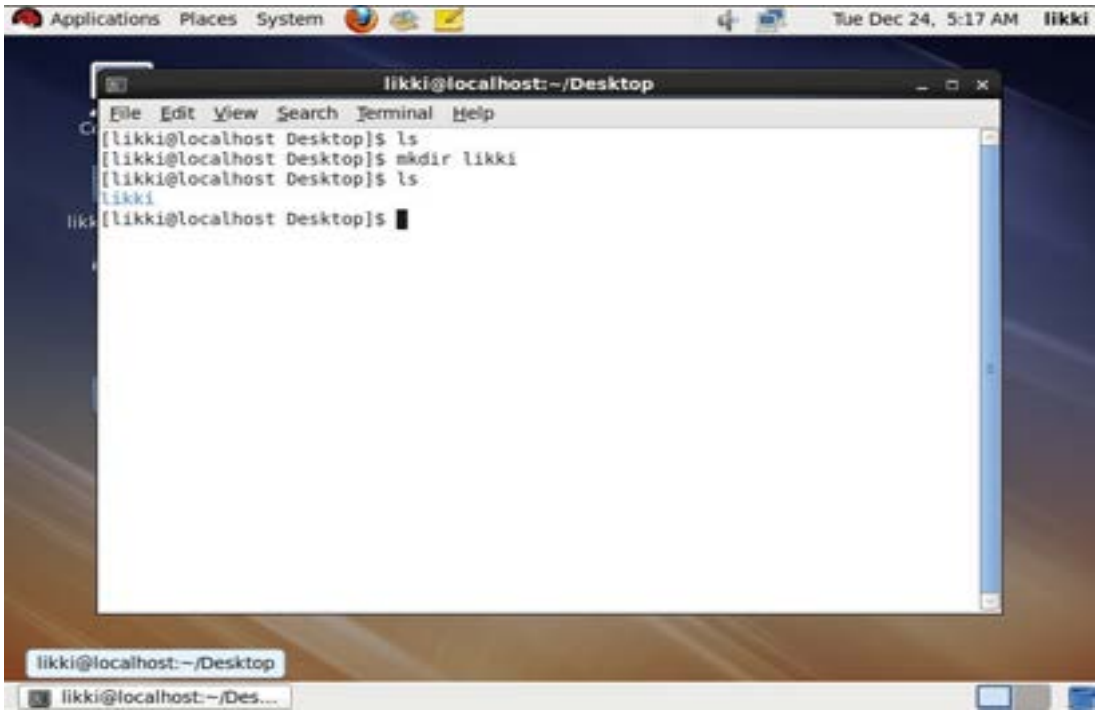
And give the commands

Command 1: ls

Command 2:mkdir likki

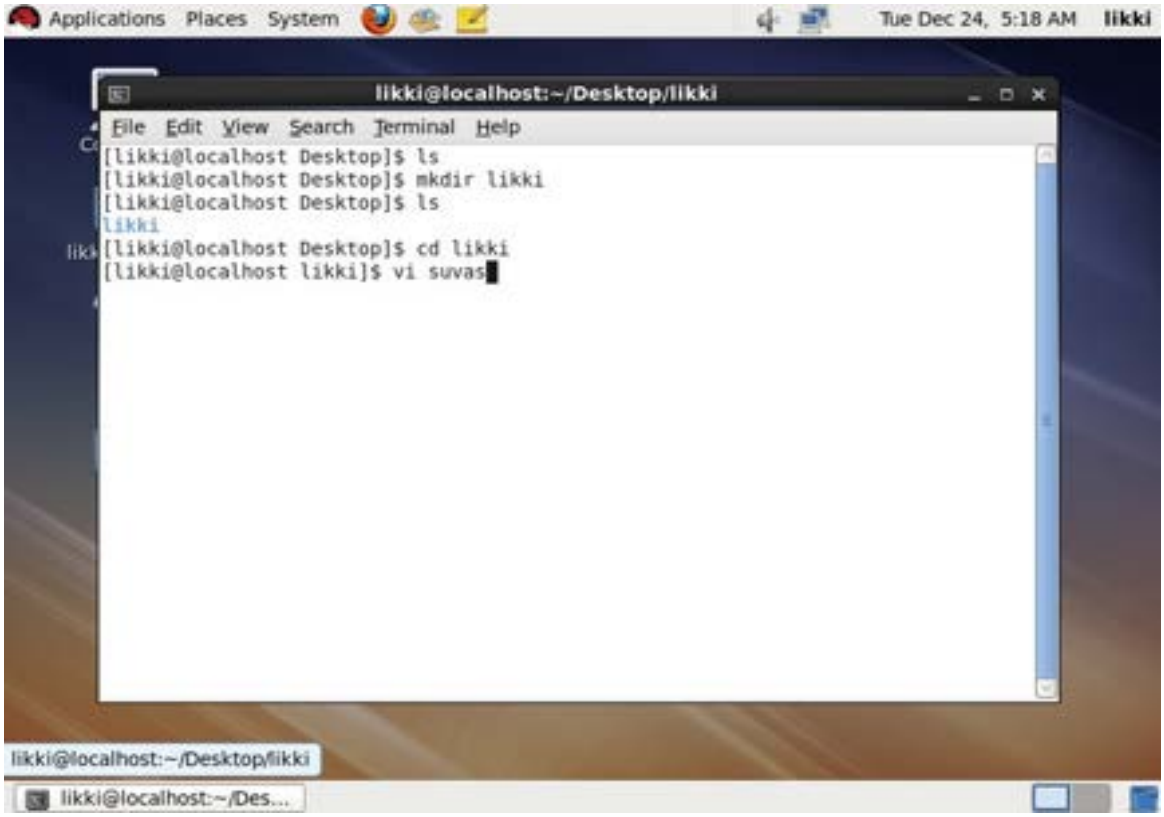


