

ESERCIZIO MACCHINE VIRTUALI VIRTUALBOX

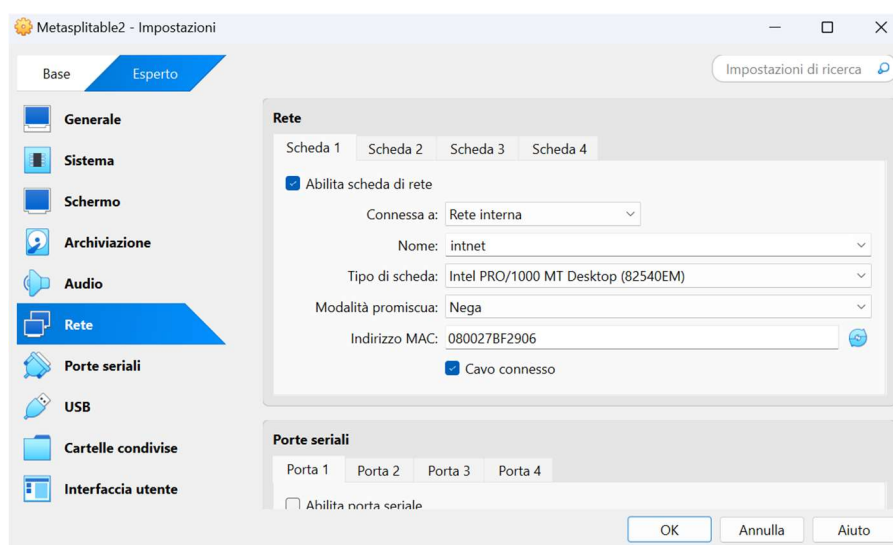
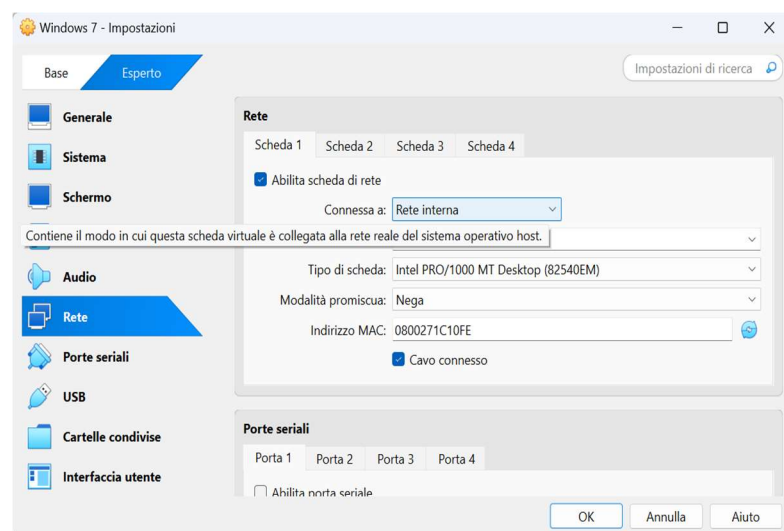
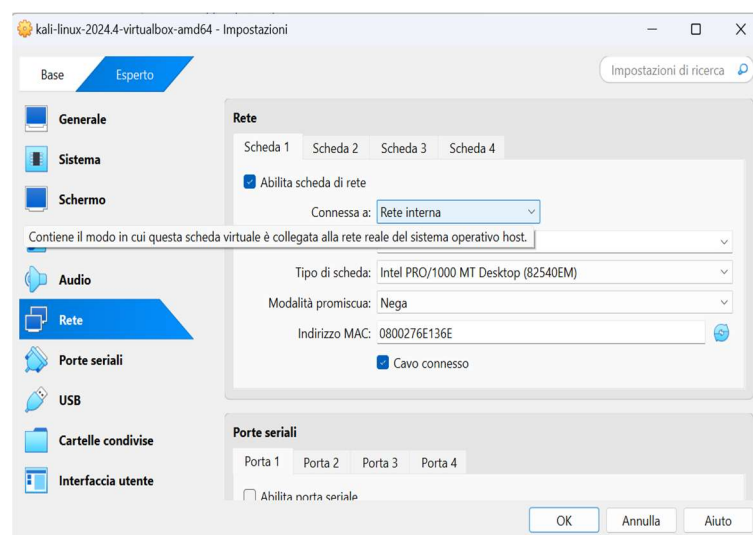
In questo esercizio andremo a creare un laboratorio virtuale composto da 3 macchine virtuali (Kali Linux, Metasploitable e Windows7) collegate tra di loro tramite rete interna.

