

# Compito W2D4 – Pratica

Corso: Cybersecurity Analyst – Epicode

Studente: Daniele Taormina

Data: 9 ottobre 2025

## Introduzione

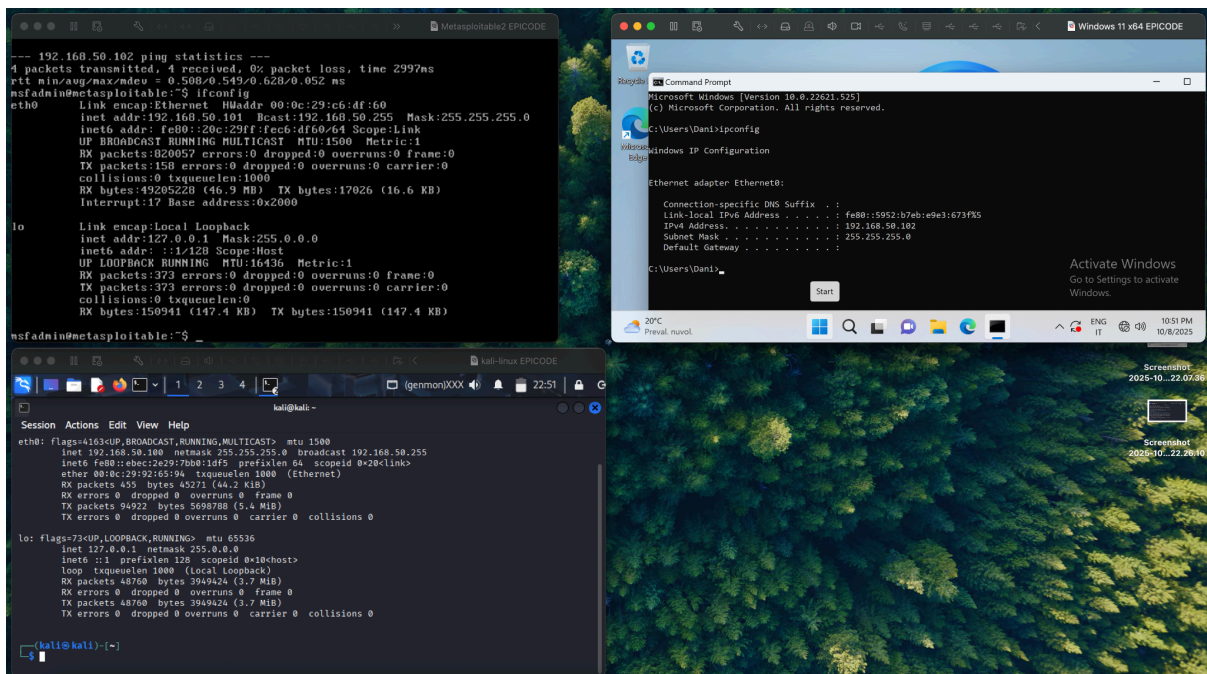
In questo esercizio ho creato un laboratorio virtuale su VMware con tre macchine: Windows 11, Kali Linux e Metasploitable2.

Lo scopo era configurare una rete interna con indirizzi IP statici e verificare la comunicazione tra le macchine tramite comandi ping.

## Indirizzi IP delle macchine

Nella schermata seguente sono visibili gli indirizzi IP assegnati manualmente a ciascuna macchina virtuale:

- Windows 11: **192.168.50.102**
- Kali Linux: **192.168.50.100**
- Metasploitable2: **192.168.50.101**