Command 3: ls



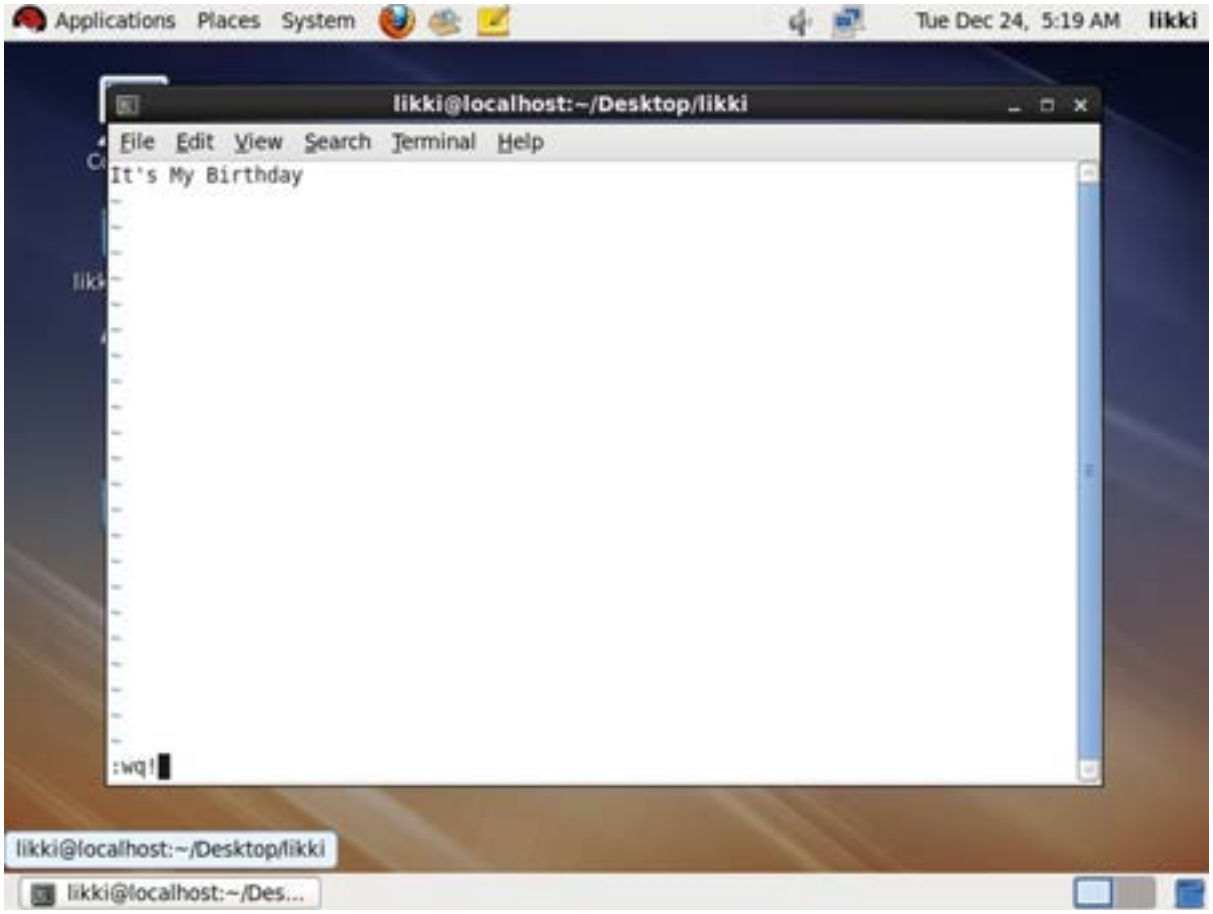
Command 4: cd likki

Command 5: vi suvas



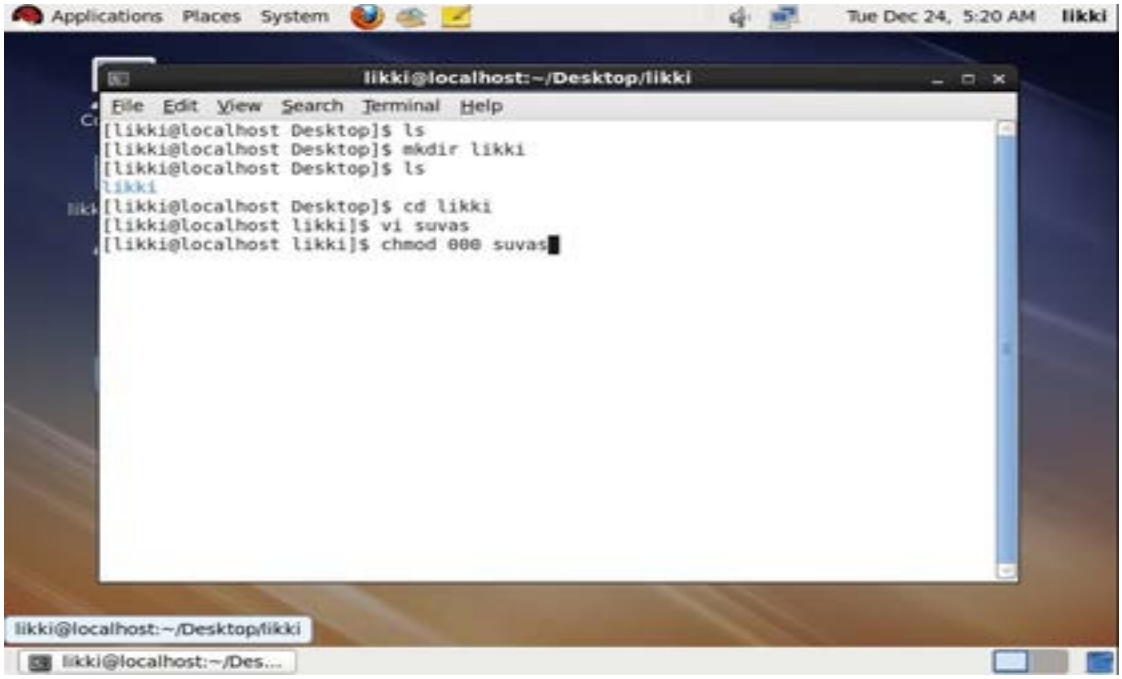
