W1D4 – CREAZIONE E CONFIGURAZIONE DEL LABORATORIO VIRTUALE (Alessio Russo)

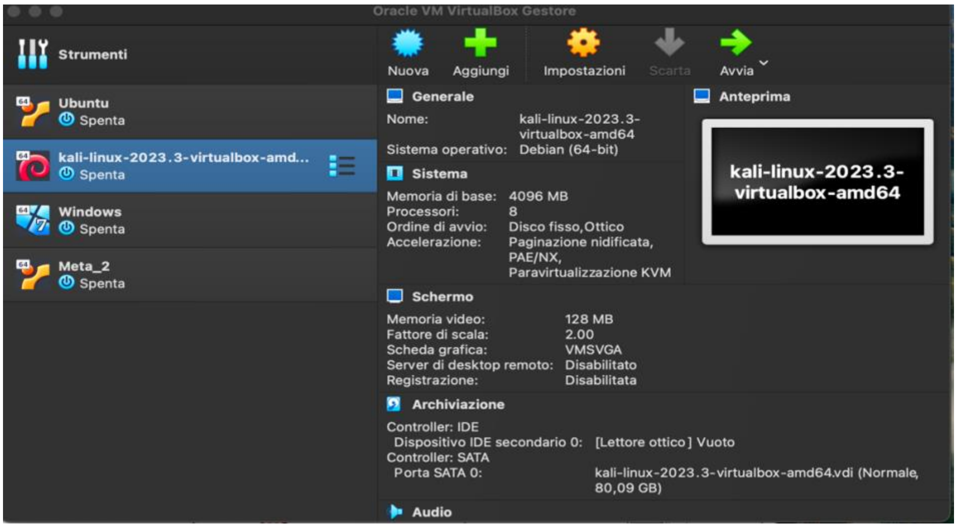
Veniva richiesto di:

- Installare **VirtualBox**;
- Installare e configurare **Kali Linux**, **Metasploitable** e **Windows 7**;
- Le macchine installate devono comunicare tra loro su rete interna (Evidenza **ping** tra macchine);
- Il sistema **host** non deve comunicare con l'ambiente virtuale.

INSTALLAZIONE DI KALI LINUX, METASPLOITABLE 2 E WINDOWS 7

Installazione effettuata tenendo conto dei requisiti di sistema della macchina utilizzata per creare l'ambiente virtuale in modo da bilanciare le prestazioni tra le macchine virtuali e il sistema operativo host. Nello specifico ho assegnato:

- **Kali Linux**: 4 Gb di RAM (di 16 Gb Totali), 8 core CPU (di 16 totali);


Oracle VM VirtualBox Gestore
Strumenti
Nuova
Aggiungi
Impostazioni
Scarta
Avvia
Ubuntu
Spenta
kali-linux-2023.3-virtualbox-amd...
Spenta
Windows
Spenta
Meta_2
Spenta
Anteprima
kali-linux-2023.3-virtualbox-amd64

Generale

Nome: kali-linux-2023.3-virtualbox-amd64
Sistema operativo: Debian (64-bit)

Sistema

Memoria di base: 4096 MB
Processori: 8
Ordine di avvio: Disco fisso,Ottico
Accelerazione: Paginazione nidificata, PAE/NX, Paravirtualizzazione KVM