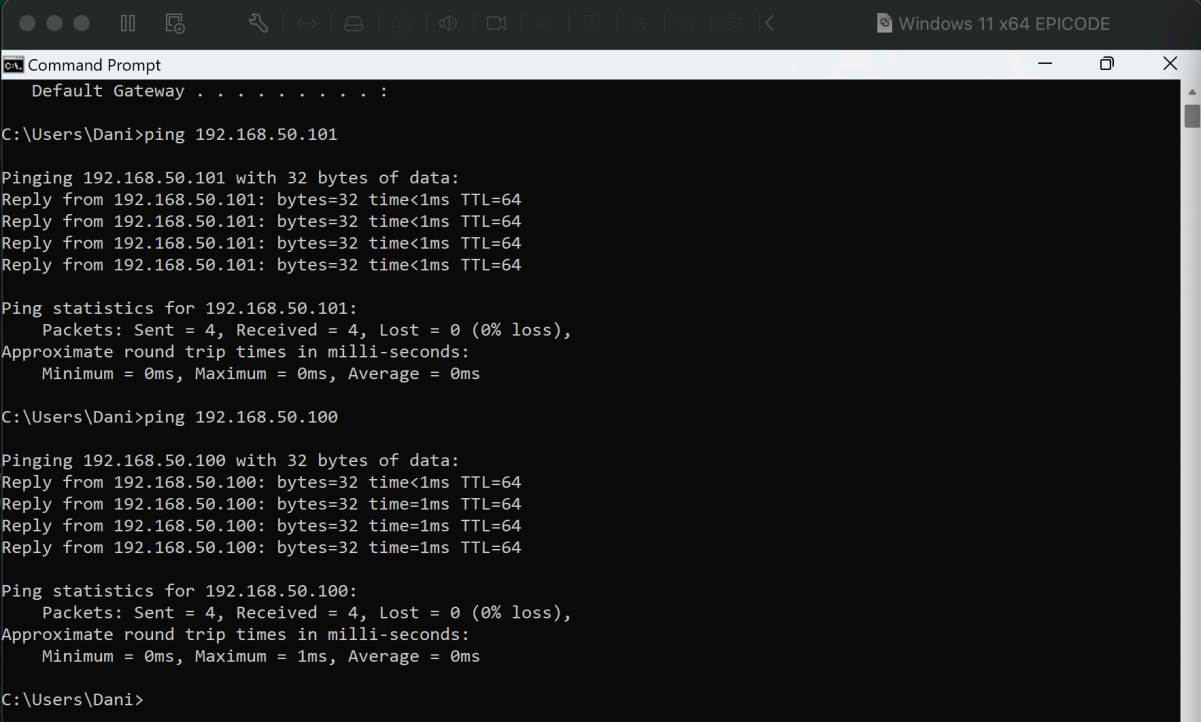


# Verifica con Ping

## Ping da Windows

Dalla macchina Windows 11 è stato eseguito il comando **ping** verso Metasploitable2 (192.168.50.101) e verso Kali Linux (192.168.50.100).