Now, the folder is created

Step 11 Enter some text in the file



Step 12: To lock the file

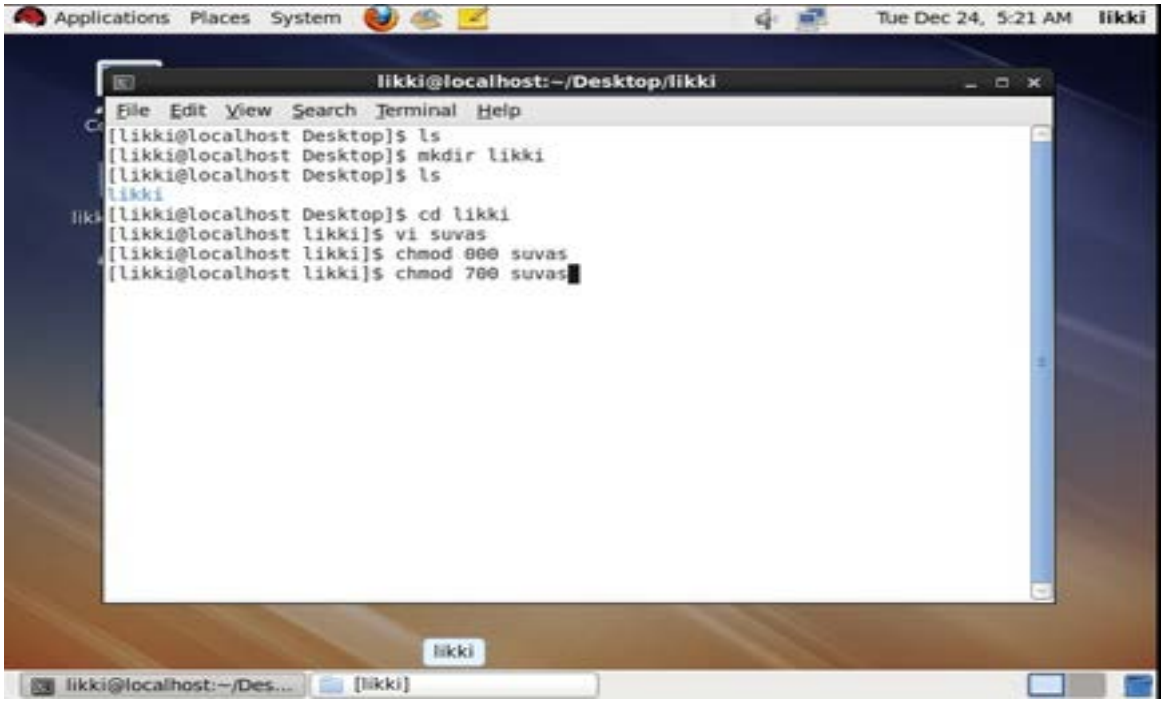