Schermo

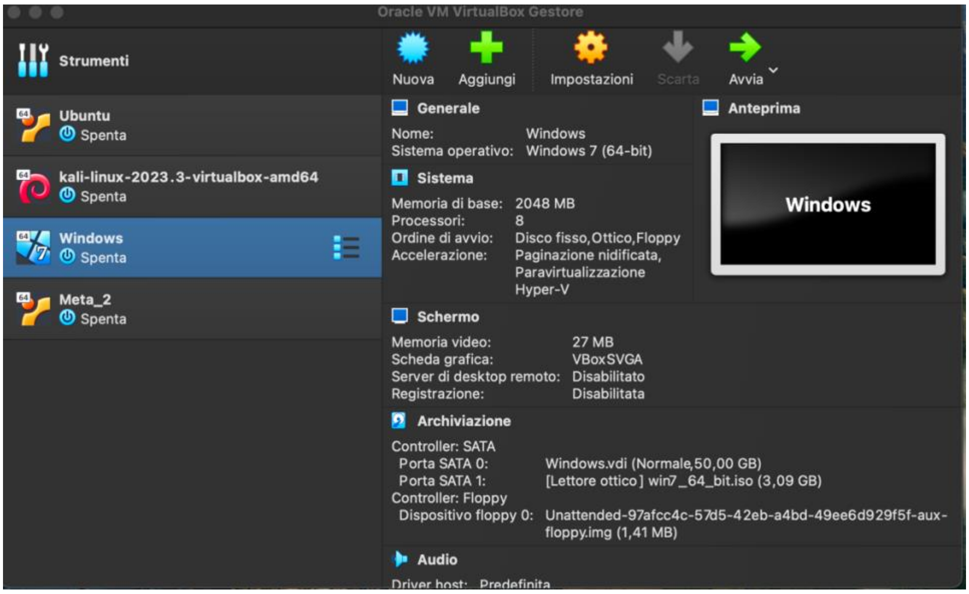
Memoria video: 128 MB
Fattore di scala: 2.00
Scheda grafica: VMSVGA
Server di desktop remoto: Disabilitato
Registrazione: Disabilitata

Archiviazione

Controller: IDE
Dispositivo IDE secondario 0: [Lettore ottico] Vuoto
Controller: SATA
Porta SATA 0: kali-linux-2023.3-virtualbox-amd64.vdi (Normale, 80,09 GB)

Audio

- **Windows 7**: 2 Gb RAM (di 16 Gb Totali), 8 core CPU (di 16 totali);



Generale

Nome: Windows
Sistema operativo: Windows 7 (64-bit)

Sistema

Memoria di base: 2048 MB
Processori: 8
Ordine di avvio: Disco fisso,Ottico,Floppy
Accelerazione: Paginazione nidificata, Paravirtualizzazione Hyper-V

Schermo

Memoria video: 27 MB
Scheda grafica: VBoxSVGA
Server di desktop remoto: Disabilitato
Registrazione: Disabilitata