In entrambi i casi i pacchetti sono stati inviati e ricevuti correttamente con **0% packet loss**.



```
Windows 11 x64 EPICODE
Command Prompt
Default Gateway . . . . . :

C:\Users\Dani>ping 192.168.50.101

Pinging 192.168.50.101 with 32 bytes of data:
Reply from 192.168.50.101: bytes=32 time<1ms TTL=64
Reply from 192.168.50.101: bytes=32 time<1ms TTL=64
Reply from 192.168.50.101: bytes=32 time<1ms TTL=64
Reply from 192.168.50.101: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.50.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Dani>ping 192.168.50.100

Pinging 192.168.50.100 with 32 bytes of data:
Reply from 192.168.50.100: bytes=32 time<1ms TTL=64
Reply from 192.168.50.100: bytes=32 time=1ms TTL=64
Reply from 192.168.50.100: bytes=32 time=1ms TTL=64
Reply from 192.168.50.100: bytes=32 time=1ms TTL=64

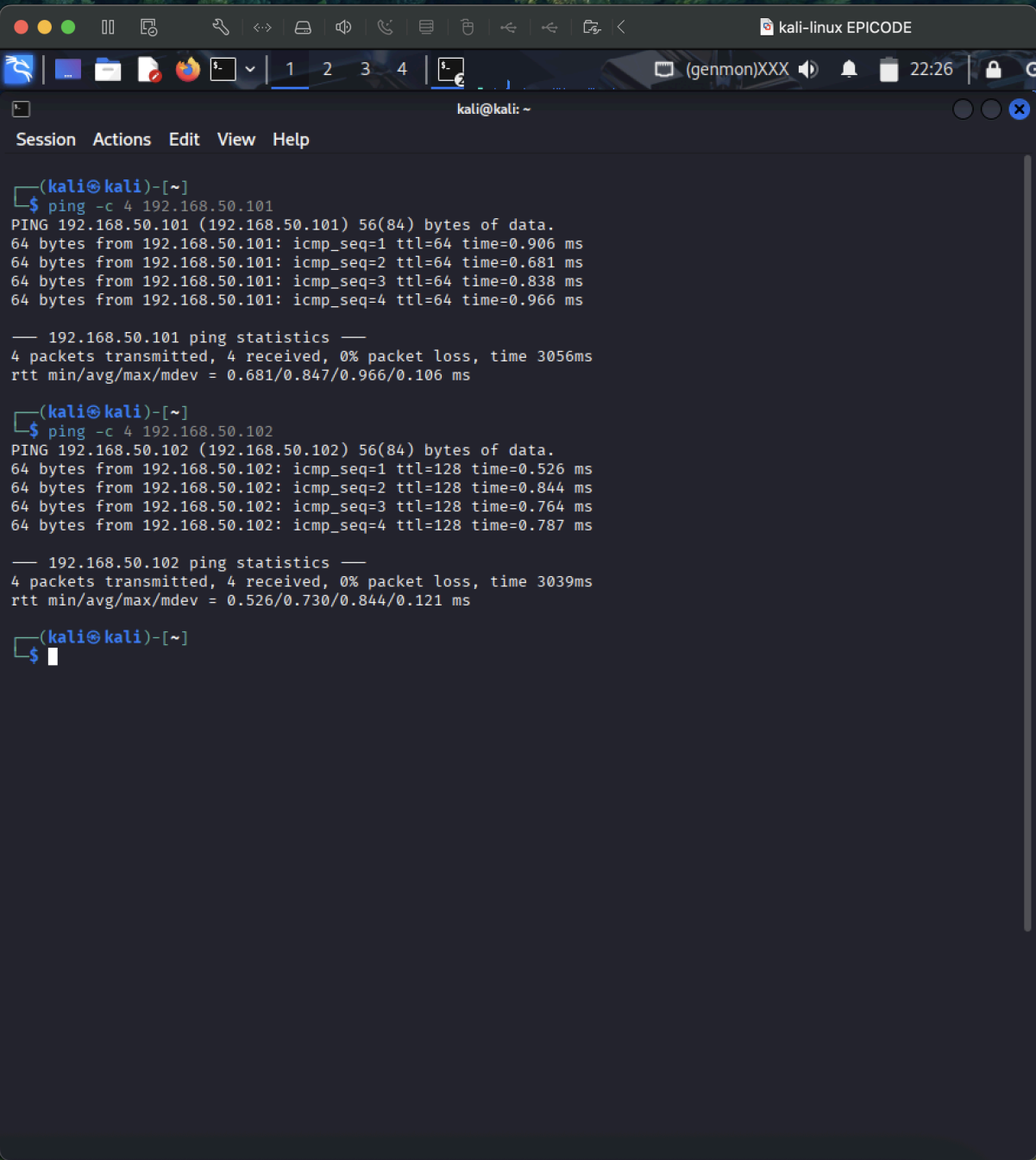
Ping statistics for 192.168.50.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Dani>
```

## Ping da Kali

Dalla macchina Kali Linux è stato eseguito il ping verso Metasploitable2 (192.168.50.101) e verso Windows (192.168.50.102).

