

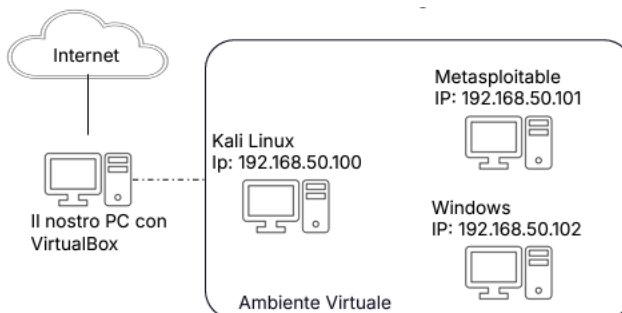
CSPT0524IT – W2D4 - PRATICA

Report di Svolgimento dell'Esercizio Pratico + Esercizio Facoltativo

Traccia:

Si richiede allo studente di creare un laboratorio virtuale, con le seguenti caratteristiche:

- Installazione e configurazione di Metasploitable
- Installazione e configurazione di Windows 10
- La macchine virtuali devono essere in grado di comunicare tra di loro su rete interna (evidenze ping tra la macchine)
- Il sistema host non deve comunicare con l'ambiente virtuale



In questo esercizio ho utilizzato Virtual Box per creare e configurare quattro Virtual Machine: **Kali-Linux**, **Metaploitable-Win10**, **Metasploitable-Linux** e **Windows7**; ho impostato la scheda di rete di tutte le vm su rete interna e assegnato un ip statico ad ognuna per poi metterle in comunicazione.

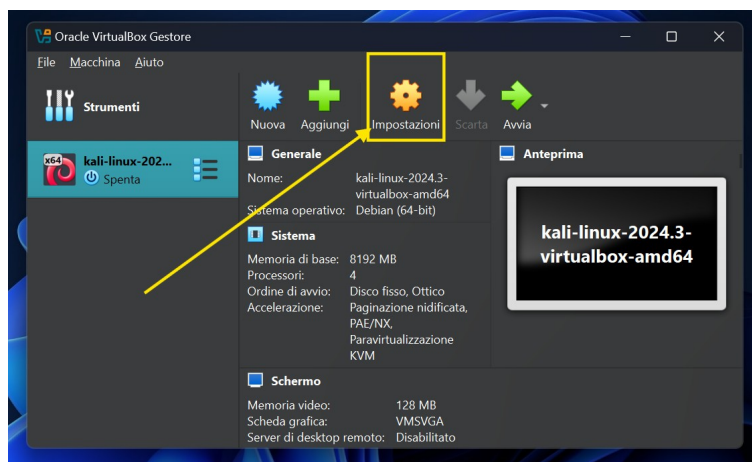
Reti Assegnate: Rete Interna

IP Assegnati: - Kali-linux	192.168.50.100
- Metasploitable-Win10	192.168.50.101
- Metasploitable-Linux	192.168.50.102
- Windows 7	192.168.50.103