RICHIESTA ESERCIZIO:

- 1.** Creare un laboratorio virtuale con le seguenti macchine:
 - Kali Linux
 - Metasploitable
 - Windows 7
- 2.** Mettere in comunicazione le 3 macchine appena create tramite rete interna
- 3.** Il PC host non deve avere nessuna connessione con le macchine virtuali

SOLUZIONE ESERCIZIO:

1. Per prima cosa, una volta create le nostre 3 macchine virtuali, dobbiamo andare a impostare ad ognuna di essa una connessione di tipo interna attraverso il menu **Impostazioni / Esperto / Rete** come mostrato nelle figure sottostanti. In questo modo creiamo una connessione di rete interna, ovvero la connessione avviene solamente tra le macchine virtuali installate, il PC host non ha alcuna connessione con le macchine virtuali.



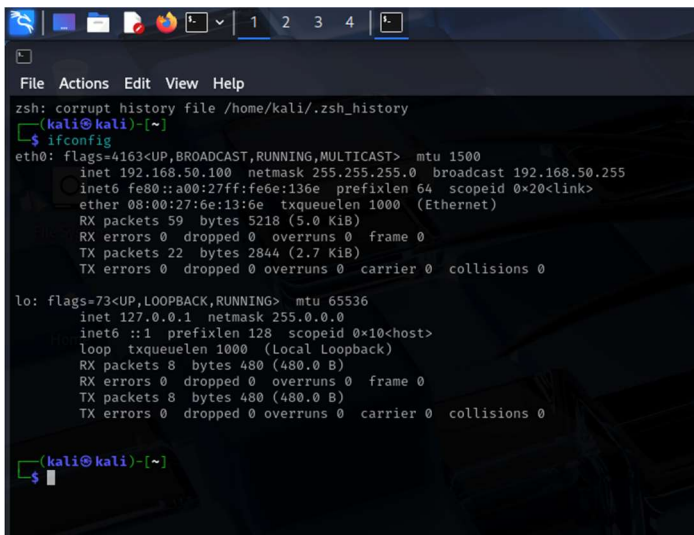
2. Una volta configurato le macchine virtuali in rete interna, dobbiamo andare ad assegnare ad ogni macchina installata un suo indirizzo IP statico.

Useremo i seguenti indirizzi IP per ogni macchina:

- Kali linux: **192.168.50.100/24**
- Metasploitable: **192.168.50.101/24**
- Windows 7: **192.168.50.102/24**

Di seguito le immagini con che dimostrano che ad ogni macchina abbiamo associato il proprio indirizzo IP statico:

Kali Linux

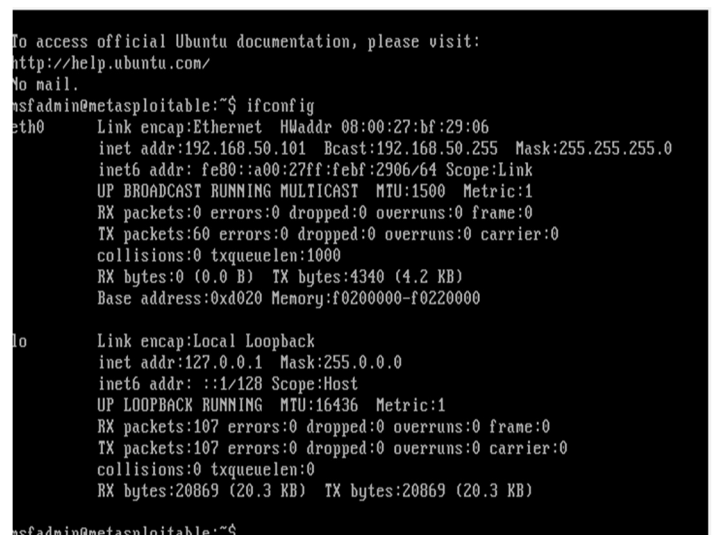


```
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.50.100 netmask 255.255.255.0 broadcast 192.168.50.255
    inet6 fe80::a00:27ff:fe6e:136e prefixlen 64 scopeid 0<link>
    ether 08:00:27:6e:13:6e txqueuelen 1000 (Ethernet)
    RX packets 59 bytes 5218 (5.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 22 bytes 2844 (2.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 480 (480.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 480 (480.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)~$
```