Enter the command as chmod 000 suvas



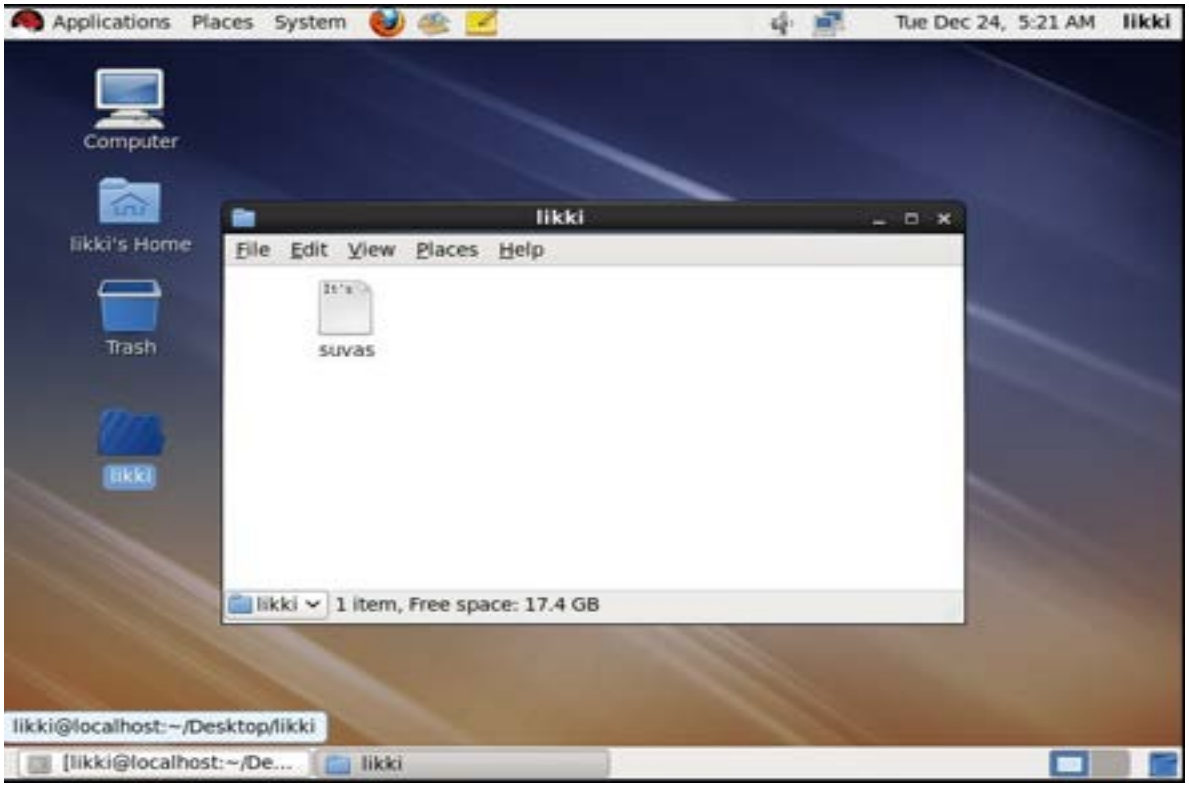
Here, the file locked

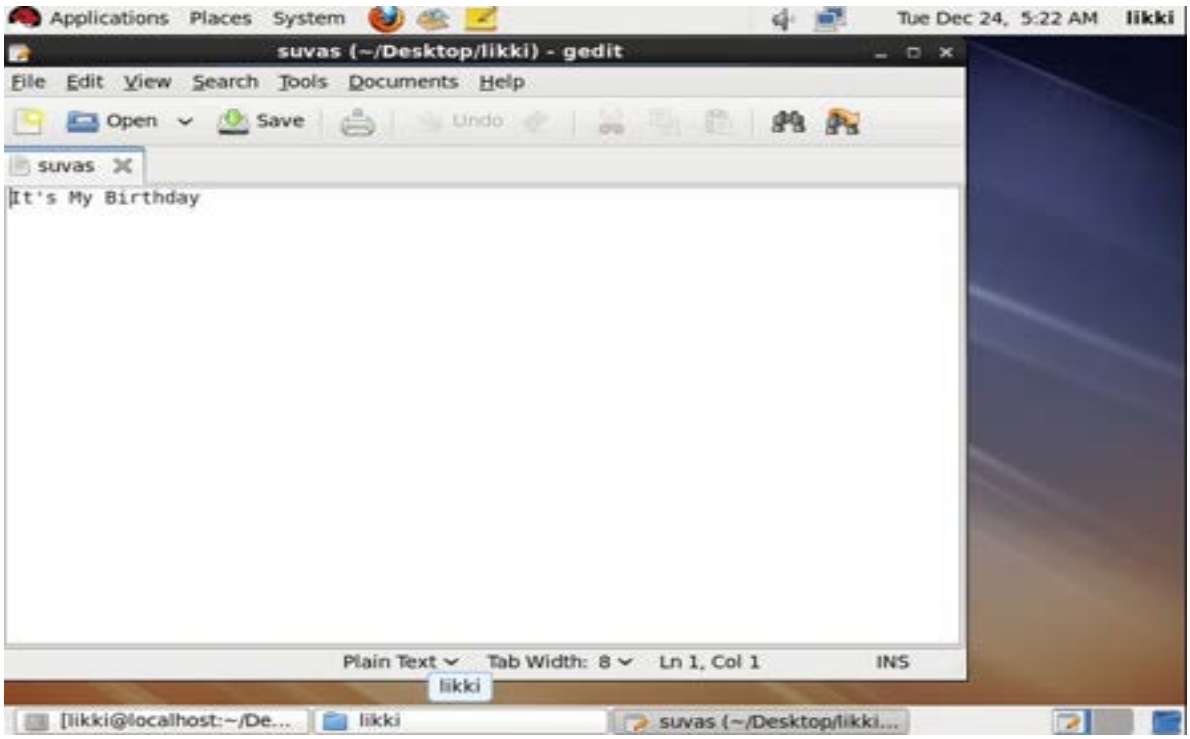
Step 13: To unlock the file