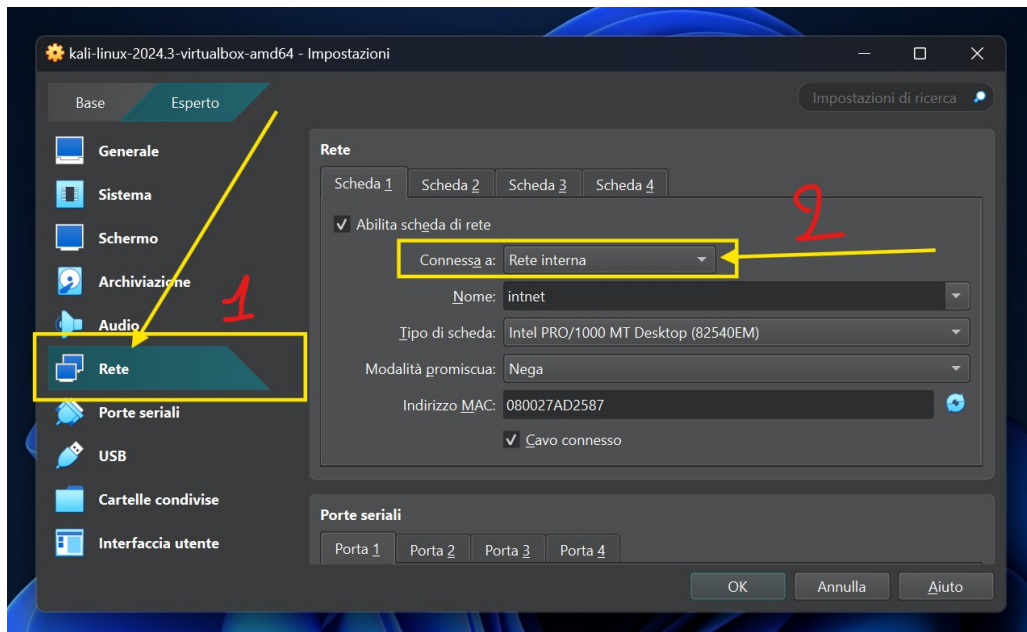
1. Kali-Linux

Impostare “Rete Interna” sulla scheda di rete di Kali-Linux

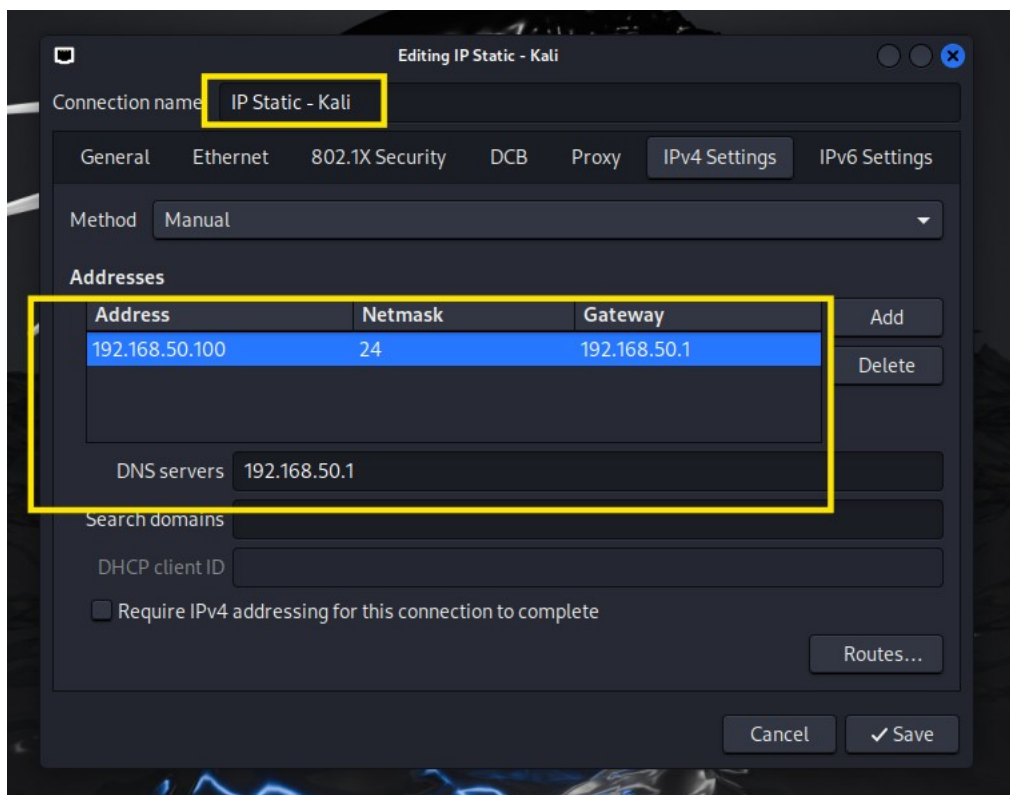
- Ho selezionato la macchina Kali dal menù verticale e premuto su impostazioni.



- Nella zona di Rete, ho impostato la scheda 1 su Rete intera.



