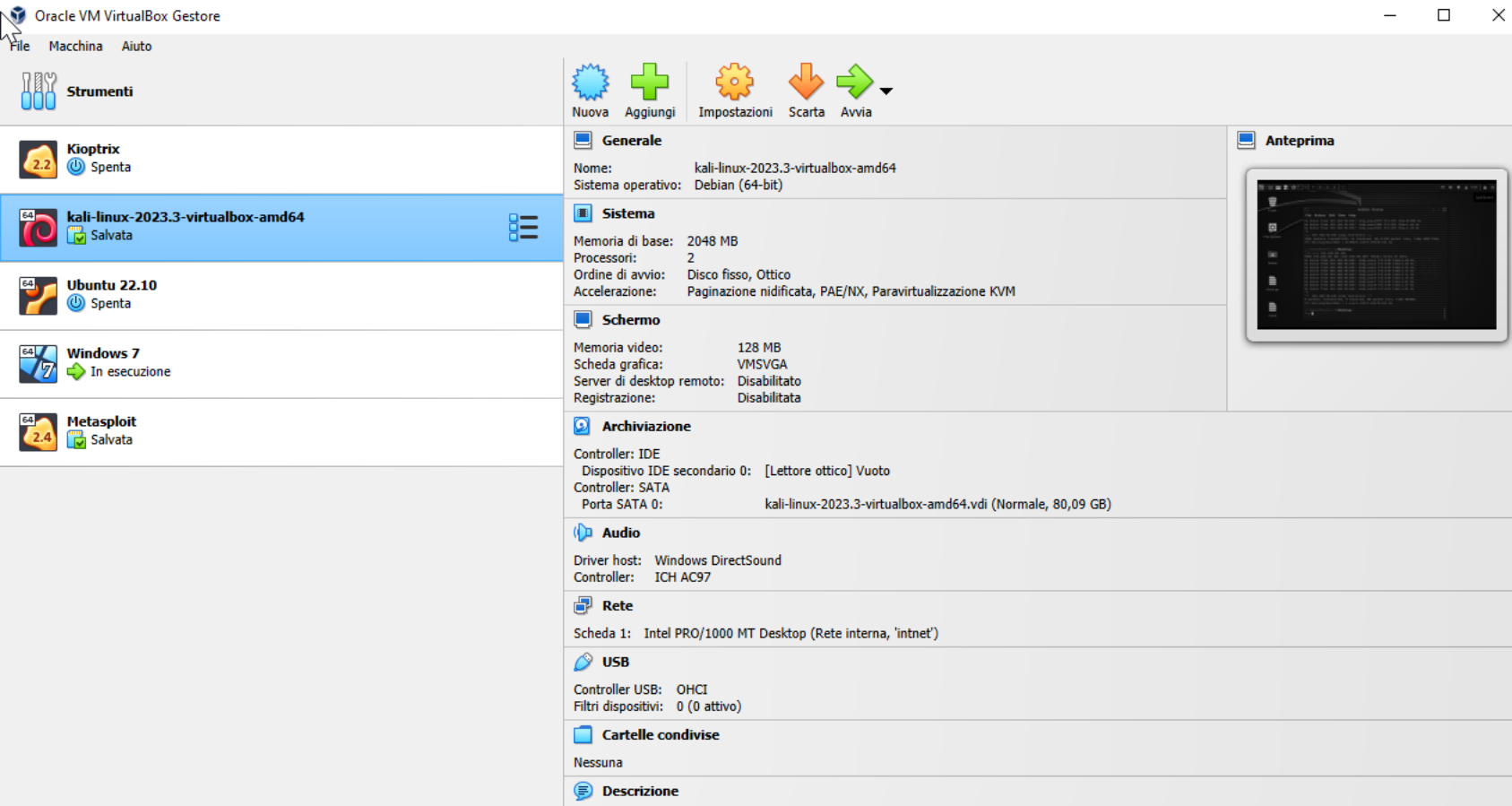


Esercitazione laboratorio virtuale

VERIFICARE LA COMUNICAZIONE TRA MACCHINA VIRTUALE ATTACCANTE ED
ALTRE 2 VM IN UNA RETE «INTERNA»

Macchine virtuali utilizzate



La macchina host ha come sistema operativo windows 10, su questa ho installato Virtual Box come virtualizzatore.

Su di esso ho creato 3 macchine virtuali con 3 SO diversi, il primo è kali linux che sarà il nostro sistema attaccante, le altre due sono le macchine da attaccare con Windows 7 e Metaesplot 2 come SO.