Enter the command ad chmod 700 suvas



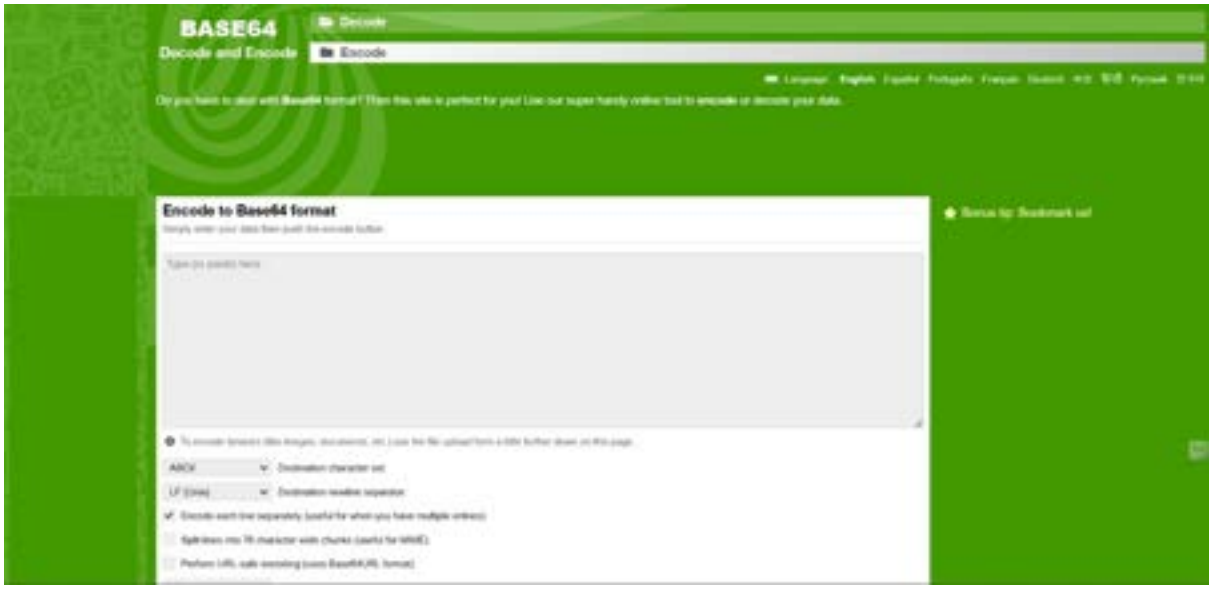
Now, we can able to see the file and the text in that