Metasploit

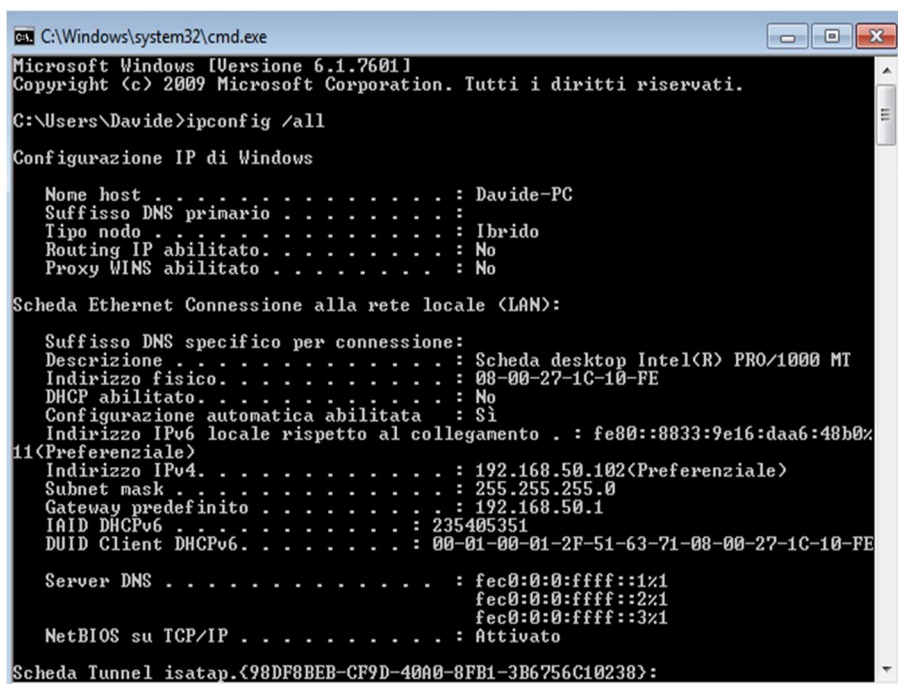


```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:bf:29:06
          inet addr:192.168.50.101 Bcast:192.168.50.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:febf:2906/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:60 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:4340 (4.2 KB)
          Base address:0xd020 Memory:f0200000-f0220000

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:107 errors:0 dropped:0 overruns:0 frame:0
          TX packets:107 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:20869 (20.3 KB)  TX bytes:20869 (20.3 KB)

msfadmin@metasploitable:~$
```

Windows 7



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Versione 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tutti i diritti riservati.

C:\Users\Davide>ipconfig /all

Configurazione IP di Windows

Nome host . . . . . : Davide-PC
Suffisso DNS primario . . . . . :
Tipo nodo . . . . . : Ibrido
Routing IP abilitato. . . . . : No
Proxy WINS abilitato . . . . . : No

Scheda Ethernet Connessione alla rete locale (LAN):

Suffisso DNS specifico per connessione:
Descrizione . . . . . : Scheda desktop Intel(R) PRO/1000 MT
Indirizzo fisico. . . . . : 08-00-27-1C-10-FE
DHCP abilitato. . . . . : No
Configurazione automatica abilitata : Si
Indirizzo IPv6 locale rispetto al collegamento . : fe80::8833:9e16:daa6:48b0%11(Preferenziale)
Indirizzo IPv4. . . . . : 192.168.50.102(Preferenziale)
Subnet mask . . . . . : 255.255.255.0
Gateway predefinito . . . . . : 192.168.50.1
IAID DHCPv6 . . . . . : 235405351
DUID Client DHCPv6. . . . . : 00-01-00-01-2F-51-63-71-08-00-27-1C-10-FE

Server DNS . . . . . : fec0:0:0:ffff::1%1
                       fec0:0:0:ffff::2%1
                       fec0:0:0:ffff::3%1