- Ho aperto Advanced Network Configuration e ho impostato la seguente configurazione:
Address: 192.168.50.100
Netmask: 24
Gateway: 192.168.50.1
DNS Server: 192.168.50.1 (Preparazione per Pfsense)



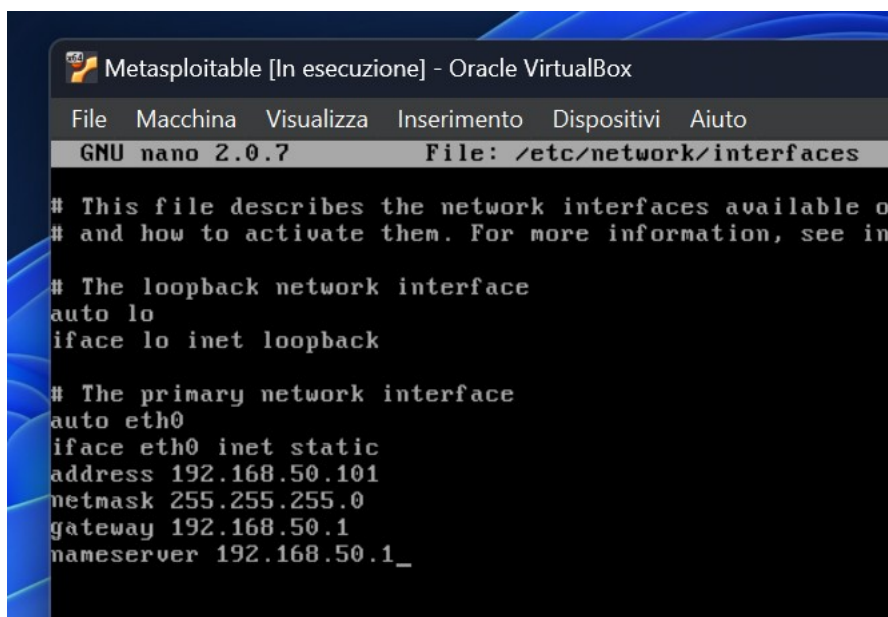
- Ho utilizzato il comando “ip a” per controllare l’indirizzo ip.

```
(kali@kali)-[~]  
$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host noprefixroute  
        valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 08:00:27:ad:25:87 brd ff:ff:ff:ff:ff:ff  
    inet 192.168.50.100/24 brd 192.168.50.255 scope global noprefixroute eth0  
        valid_lft forever preferred_lft forever  
    inet6 fe80::14dc:fbc3:35a0:6265/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever
```