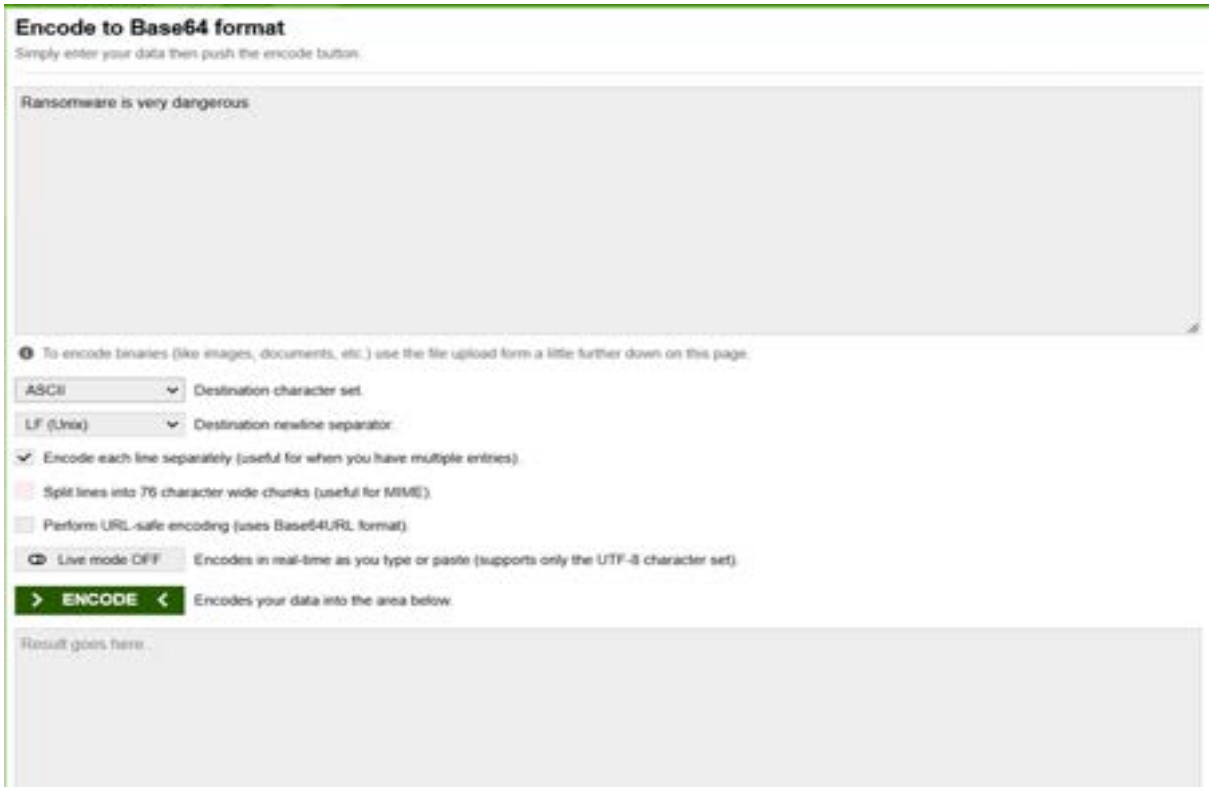


Implementation Of Ransomware Using Base64

Step 1: Open Base64 and select “Encode”