NetBIOS su TCP/IP . . . . . : Attivato

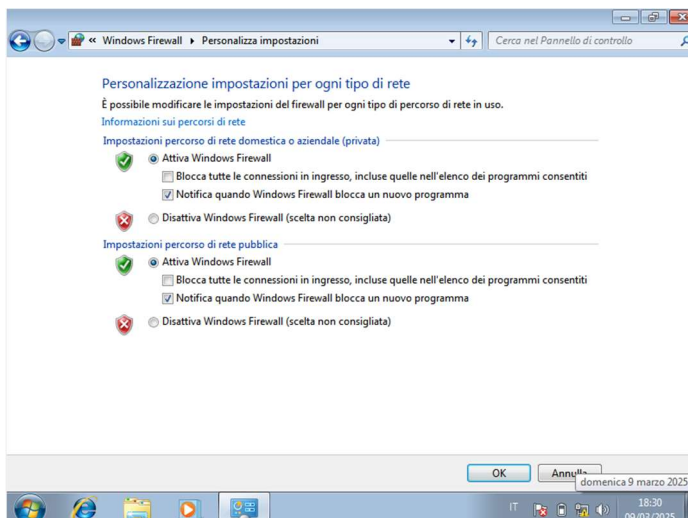
Scheda Tunnel isatap.{98DF8BEB-CF9D-40A0-8FB1-3B6756C10238}:
```

3. Ultimo step che dobbiamo fare è andare a testare se le macchine comunicano tra di loro. Per verificarlo andiamo ad aprire il terminale su ogni macchina ed eseguiamo il comando ping verso l'indirizzo IP di ogni altra macchina installata.

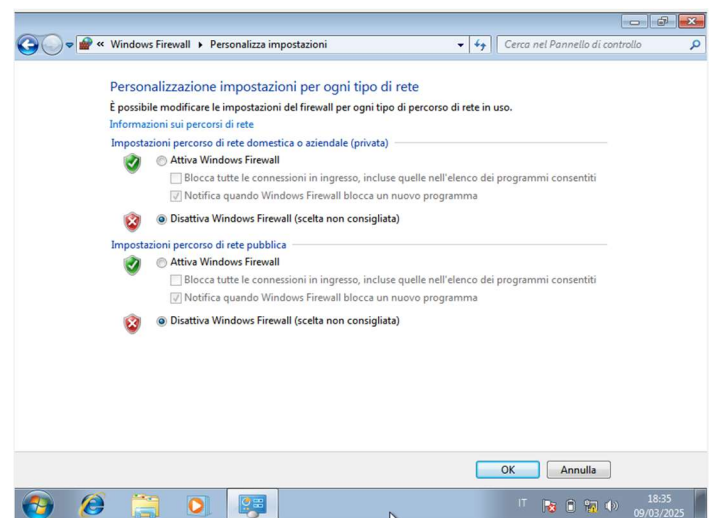
NOTA:

Per far sì che Kali Linux e Metasploitable possano comunicare con Windows 7, è necessario disattivare il firewall sul sistema operativo Windows 7.

Firewall ON



Firewall OFF



Di seguito invece le immagini di ogni test ping effettuato da ogni macchina ad ogni altra macchina. Notare l'avvenuto scambio di pacchetti ad ogni immagine.

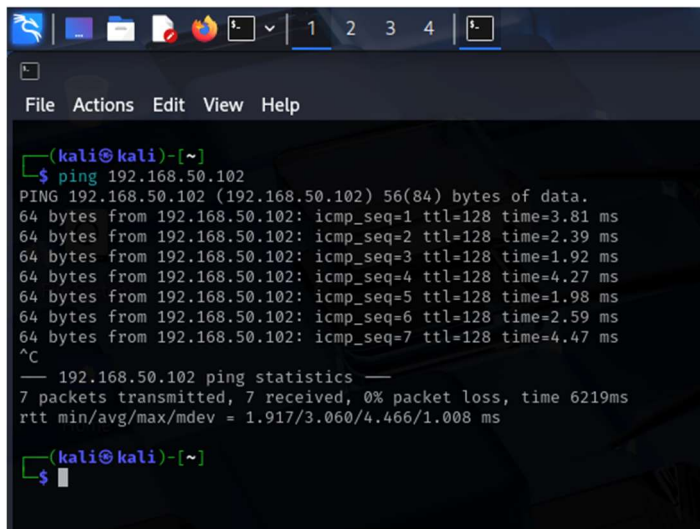
- Ping da **Kali Linux** a **Metasploitable**