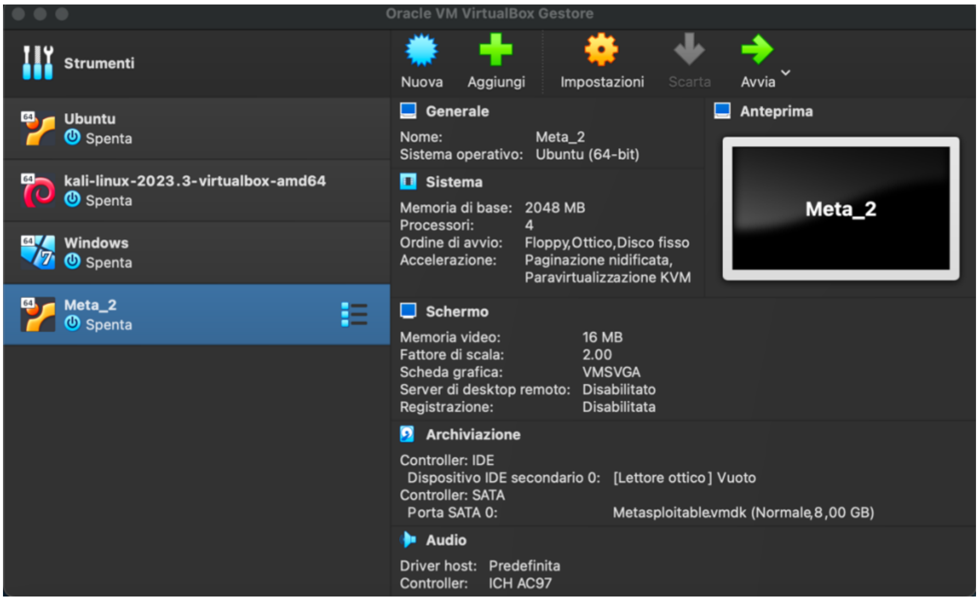
Archiviazione

Controller: SATA
Porta SATA 0: Windows.vdi (Normale,50,00 GB)
Porta SATA 1: [Lettore ottico] win7_64_bit.iso (3,09 GB)
Controller: Floppy
Dispositivo floppy 0: Unattended-97afcc4c-57d5-42eb-a4bd-49ee6d929f5f-aux-floppy.img (1,41 MB)

Audio

Driver host: Predefinita

- **Metasploitable 2**: 2 Gb RAM (di 16 totali), 4 core CPU (di 16 totali);



Generale

Nome: Meta_2
Sistema operativo: Ubuntu (64-bit)

Sistema

Memoria di base: 2048 MB
Processori: 4
Ordine di avvio: Floppy,Ottico,Disco fisso
Accelerazione: Paginazione nidificata, Paravirtualizzazione KVM

Schermo

Memoria video: 16 MB
Fattore di scala: 2.00
Scheda grafica: VMSVGA
Server di desktop remoto: Disabilitato
Registrazione: Disabilitata

Archiviazione

Controller: IDE
Dispositivo IDE secondario 0: [Lettore ottico] Vuoto
Controller: SATA
Porta SATA 0: Metasploitable.vmdk (Normale,8,00 GB)

Audio

Driver host: Predefinita
Controller: ICH AC97

DETERMINAZIONE DI IP STATICO E COMUNICAZIONE TRA LE MACCHINE VIRTUALI

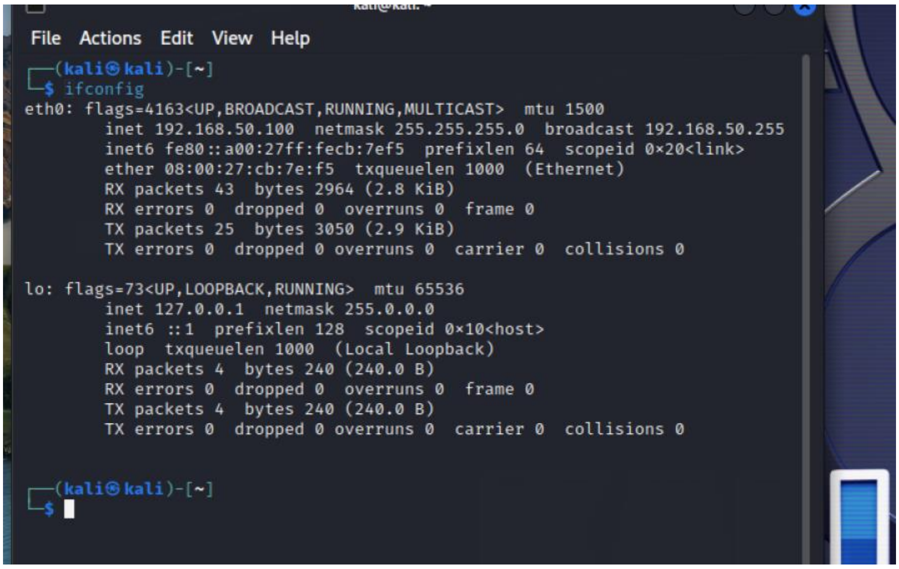
1. KALI LINUX:

la determinazione dell'ip statico è avvenuta attraverso i comandi: sudo nano /etc/network/interfaces determinando:

inet 192.168.50.100 (indirizzo IP static)