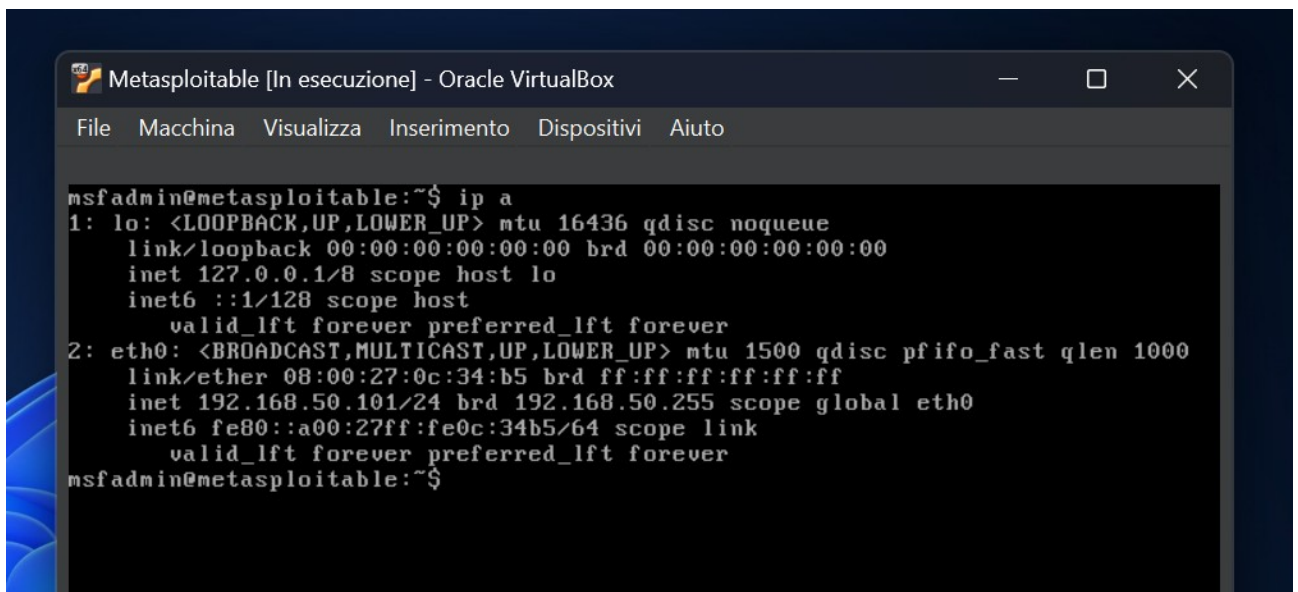
2. Metasploitable – Linux

- Dopo aver impostato la scheda di rete su “Rete Interna” ho acceso la VM e, con nano ho editato il file “/etc/network/interfaces” aggiungendo le configurazioni seguenti:

```
iface eth0 inet static  
address 192.168.50.101  
netmask 255.255.255.0  
gateway 192.168.50.1  
nameserver 192.168.50.1
```



- Infine ho riavviato il network service con il comando “sudo /etc/init.d/networking restart” e successivamente ho chiamato “ip a” per controllare l’ip assegnato

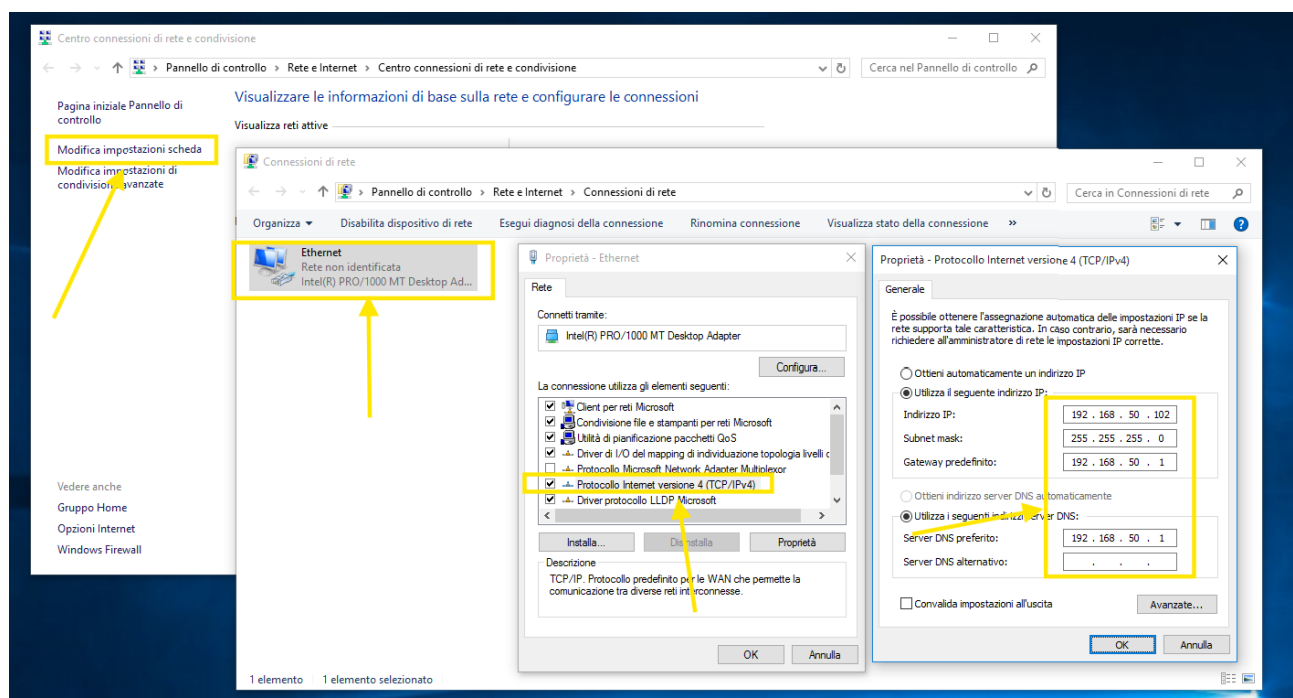


```
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:0c:34:b5 brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.101/24 brd 192.168.50.255 scope global eth0
    inet6 fe80::a00:27ff:fe0c:34b5/64 scope link
        valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
```