Il risultato mostra 4 pacchetti inviati e ricevuti con successo, senza perdite.



```
(kali@kali)-[~]
$ ping -c 4 192.168.50.101
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data.
64 bytes from 192.168.50.101: icmp_seq=1 ttl=64 time=0.906 ms
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=0.681 ms
64 bytes from 192.168.50.101: icmp_seq=3 ttl=64 time=0.838 ms
64 bytes from 192.168.50.101: icmp_seq=4 ttl=64 time=0.966 ms

--- 192.168.50.101 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3056ms
rtt min/avg/max/mdev = 0.681/0.847/0.966/0.106 ms

(kali@kali)-[~]
$ ping -c 4 192.168.50.102
PING 192.168.50.102 (192.168.50.102) 56(84) bytes of data.
64 bytes from 192.168.50.102: icmp_seq=1 ttl=128 time=0.526 ms
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=0.844 ms
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=0.764 ms
64 bytes from 192.168.50.102: icmp_seq=4 ttl=128 time=0.787 ms

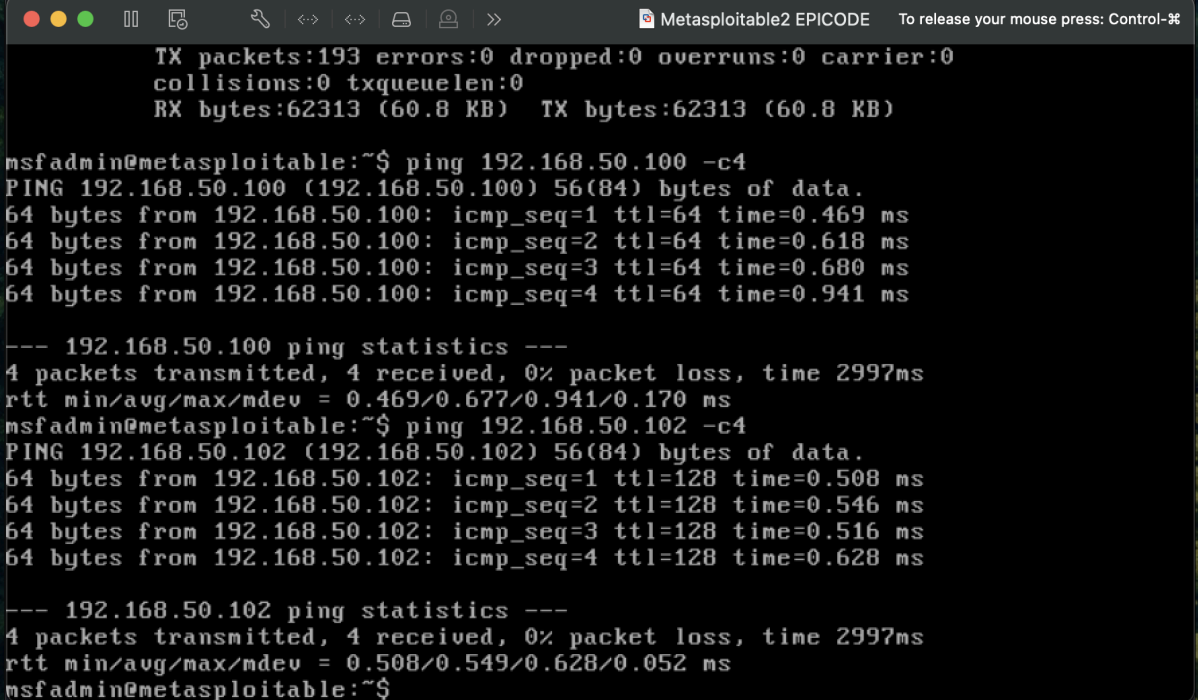
--- 192.168.50.102 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3039ms
rtt min/avg/max/mdev = 0.526/0.730/0.844/0.121 ms

(kali@kali)-[~]
$
```

## Ping da Metasploitable2

Dalla macchina Metasploitable2 è stato eseguito il ping verso Kali Linux (192.168.50.100) e verso Windows (192.168.50.102).

Anche in questo caso la comunicazione è riuscita con **0% packet loss**.



```
TX packets:193 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:62313 (60.8 KB) TX bytes:62313 (60.8 KB)

msfadmin@metasploitable:~$ ping 192.168.50.100 -c4
PING 192.168.50.100 (192.168.50.100) 56(84) bytes of data.
64 bytes from 192.168.50.100: icmp_seq=1 ttl=64 time=0.469 ms
64 bytes from 192.168.50.100: icmp_seq=2 ttl=64 time=0.618 ms
64 bytes from 192.168.50.100: icmp_seq=3 ttl=64 time=0.680 ms
64 bytes from 192.168.50.100: icmp_seq=4 ttl=64 time=0.941 ms

--- 192.168.50.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2997ms
rtt min/avg/max/mdev = 0.469/0.677/0.941/0.170 ms
msfadmin@metasploitable:~$ ping 192.168.50.102 -c4
PING 192.168.50.102 (192.168.50.102) 56(84) bytes of data.
64 bytes from 192.168.50.102: icmp_seq=1 ttl=128 time=0.508 ms
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=0.546 ms
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=0.516 ms
64 bytes from 192.168.50.102: icmp_seq=4 ttl=128 time=0.628 ms

--- 192.168.50.102 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2997ms
rtt min/avg/max/mdev = 0.508/0.549/0.628/0.052 ms
msfadmin@metasploitable:~$
```

Anche se non era richiesto dall'esercizio, ho deciso di utilizzare lo strumento **netdiscover** per avere una conferma ulteriore della configurazione di rete.