netmask: 255.255.255.0

broadcast 192.168.50.255

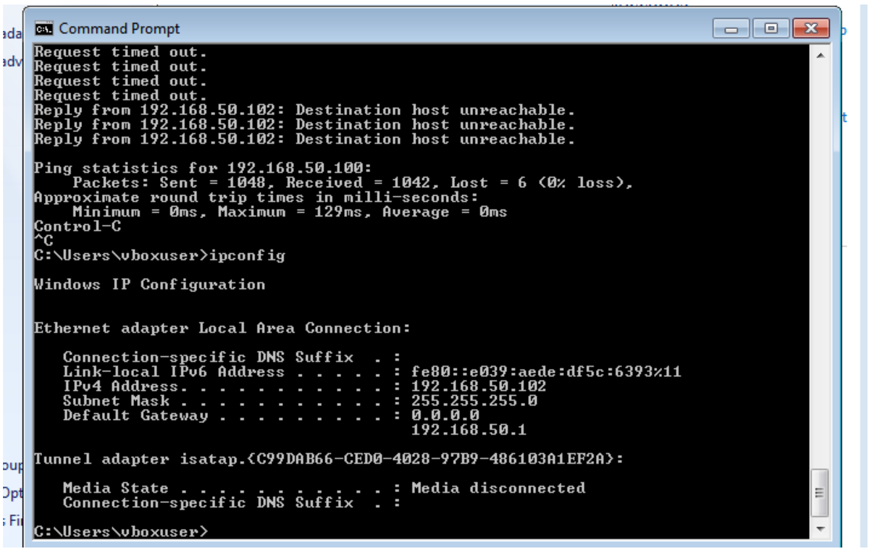


```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.50.100  netmask 255.255.255.0  broadcast 192.168.50.255
        inet6 fe80::a00:27ff:fecb:7ef5  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:cb:7e:f5  txqueuelen 1000  (Ethernet)
        RX packets 43  bytes 2964 (2.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 25  bytes 3050 (2.9 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


┌──(kali㉿kali)-[~]
└─$ ▌
```

2. Windows 7:

La determinazione dell’IP statico è avvenuta attraverso le impostazioni di rete nello specifico sono andato a modificare manualmente le voci di indirizzo di rete cliccando su proprietà delle stesse, determinando:

- IP-statico: 192.168.50.102;
- Netmask: 255.255.255.0;

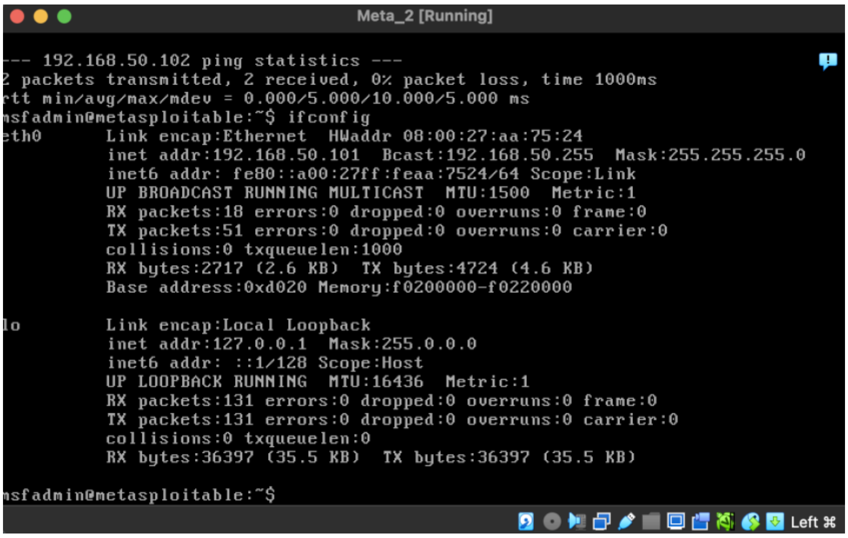


```
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.50.102: Destination host unreachable.
Reply from 192.168.50.102: Destination host unreachable.
Reply from 192.168.50.102: Destination host unreachable.

Ping statistics for 192.168.50.100:
    Packets: Sent = 1048, Received = 1042, Lost = 6 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 129ms, Average = 0ms
Control-C
^C
C:\Users\vboxuser>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::e039:aede:df5c:6393%11
   IPv4 Address. . . . . . . . . . . : 192.168.50.102
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 0.0.0.0
                                       192.168.50.1

Tunnel adapter isatap.{C99DAB66-CED0-4028-97B9-486103A1EF2A}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\vboxuser>
```