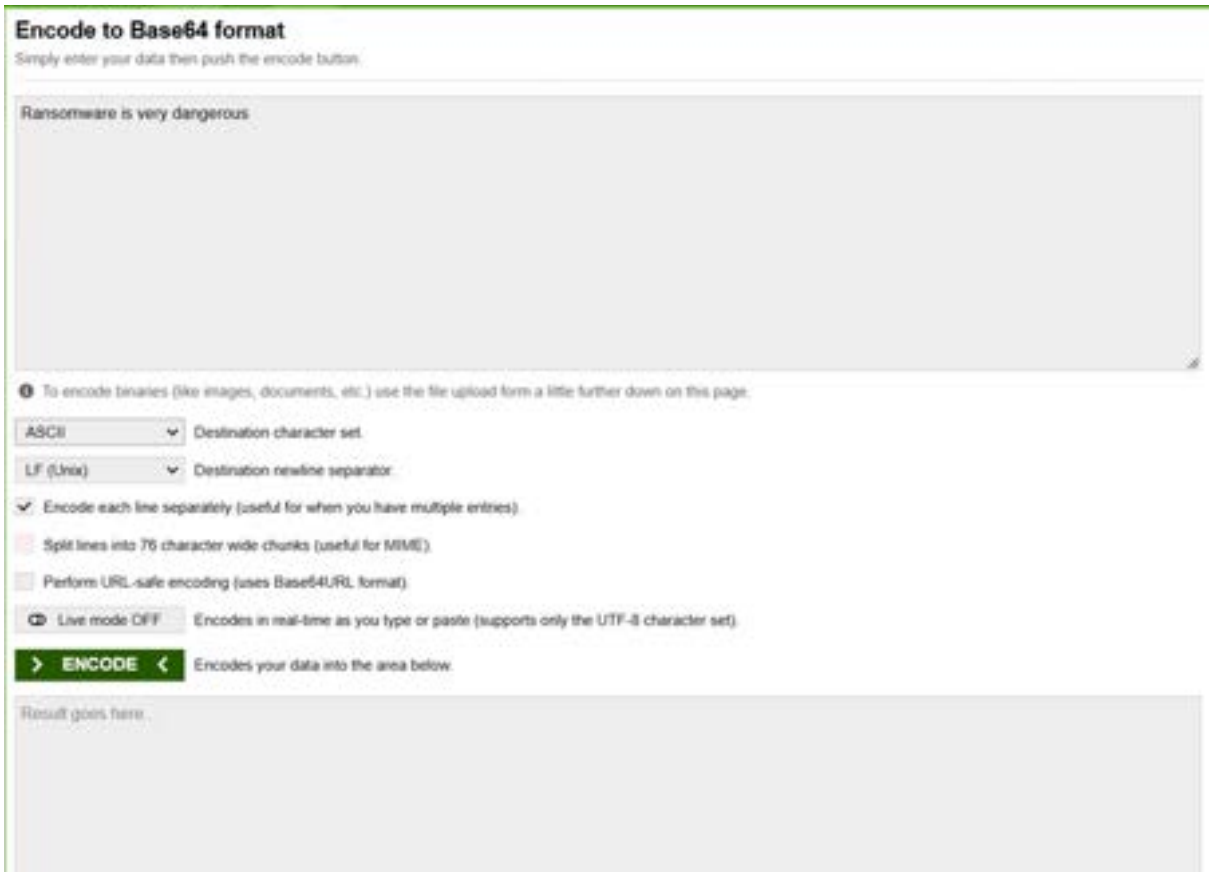


Step 2: Enter some text in the textbox



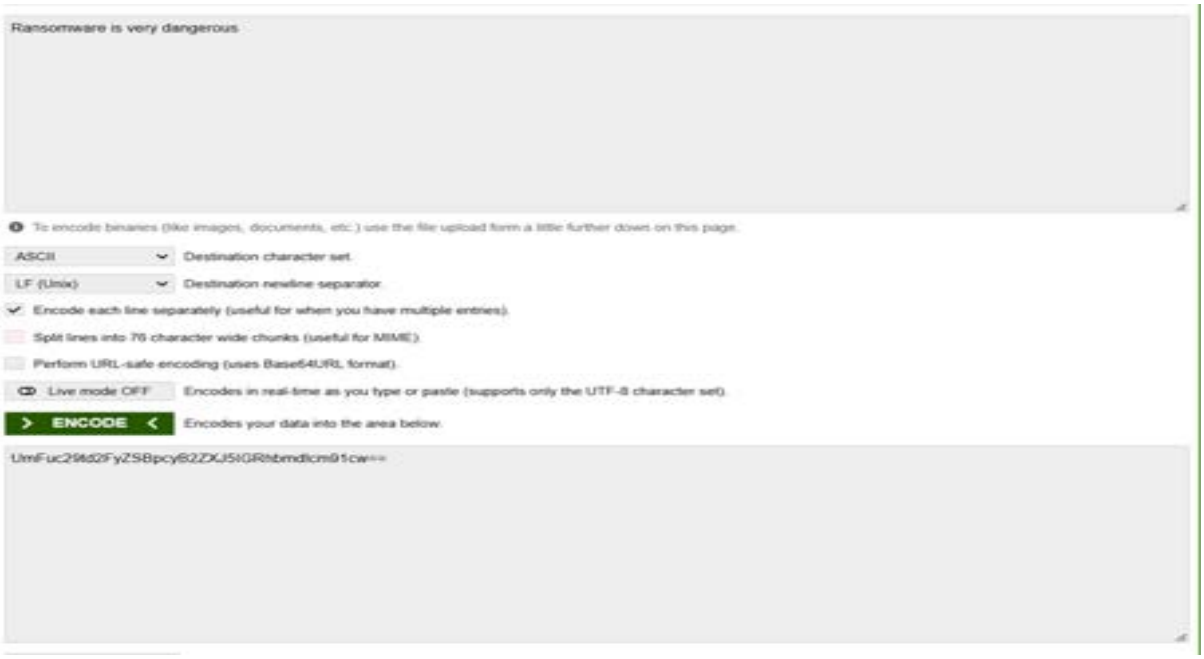
Step 3: Select destination character set as ASCII