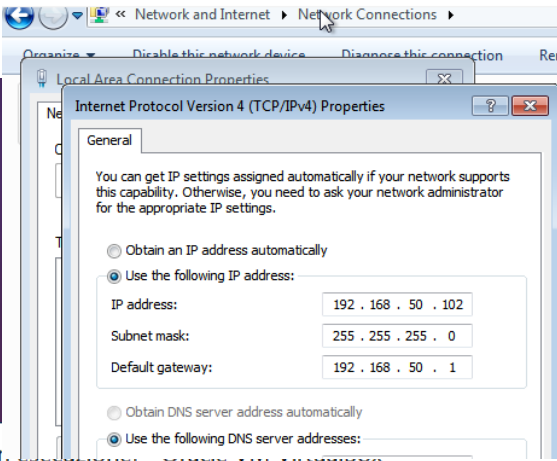
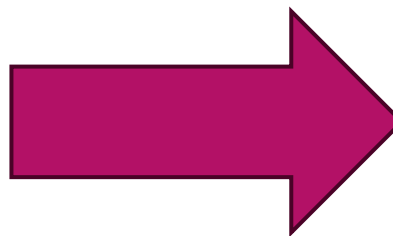
L'obiettivo dell'esercizio è semplicemente di fare in modo che la macchina con Kali riesca a comunicare con le altre due su una rete interna di cui fanno parte solo tutte e 3.

Attribuzione ip statici alle 3 VM

In base alle indicazioni fornite ho attribuito un determinato indirizzo ip a ognuna delle VM create.

Durante il laboratorio, utilizzeremo un indirizzamento statico delle nostre macchine. Ovvero, tutte le macchine all'accensione, riceveranno l'ip assegnato in tabella

Macchina Virtuale	Indirizzo IP
Kali Linux	192.168.50.100
Metasploitable	192.168.50.101
Windows 7	192.168.50.102



File Macchina Visualizza Inserimento Dispositivi Aiuto

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:57:bc:68
          inet addr:192.168.50.101  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe57:bc68/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:768 errors:0 dropped:0 overruns:0 frame:0
          TX packets:144 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:55396 (54.0 KB)  TX bytes:13114 (12.8 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:218 errors:0 dropped:0 overruns:0 frame:0
          TX packets:218 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:68061 (66.4 KB)  TX bytes:68061 (66.4 KB)
```

```
(kali@kali)-[~/Desktop]
$ 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:fe57:bc68/64  prefixlen 64  scopeid 0x20<link>
      ether 08:00:27:57:bc:68  txqueuelen 1000  (Ethernet)
      RX packets 532  bytes 46764 (45.6 KiB)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 4299  bytes 361164 (352.6 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 0x10<host>
      loop txqueuelen 1000  (Local Loopback)
      RX packets 4  bytes 240 (240.0 B)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 4  bytes 240 (240.0 B)
      TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
```

Da Kali riesco a comunicare con le altre 2 VM?

File Macchina Visualizza Inserimento Dispositivi Aiuto

```
kali@kali: ~/Desktop
File Actions Edit View Help
ether 08:00:27:cb:7e:f5 txqueuelen 1000 (Ethernet)
RX packets 532 bytes 46764 (45.6 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 4299 bytes 361164 (352.6 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 4 bytes 240 (240.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 4 bytes 240 (240.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali@kali)-[~/Desktop]
$ 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=1.94 ms
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=1.84 ms
64 bytes from 192.168.50.101: icmp_seq=3 ttl=64 time=1.80 ms
64 bytes from 192.168.50.101: icmp_seq=4 ttl=64 time=16.9 ms
^C
--- 192.168.50.101 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 1.799/5.616/16.886/6.506 ms

(kali@kali)-[~/Desktop]
$ 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=3.31 ms
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=1.27 ms
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=1.14 ms
64 bytes from 192.168.50.102: icmp_seq=4 ttl=128 time=0.796 ms
^C
--- 192.168.50.102 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3011ms
rtt min/avg/max/mdev = 0.796/1.628/3.308/0.985 ms

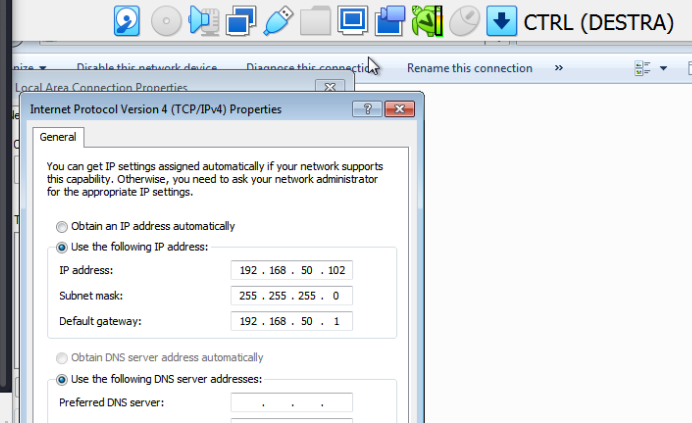
(kali@kali)-[~/Desktop]
$
```

```
Metasploit [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

admin@metasploitable:~$ ifconfig
eth0:
Link encap:Ethernet HWaddr 08:00:27:57:bc:68
inet addr:192.168.50.101 Bcast:192.168.50.255 Mask:255.255.255.0
inet6 addr: fe80::a00:27ff:fe57:bc68/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:768 errors:0 dropped:0 overruns:0 frame:0
TX packets:144 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:55396 (54.0 KB) TX bytes:13114 (12.8 KB)
Base address:0xd020 Memory:f0200000-f0220000