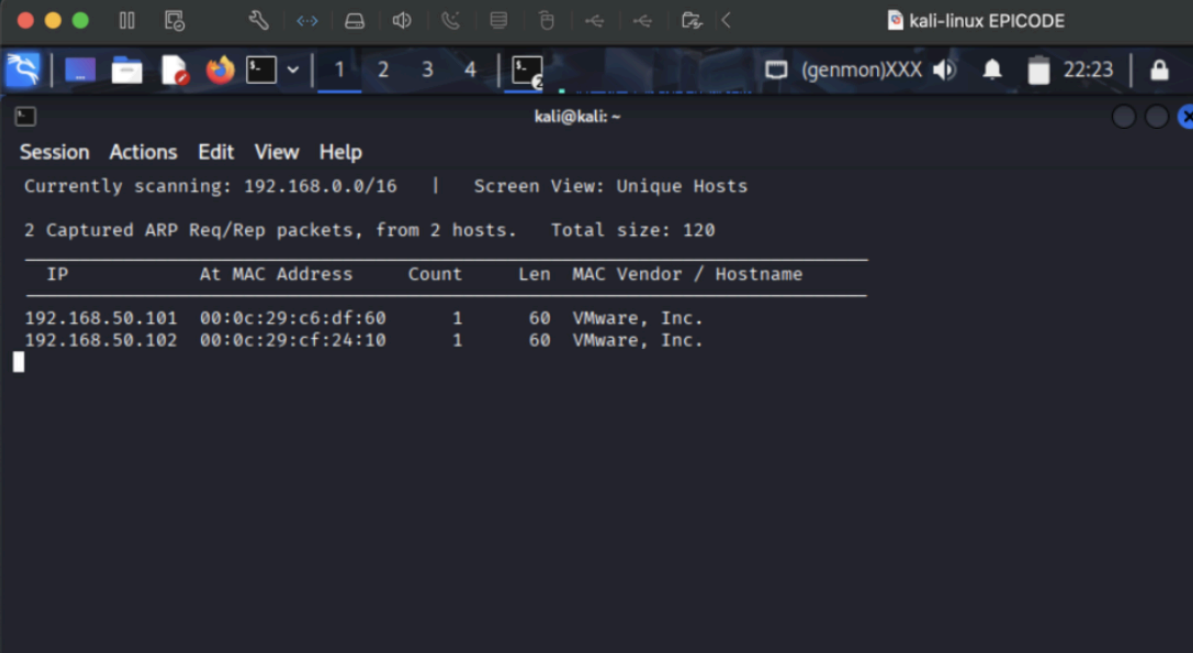
Il comando ha rilevato correttamente le tre macchine collegate nella stessa rete interna:

192.168.50.100 Kali Linux

192.168.50.101 Metasploitable2

192.168.50.102 Windows 11

Questo risultato conferma la buona riuscita della configurazione e della comunicazione tra le VM.



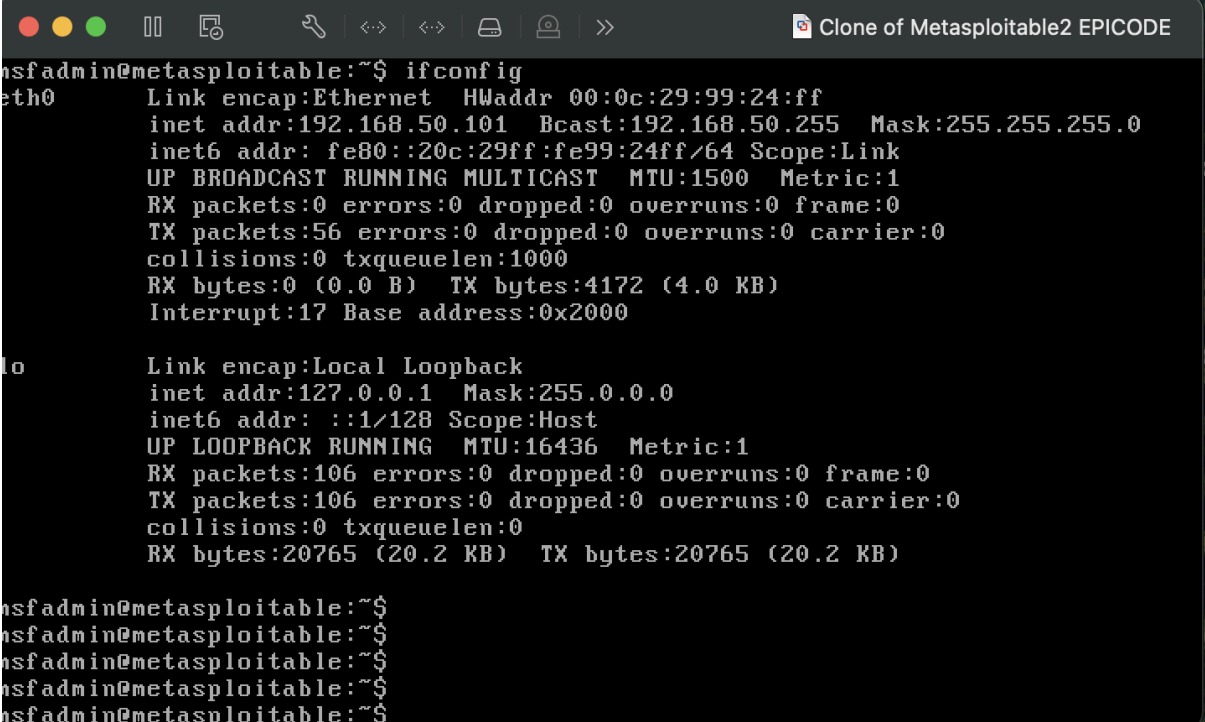
```
kali@kali: ~  
Session Actions Edit View Help  
Currently scanning: 192.168.0.0/16 | Screen View: Unique Hosts  
2 Captured ARP Req/Rep packets, from 2 hosts. Total size: 120  
+-----+-----+-----+-----+-----+-----+  
IP           At MAC Address    Count  Len  MAC Vendor / Hostname  
+-----+-----+-----+-----+-----+-----+  
192.168.50.101 00:0c:29:c6:df:60    1     60  VMware, Inc.  
192.168.50.102 00:0c:29:cf:24:10    1     60  VMware, Inc.
```