3. METASPLOITABLE 2

la determinazione dell’ip statico è avvenuta attraverso i comandi: sudo nano /etc/network/interfaces determinando:

- inet 192.168.50.101 (indirizzo IP statico);
- mask: 255.255.255.0;
- broadcast 192.168.50.255;



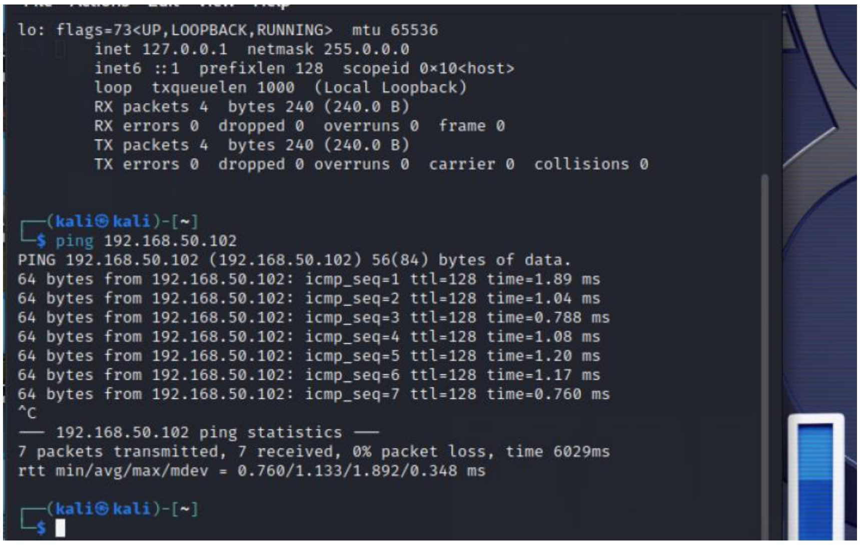
```
--- 192.168.50.102 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 0.000/5.000/10.000/5.000 ms
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:aa:75:24
          inet addr:192.168.50.101  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feaa:7524/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:18 errors:0 dropped:0 overruns:0 frame:0
          TX packets:51 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2717 (2.6 KB)  TX bytes:4724 (4.6 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:131 errors:0 dropped:0 overruns:0 frame:0
          TX packets:131 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:36397 (35.5 KB)  TX bytes:36397 (35.5 KB)

msfadmin@metasploitable:~$
```

Successivamente ho proceduto alla verifica della connessione tra le 3 macchine virtuali attraverso la funzione **ping** digitata in terminale seguita dagli indirizzi ip - statici delle macchine virtuali precedentemente determinati.

Nello specifico come da immagini si può facilmente vedere che:

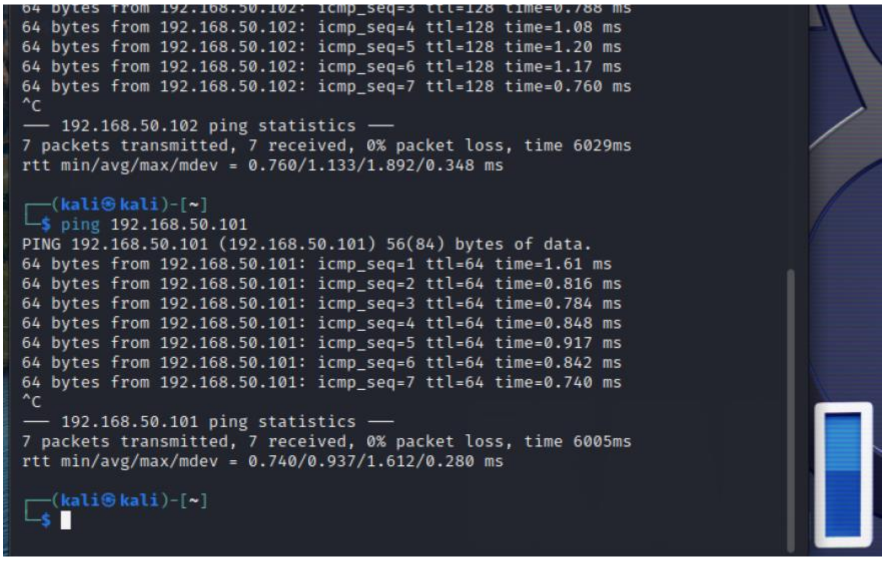
a. Kali comunica con Windows e Metasploitable 2:

1. Kali → Windows



```
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


┌──(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=1.89 ms
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=1.04 ms
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=0.788 ms
64 bytes from 192.168.50.102: icmp_seq=4 ttl=128 time=1.08 ms
64 bytes from 192.168.50.102: icmp_seq=5 ttl=128 time=1.20 ms
64 bytes from 192.168.50.102: icmp_seq=6 ttl=128 time=1.17 ms
64 bytes from 192.168.50.102: icmp_seq=7 ttl=128 time=0.760 ms
^C
── 192.168.50.102 ping statistics ──
7 packets transmitted, 7 received, 0% packet loss, time 6029ms
rtt min/avg/max/mdev = 0.760/1.133/1.892/0.348 ms

┌──(kali㉿kali)-[~]
└─$ 
```

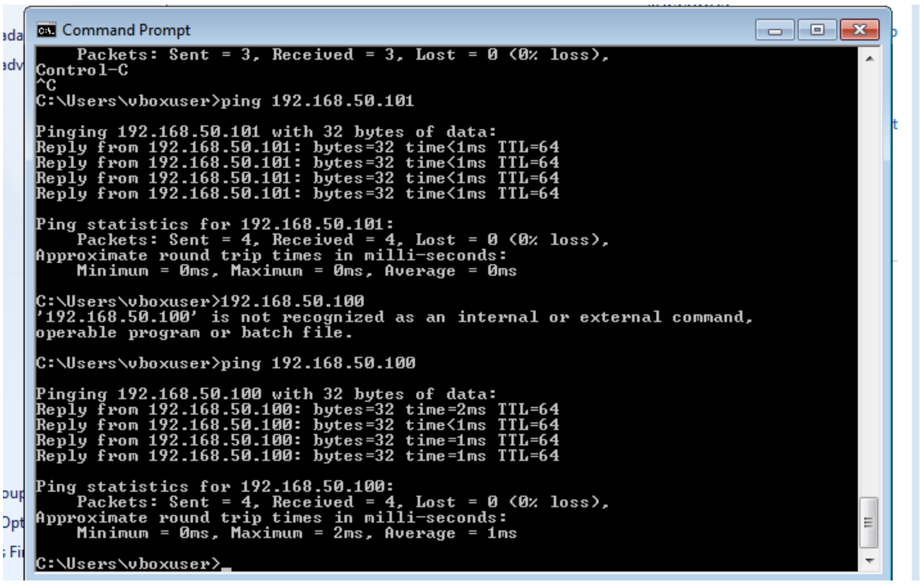
2. Kali→ Metasploitable 2



```
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=0.788 ms
64 bytes from 192.168.50.102: icmp_seq=4 ttl=128 time=1.08 ms
64 bytes from 192.168.50.102: icmp_seq=5 ttl=128 time=1.20 ms
64 bytes from 192.168.50.102: icmp_seq=6 ttl=128 time=1.17 ms
64 bytes from 192.168.50.102: icmp_seq=7 ttl=128 time=0.760 ms
^C
── 192.168.50.102 ping statistics ──
7 packets transmitted, 7 received, 0% packet loss, time 6029ms
rtt min/avg/max/mdev = 0.760/1.133/1.892/0.348 ms

┌──(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=1.61 ms
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=0.816 ms
64 bytes from 192.168.50.101: icmp_seq=3 ttl=64 time=0.784 ms
64 bytes from 192.168.50.101: icmp_seq=4 ttl=64 time=0.848 ms
64 bytes from 192.168.50.101: icmp_seq=5 ttl=64 time=0.917 ms
64 bytes from 192.168.50.101: icmp_seq=6 ttl=64 time=0.842 ms
64 bytes from 192.168.50.101: icmp_seq=7 ttl=64 time=0.740 ms
^C
── 192.168.50.101 ping statistics ──
7 packets transmitted, 7 received, 0% packet loss, time 6005ms
rtt min/avg/max/mdev = 0.740/0.937/1.612/0.280 ms

┌──(kali㉿kali)-[~]
└─$ 
```