```
File Actions Edit View Help

(kali@kali)-[~]
$ ping 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=5.78 ms
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=3.46 ms
64 bytes from 192.168.50.101: icmp_seq=3 ttl=64 time=1.39 ms
64 bytes from 192.168.50.101: icmp_seq=4 ttl=64 time=1.31 ms
64 bytes from 192.168.50.101: icmp_seq=5 ttl=64 time=8.44 ms
64 bytes from 192.168.50.101: icmp_seq=6 ttl=64 time=2.45 ms
64 bytes from 192.168.50.101: icmp_seq=7 ttl=64 time=2.70 ms
64 bytes from 192.168.50.101: icmp_seq=8 ttl=64 time=3.36 ms
^C
--- 192.168.50.101 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7615ms
rtt min/avg/max/mdev = 1.314/3.611/8.442/2.250 ms

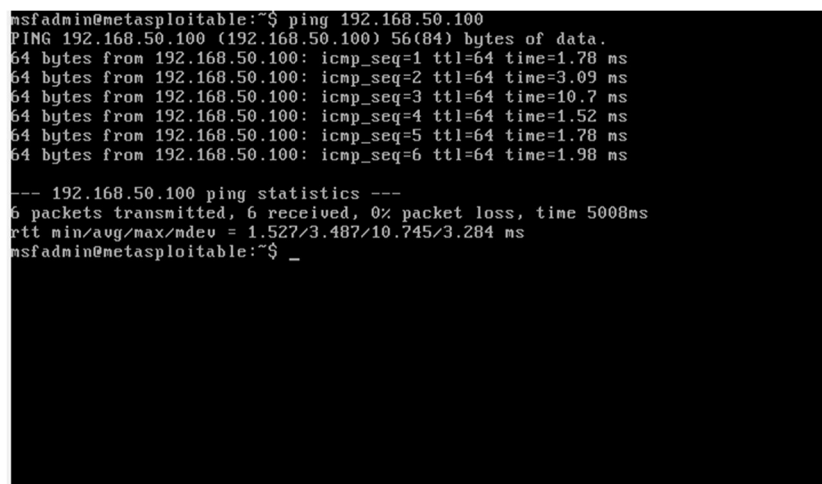
(kali@kali)-[~]
$
```

- Ping da **Kali Linux** a **Windows 7**



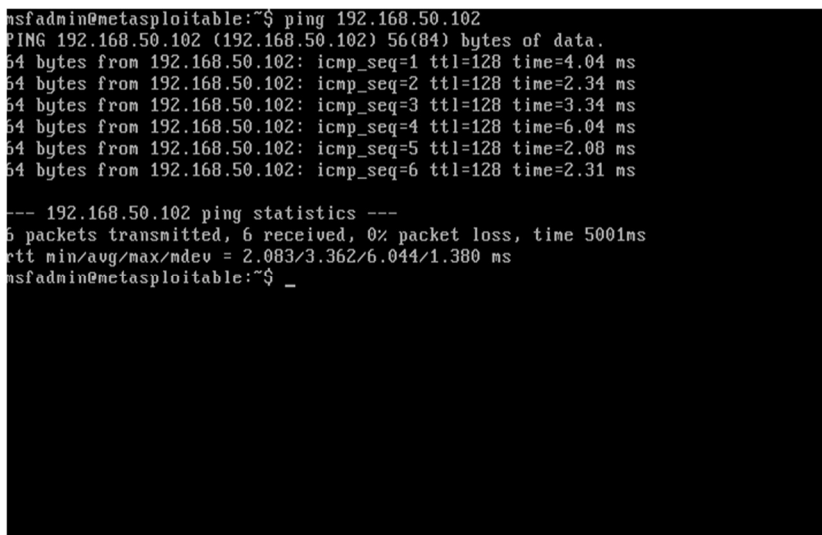
```
(kali㉿kali)-[~]
$ ping 192.168.50.102
PING 192.168.50.102 (192.168.50.102) 56(84) bytes of data.
64 bytes from 192.168.50.102: icmp_seq=1 ttl=128 time=3.81 ms
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=2.39 ms
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=1.92 ms
64 bytes from 192.168.50.102: icmp_seq=4 ttl=128 time=4.27 ms