3. Metasploitable – WIN10

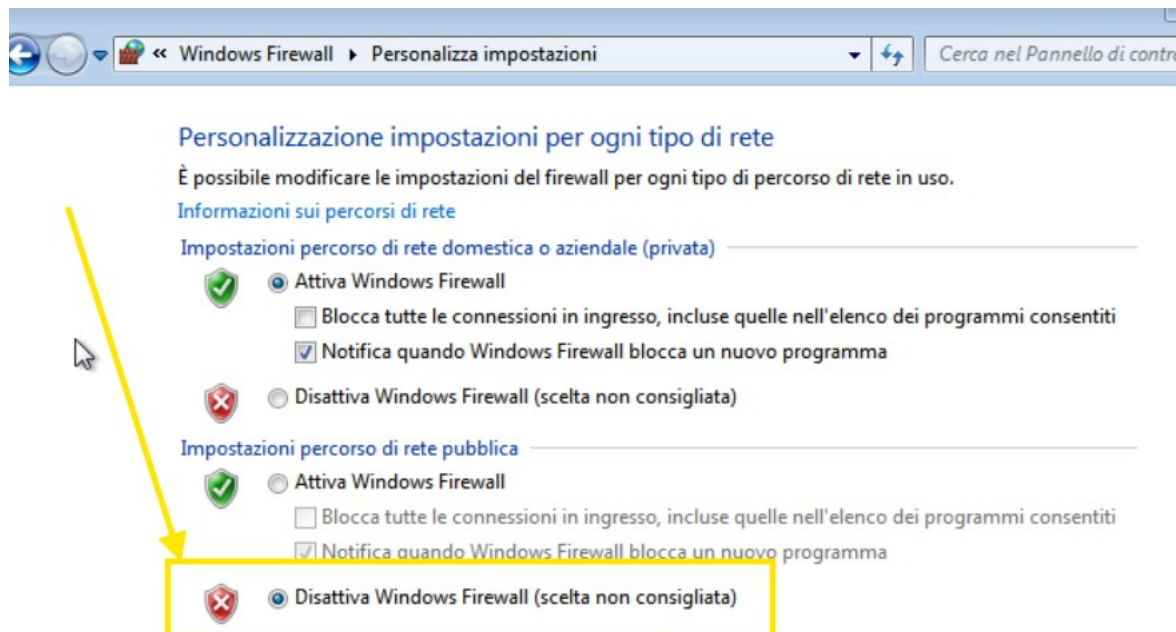
- Dopo aver impostato la scheda di rete su “Rete Interna” ho acceso la VM e mi sono recato nel “Centro connessioni di rete” poi “Modifica impostazioni scheda”, poi ho aperto le proprietà della scheda di rete “Ethernet” e nella sezione “TCP/IP” ho impostato la configurazione che segue:

Indirizzo IP: 192.168.50.102
Subnet mask: 255.255.255.0
Gateway predefinito: 192.168.50.1
Server DNS preferito: 192.168.50.1



4. Windows 7

- Dopo aver impostato la scheda di rete su “Rete Interna” ho acceso la VM e ho disabilitato il firewall di rete pubblica per consentire di essere raggiunto dalle altre macchine in rete.



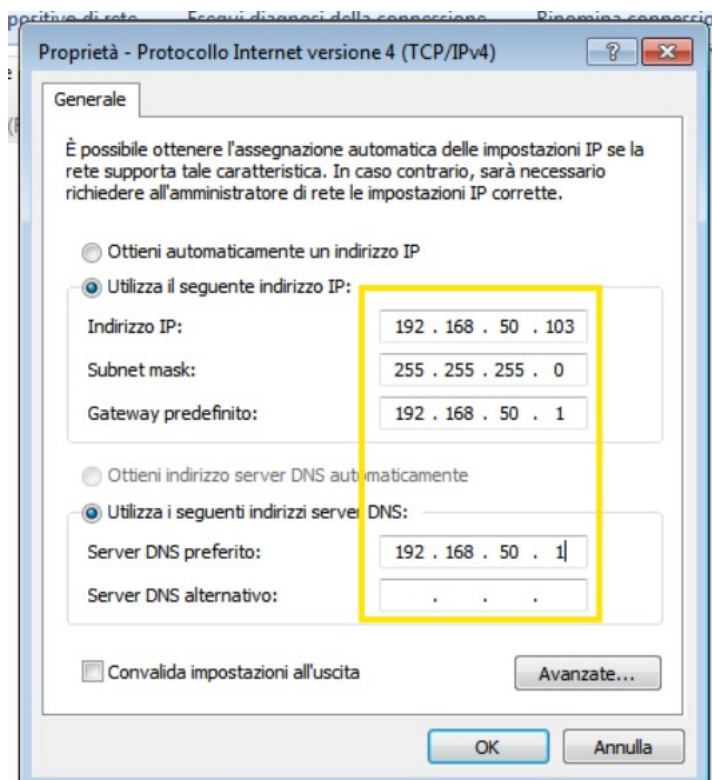
- Mi sono recato nel “Centro connessioni di rete” poi “Modifica impostazioni scheda”, poi ho aperto le proprietà della scheda di rete “Ethernet” e nella sezione “TCP/IP” ho impostato la configurazione che segue:

Indirizzo IP: 192.168.50.103

Subnet mask: 255.255.255.0

Gateway predefinito: 192.168.50.1

Server DNS preferito: 192.168.50.1



5. Test dei PING

Kali-Linux 192.168.50.100 ↔ 192.168.50.101 Metasploitable-Linux

The image shows two terminal windows side-by-side. The left window is a Kali-Linux terminal with the command `ping 192.168.50.101` executed. The output shows 9 successful pings with 0% packet loss. The right window is a Metasploitable-Linux terminal with the command `ping 192.168.50.100` executed. The output shows 7 successful pings with 0% packet loss. Yellow arrows point from the IP addresses in the text above to the corresponding IP addresses in the terminal commands.

```
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=3.26 ms
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=2.92 ms
64 bytes from 192.168.50.101: icmp_seq=3 ttl=64 time=2.75 ms
64 bytes from 192.168.50.101: icmp_seq=4 ttl=64 time=1.91 ms
64 bytes from 192.168.50.101: icmp_seq=5 ttl=64 time=2.26 ms
64 bytes from 192.168.50.101: icmp_seq=6 ttl=64 time=1.78 ms
64 bytes from 192.168.50.101: icmp_seq=7 ttl=64 time=3.16 ms
64 bytes from 192.168.50.101: icmp_seq=8 ttl=64 time=1.88 ms
64 bytes from 192.168.50.101: icmp_seq=9 ttl=64 time=1.88 ms
^C
--- 192.168.50.101 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8036
```

```
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=1.97 ms
64 bytes from 192.168.50.100: icmp_seq=2 ttl=64 time=1.67 ms
64 bytes from 192.168.50.100: icmp_seq=3 ttl=64 time=1.43 ms
64 bytes from 192.168.50.100: icmp_seq=4 ttl=64 time=1.97 ms
64 bytes from 192.168.50.100: icmp_seq=5 ttl=64 time=1.33 ms
64 bytes from 192.168.50.100: icmp_seq=6 ttl=64 time=1.35 ms
64 bytes from 192.168.50.100: icmp_seq=7 ttl=64 time=1.86 ms
^C
--- 192.168.50.100 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6001ms
rtt min/avg/max/mdev = 1.335/1.657/1.972/0.267 ms
msfadmin@metasploitable:~$
```

Kali-Linux 192.168.50.100 ↔ 192.168.50.102 Metasploitable-Win10

The image shows two terminal windows side-by-side. The left window is a Kali-Linux terminal with the command `ping 192.168.50.102` executed. The output shows 6 successful pings with 0% packet loss. The right window is a Windows 7 terminal with the command `ping 192.168.50.100` executed. The output shows 4 successful pings with 0% packet loss. Yellow arrows point from the IP addresses in the text above to the corresponding IP addresses in the terminal commands.

```
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=1.74 ms
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=1.56 ms
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=1.46 ms
64 bytes from 192.168.50.102: icmp_seq=4 ttl=128 time=1.28 ms
64 bytes from 192.168.50.102: icmp_seq=5 ttl=128 time=1.34 ms
64 bytes from 192.168.50.102: icmp_seq=6 ttl=128 time=1.22 ms
^C
--- 192.168.50.102 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5179ms
rtt min/avg/max/mdev = 1.221/1.430/1.735/0.175 ms
```

```
C:\Users\Francesco>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=3ms TTL=64
Risposta da 192.168.50.100: byte=32 durata=1ms TTL=64
Risposta da 192.168.50.100: byte=32 durata=7ms TTL=64
Risposta da 192.168.50.100: byte=32 durata=1ms 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 = 1ms, Massimo = 7ms, Medio = 3ms
```