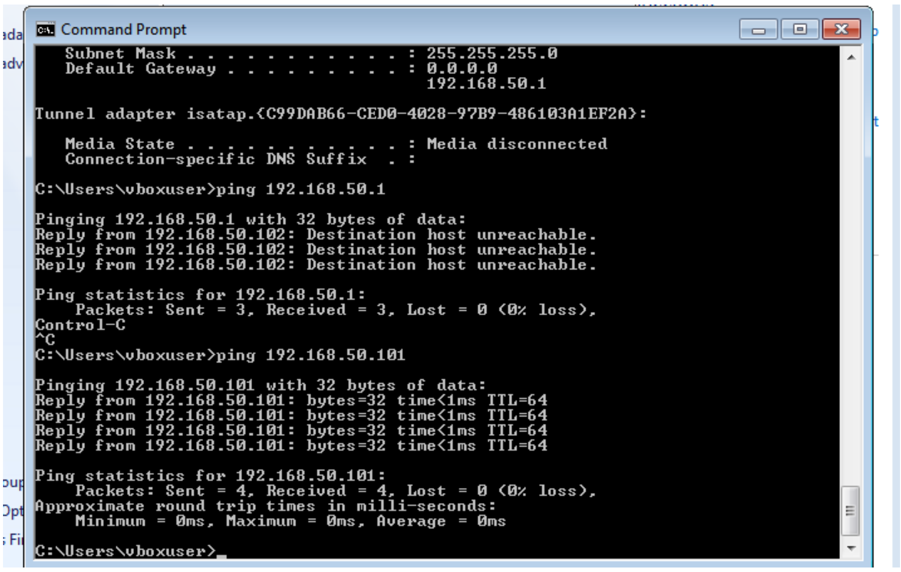
b. Windows comunica con Kali e Metasploitable 2:

1. Windows→ Kali



```
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Control-C
^C
C:\Users\vboxuser>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\vboxuser>192.168.50.100
'192.168.50.100' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\vboxuser>ping 192.168.50.100

Pinging 192.168.50.100 with 32 bytes of data:
Reply from 192.168.50.100: bytes=32 time=2ms 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 = 2ms, Average = 1ms

C:\Users\vboxuser>_
```