64 bytes from 192.168.50.102: icmp_seq=5 ttl=128 time=1.98 ms
64 bytes from 192.168.50.102: icmp_seq=6 ttl=128 time=2.59 ms
64 bytes from 192.168.50.102: icmp_seq=7 ttl=128 time=4.47 ms
^C
--- 192.168.50.102 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6219ms
rtt min/avg/max/mdev = 1.917/3.060/4.466/1.008 ms
(kali㉿kali)-[~]
$
```

- Ping da **Metasploitable** a **Kali Linux**



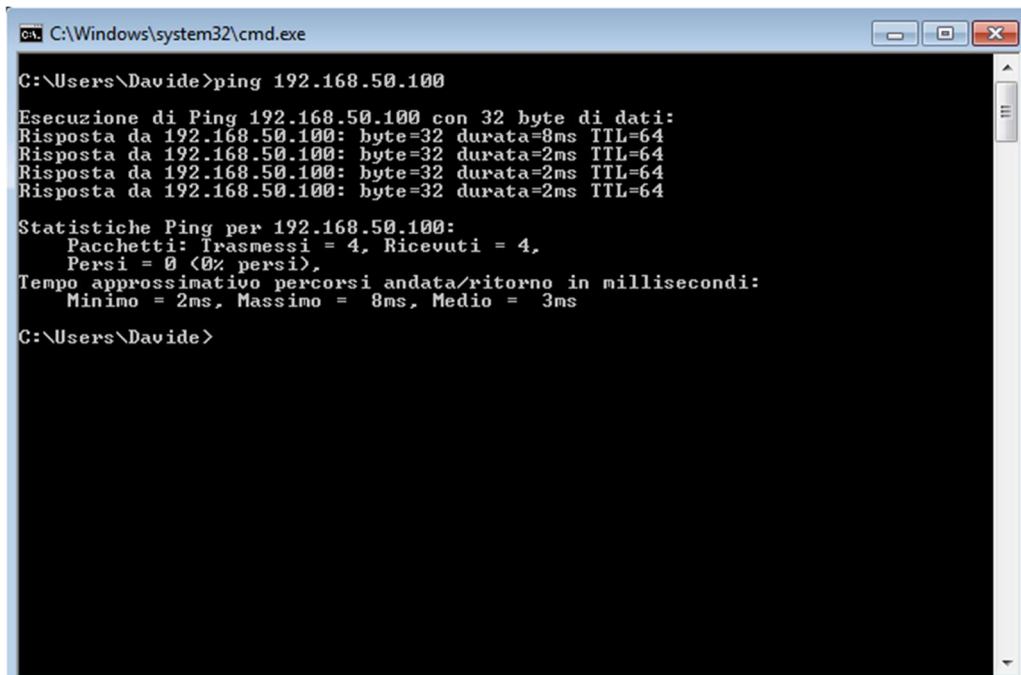
```
msfadmin@metasploitable:~$ ping 192.168.50.100
PING 192.168.50.100 (192.168.50.100) 56(84) bytes of data.
64 bytes from 192.168.50.100: icmp_seq=1 ttl=64 time=1.78 ms
64 bytes from 192.168.50.100: icmp_seq=2 ttl=64 time=3.09 ms
64 bytes from 192.168.50.100: icmp_seq=3 ttl=64 time=10.7 ms
64 bytes from 192.168.50.100: icmp_seq=4 ttl=64 time=1.52 ms
64 bytes from 192.168.50.100: icmp_seq=5 ttl=64 time=1.78 ms
64 bytes from 192.168.50.100: icmp_seq=6 ttl=64 time=1.98 ms
--- 192.168.50.100 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5008ms
rtt min/avg/max/mdev = 1.527/3.487/10.745/3.284 ms
msfadmin@metasploitable:~$
```

- Ping da **Metasploitable** a **Windows 7**