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:218 errors:0 dropped:0 overruns:0 frame:0
TX packets:218 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:68061 (66.4 KB) TX bytes:68061 (66.4 KB)

admin@metasploitable:~$
```



A sinistra abbiamo Kali e a destra windows7 e Metasploit2. Come possiamo notare nella configurazione tutte e 3 hanno come gateway 192.168.50.1 che permetterà ai pc di comunicare tra loro. Avendo settato gli ip statici in precedenza ho verificato col comando ping la raggiungibilità delle due macchine e non essendoci pacchetti persi ed essendoci le risposte da parte delle 2 macchine vuol dire che c'è comunicazione.

```

C:\Users\royve>arp -a

Interfaccia: 192.168.56.1 --- 0x4
Indirizzo Internet  Indirizzo fisico  Tipo
192.168.56.255      ff-ff-ff-ff-ff-ff  statico
224.0.0.2           01-00-5e-00-00-02  statico
224.0.0.22          01-00-5e-00-00-16  statico
224.0.0.251         01-00-5e-00-00-fb  statico
224.0.0.252         01-00-5e-00-00-fc  statico
239.192.152.143     01-00-5e-40-98-8f  statico
239.255.255.250     01-00-5e-7f-ff-fa  statico
255.255.255.255     ff-ff-ff-ff-ff-ff  statico

Interfaccia: 192.168.11.1 --- 0x5
Indirizzo Internet  Indirizzo fisico  Tipo
192.168.11.254      00-50-56-fb-d2-e9  dinamico
192.168.11.255      ff-ff-ff-ff-ff-ff  statico
224.0.0.2           01-00-5e-00-00-02  statico
224.0.0.22          01-00-5e-00-00-16  statico
224.0.0.251         01-00-5e-00-00-fb  statico
224.0.0.252         01-00-5e-00-00-fc  statico
239.192.152.143     01-00-5e-40-98-8f  statico
239.255.255.250     01-00-5e-7f-ff-fa  statico
255.255.255.255     ff-ff-ff-ff-ff-ff  statico

Interfaccia: 192.168.1.7 --- 0x9
Indirizzo Internet  Indirizzo fisico  Tipo
192.168.1.1         14-2e-5e-50-31-e2  dinamico
192.168.1.9         b8-8a-60-b4-af-32  dinamico
192.168.1.255       ff-ff-ff-ff-ff-ff  statico
224.0.0.22          01-00-5e-00-00-16  statico
224.0.0.251         01-00-5e-00-00-fb  statico
224.0.0.252         01-00-5e-00-00-fc  statico
239.255.255.250     01-00-5e-7f-ff-fa  statico
255.255.255.255     ff-ff-ff-ff-ff-ff  statico

Interfaccia: 192.168.40.1 --- 0x13
Indirizzo Internet  Indirizzo fisico  Tipo
192.168.40.254      00-50-56-fe-08-25  dinamico
192.168.40.255      ff-ff-ff-ff-ff-ff  statico
224.0.0.2           01-00-5e-00-00-02  statico
224.0.0.22          01-00-5e-00-00-16  statico
224.0.0.251         01-00-5e-00-00-fb  statico
224.0.0.252         01-00-5e-00-00-fc  statico
239.192.152.143     01-00-5e-40-98-8f  statico
239.255.255.250     01-00-5e-7f-ff-fa  statico
255.255.255.255     ff-ff-ff-ff-ff-ff  statico

C:\Users\royve>

```

```

C:\Users\royve>arp -a

Microsoft Windows [Versione 10.0.19045.3570]
(c) Microsoft Corporation. Tutti i diritti sono riservati.

C:\Users\royve>ping 192.168.50.102

Esecuzione di Ping 192.168.50.102 con 32 byte di dati:
Richiesta scaduta.
Richiesta scaduta.
Richiesta scaduta.
Richiesta scaduta.

Statistiche Ping per 192.168.50.102:
    Pacchetti: Trasmessi = 4, Ricevuti = 0,
    Persi = 4 (100% persi),

C:\Users\royve>ping 192.168.50.101

Esecuzione di Ping 192.168.50.101 con 32 byte di dati:
Richiesta scaduta.
Richiesta scaduta.
Richiesta scaduta.
Richiesta scaduta.

Statistiche Ping per 192.168.50.101:
    Pacchetti: Trasmessi = 4, Ricevuti = 0,
    Persi = 4 (100% persi),

C:\Users\royve>

```

In ultimo dovevamo verificare l'impossibilità di connetterci con la macchina host alla rete interna creata per e con le VM. Quindi ho usato prima il protocollo arp per vedere i dispositivi nella lan e nessuna delle VM è stata visualizzata, più specificamente ho provato anche ad effettuare il ping delle 2 VM dal prompt dei comandi ottenendo solo richieste scadute e quindi l'irraggiungibilità di queste VM.