Kali-Linux 192.168.50.100 ↔ 192.168.50.103 Windows7

The image shows two terminal windows side-by-side. The left window is a Kali-Linux terminal with the command `ping 192.168.50.102` executed. The output shows 6 successful pings with 0% packet loss. The right window is a Windows 10 terminal with the command `ping 192.168.50.100` executed. The output shows 4 successful pings with 0% packet loss. Yellow arrows point from the IP addresses in the text above to the corresponding IP addresses in the terminal commands.

```
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=1.14 ms
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=1.48 ms
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=1.16 ms
64 bytes from 192.168.50.102: icmp_seq=4 ttl=128 time=1.17 ms
64 bytes from 192.168.50.102: icmp_seq=5 ttl=128 time=1.47 ms
64 bytes from 192.168.50.102: icmp_seq=6 ttl=128 time=1.75 ms
^C
--- 192.168.50.102 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5013ms
rtt min/avg/max/mdev = 1.140/1.361/1.750/0.225 ms
```

```
C:\Users\user>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=14ms TTL=64
Risposta da 192.168.50.100: byte=32 durata=1ms TTL=64
Risposta da 192.168.50.100: byte=32 durata=1ms TTL=64
Risposta da 192.168.50.100: byte=32 durata=1ms TTL=64

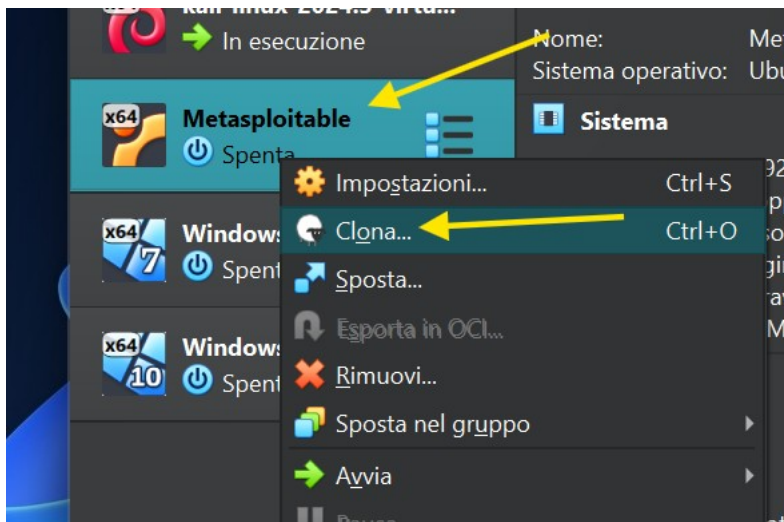
Statistiche Ping per 192.168.50.100:
Pacchetti: Trasmessi = 4, Ricevuti = 4,
Persi = 0 (0% persi),
Tempo approssimativo percorsi andata/ritorno in millisecondi:
Minimo = 1ms, Massimo = 14ms, Medio = 4ms
```