```
msfadmin@metasploitable:~$ ping 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=4.04 ms
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=2.34 ms
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=3.34 ms
64 bytes from 192.168.50.102: icmp_seq=4 ttl=128 time=6.04 ms
64 bytes from 192.168.50.102: icmp_seq=5 ttl=128 time=2.08 ms
64 bytes from 192.168.50.102: icmp_seq=6 ttl=128 time=2.31 ms
--- 192.168.50.102 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5001ms
rtt min/avg/max/mdev = 2.083/3.362/6.044/1.380 ms
msfadmin@metasploitable:~$
```

- Ping da **Windows 7** a **Kali Linux**



```
C:\Windows\system32\cmd.exe

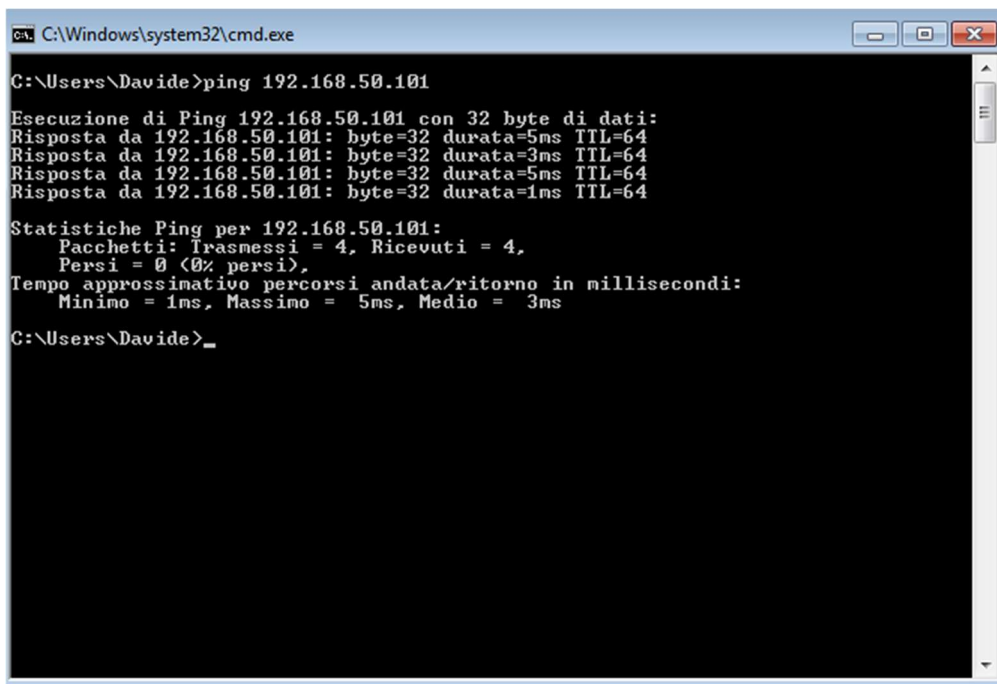
C:\Users\Davide>ping 192.168.50.100

Esecuzione di Ping 192.168.50.100 con 32 byte di dati:
Risposta da 192.168.50.100: byte=32 durata=8ms TTL=64
Risposta da 192.168.50.100: byte=32 durata=2ms TTL=64
Risposta da 192.168.50.100: byte=32 durata=2ms TTL=64
Risposta da 192.168.50.100: byte=32 durata=2ms TTL=64

Statistiche Ping per 192.168.50.100:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
    Tempo approssimativo percorsi andata/ritorno in millisecondi:
        Minimo = 2ms, Massimo = 8ms, Medio = 3ms

C:\Users\Davide>
```

- Ping da **Windows 7** a **Metasploitable**



```
C:\Windows\system32\cmd.exe

C:\Users\Davide>ping 192.168.50.101

Esecuzione di Ping 192.168.50.101 con 32 byte di dati:
Risposta da 192.168.50.101: byte=32 durata=5ms TTL=64
Risposta da 192.168.50.101: byte=32 durata=3ms TTL=64
Risposta da 192.168.50.101: byte=32 durata=5ms TTL=64
Risposta da 192.168.50.101: byte=32 durata=1ms TTL=64

Statistiche Ping per 192.168.50.101:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
    Tempo approssimativo percorsi andata/ritorno in millisecondi:
        Minimo = 1ms, Massimo = 5ms, Medio = 3ms

C:\Users\Davide>
```

Davide Mirani