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



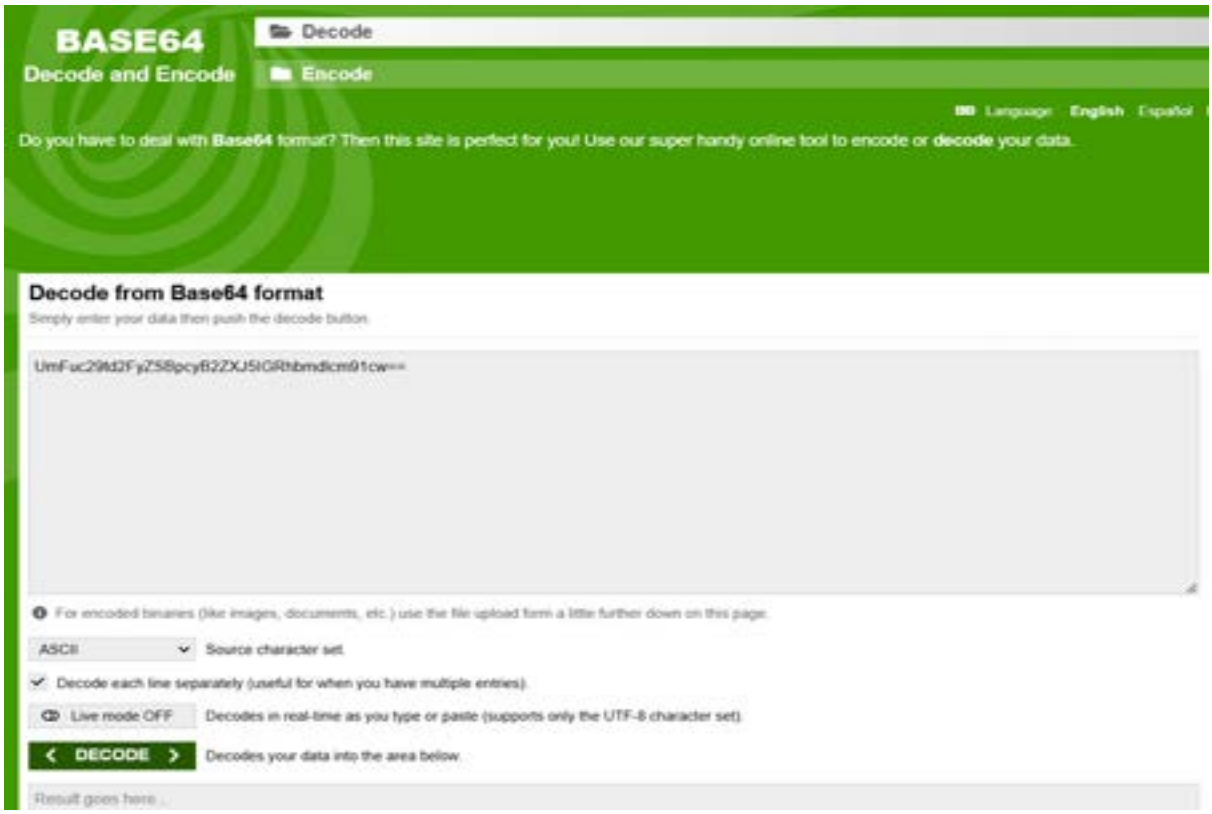
Step 5: Click Encode

Then the text is generated into ciphertext

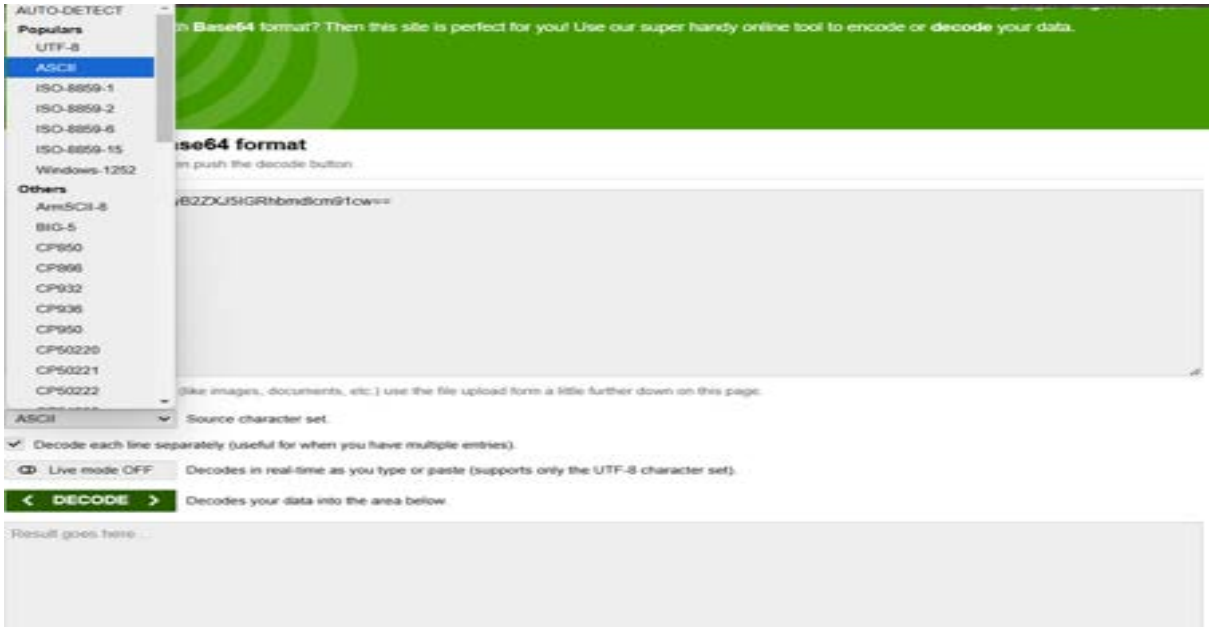


Copy the ciphertext

Step 6: Select Decode and paste the ciphertext



Step 7: Select source character set as ASCII



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

Then, Click Decode

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.