## Sezione facoltativa – Clone di Metasploitable2 (e verifica)

Ho creato un clone della macchina **Metasploitable2** come esercizio facoltativo. Dopo aver avviato il clone ho eseguito ifconfig per verificare che la macchina clonata riportasse lo stesso indirizzo IP atteso nella rete virtuale.

Successivamente ho eseguito un ping dalla macchina clonata verso una delle altre VM per verificare che il clone svolgesse le stesse funzioni della macchina originale.

### Test eseguiti e risultati:



```
nsfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:99:24:ff
          inet addr:192.168.50.101  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe99:24ff/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:56 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:4172 (4.0 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:106 errors:0 dropped:0 overruns:0 frame:0
          TX packets:106 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:20765 (20.2 KB)  TX bytes:20765 (20.2 KB)

nsfadmin@metasploitable:~$
nsfadmin@metasploitable:~$
nsfadmin@metasploitable:~$
nsfadmin@metasploitable:~$
nsfadmin@metasploitable:~$
```

output ifconfig sulla VM clonata — si vede l'indirizzo IP assegnato (uguale a quello previsto per la macchina nella rete).

```
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:106 errors:0 dropped:0 overruns:0 frame:0
TX packets:106 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:20765 (20.2 KB) TX bytes:20765 (20.2 KB)

msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ ping 192.168.50.100
PING 192.168.50.100 (192.168.50.100) 56(84) bytes of data.
64 bytes from 192.168.50.100: icmp_seq=1 ttl=64 time=2.26 ms
64 bytes from 192.168.50.100: icmp_seq=2 ttl=64 time=0.447 ms
64 bytes from 192.168.50.100: icmp_seq=3 ttl=64 time=0.256 ms
64 bytes from 192.168.50.100: icmp_seq=4 ttl=64 time=0.408 ms
64 bytes from 192.168.50.100: icmp_seq=5 ttl=64 time=0.434 ms
64 bytes from 192.168.50.100: icmp_seq=6 ttl=64 time=0.382 ms
64 bytes from 192.168.50.100: icmp_seq=7 ttl=64 time=0.410 ms
64 bytes from 192.168.50.100: icmp_seq=8 ttl=64 time=0.408 ms

--- 192.168.50.100 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7002ms
rtt min/avg/max/mdev = 0.256/0.626/2.269/0.623 ms
msfadmin@metasploitable:~$ _
```

ping dalla VM clonata verso macchina kali — il ping ha avuto esito positivo (0% packet loss).

## Conclusion

Grazie alle prove effettuate si dimostra che le tre macchine virtuali comunicano correttamente nella rete interna.

Ogni VM è stata in grado di pingare le altre due senza perdite di pacchetti; inoltre la creazione e il test del clone di Metasploitable2 mostrano che il clone opera come l'originale.

La scansione netdiscover ha confermato la presenza degli host nella rete.

L'esercizio è stato completato con successo.