6. Esercizio Facoltativo

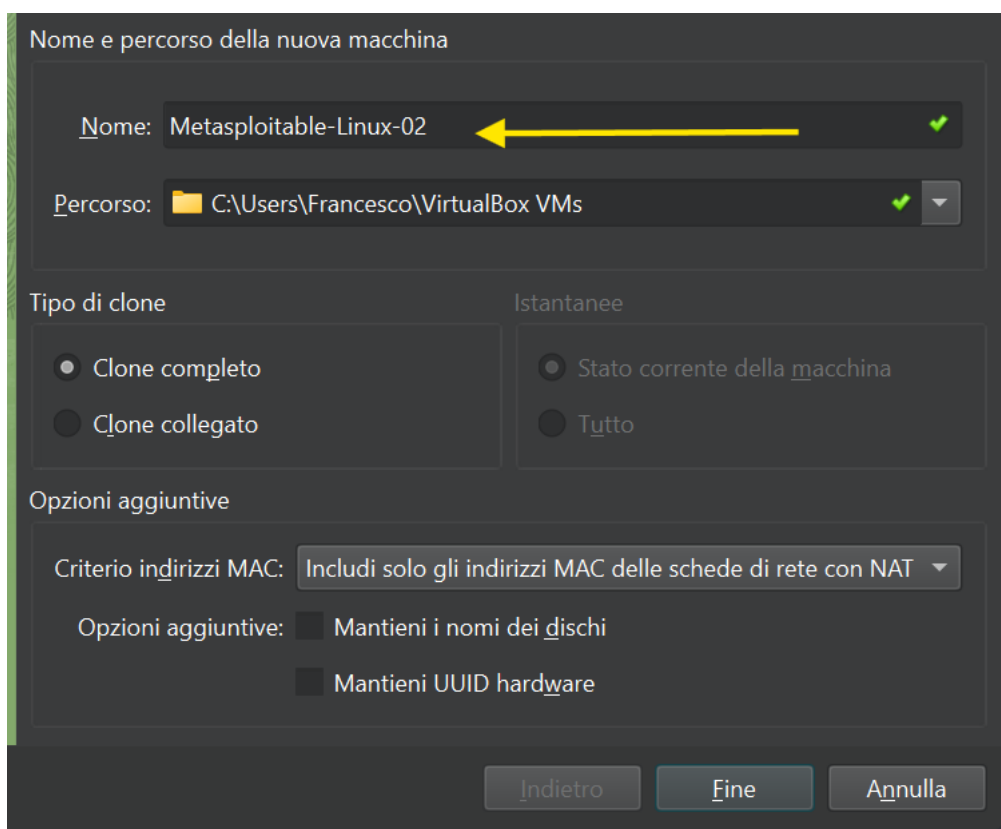
Traccia:

Si richiede di creare una versione di recovery di una delle macchine appena create, come ad esempio l'opzione Clona. Clonare dunque una macchina a piacere, rinominandola in modo opportuno, e verificarne il corretto funzionamento.

- Ho premuto il tasto destro del mouse sulla macchina da clonare e premuto su "clone".



- Ho modificato il nome della macchina e premuto su fine.



- Ho acceso la macchina clone e assegnato IP statico 192.168.50.104

```
Metasploitable-Linux-02 [In esecuzione] - Ora
File  Macchina  Visualizza  Inserimento  Dis
GNU nano 2.0.7  File: /etc/

# This file describes the network in
# and how to activate them. For more

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.50.104
netmask 255.255.255.0
gateway 192.168.50.1
nameserver 192.168.50.1
```

- Ho riavviato il servizio di rete con “sudo /etc/init.d/networking restart” e ho utilizzato “ip a” per controllare la configurazione.

```
Metasploitable-Linux-02 [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16384 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:4a:54:d1 brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.104/24 brd 192.168.50.255 scope global eth0
    inet6 fe80::a00:27ff:fe4a:54d1/64 scope link
        valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ _
```

- Infine ho effettuato il ping da Kali a Metasploitable Clone e viceversa.

```
kali-linux-2024.3-virtualbox-amd64 [In esecuzione] - Ora...
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

(kali@kali)~$ ping 192.168.50.104
PING 192.168.50.104 (192.168.50.104) 56(84) bytes of data:
64 bytes from 192.168.50.104: icmp_seq=1 ttl=64 time=6.06 ms
64 bytes from 192.168.50.104: icmp_seq=2 ttl=64 time=1.82 ms
64 bytes from 192.168.50.104: icmp_seq=3 ttl=64 time=1.43 ms
64 bytes from 192.168.50.104: icmp_seq=4 ttl=64 time=1.30 ms
64 bytes from 192.168.50.104: icmp_seq=5 ttl=64 time=1.59 ms
64 bytes from 192.168.50.104: icmp_seq=6 ttl=64 time=1.67 ms
^C
--- 192.168.50.104 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5084ms
rtt min/avg/max/mdev = 1.295/2.310/6.055/1.682 ms

Metasploitable-Linux-02 [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

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=1.54 ms
64 bytes from 192.168.50.100: icmp_seq=2 ttl=64 time=1.61 ms
64 bytes from 192.168.50.100: icmp_seq=3 ttl=64 time=1.70 ms
64 bytes from 192.168.50.100: icmp_seq=4 ttl=64 time=1.30 ms
64 bytes from 192.168.50.100: icmp_seq=5 ttl=64 time=1.74 ms
64 bytes from 192.168.50.100: icmp_seq=6 ttl=64 time=1.74 ms
--- 192.168.50.100 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 4996ms
rtt min/avg/max/mdev = 0.756/1.446/1.749/0.341 ms
msfadmin@metasploitable:~$
```