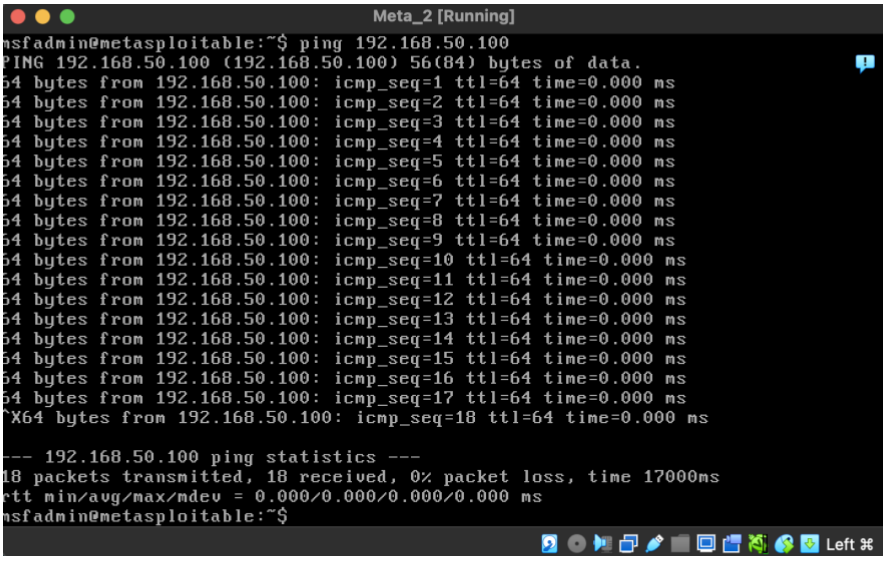
2. Windows → Metasploitable 2



```
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 0.0.0.0
                                       192.168.50.1

Tunnel adapter isatap.{C99DAB66-CED0-4028-97B9-486103A1EF2A}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\vboxuser>ping 192.168.50.1

Pinging 192.168.50.1 with 32 bytes of data:
Reply from 192.168.50.102: Destination host unreachable.
Reply from 192.168.50.102: Destination host unreachable.
Reply from 192.168.50.102: Destination host unreachable.

Ping statistics for 192.168.50.1:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Control-C
^C
C:\Users\vboxuser>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\vboxuser>_
```

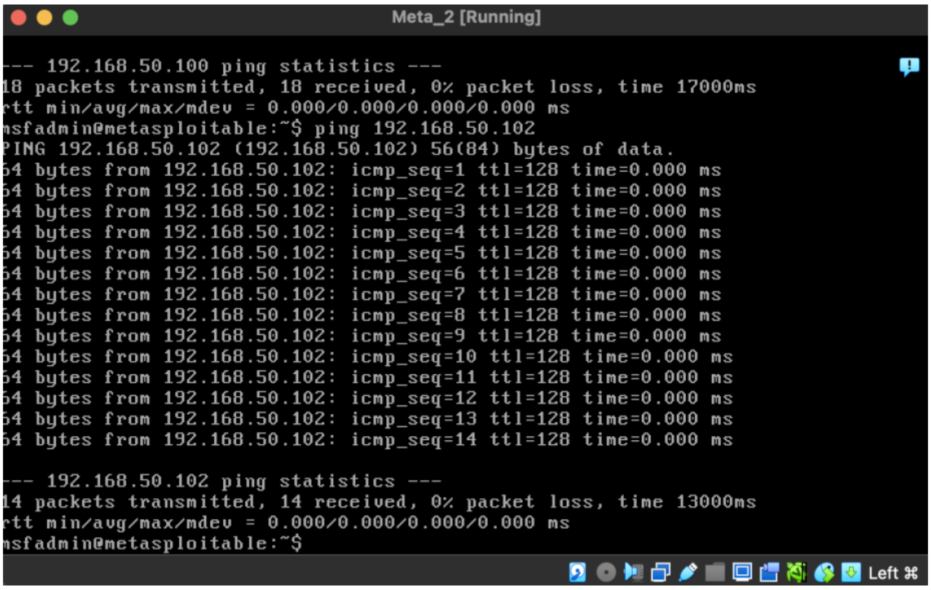
c. Metasploitable 2 comunica con Kali e Windows

1. Metasploitable 2 → Kali



```
nsfadmin@metasploitable:~$ ping 192.168.50.100
PING 192.168.50.100 (192.168.50.100) 56(84) bytes of data.
54 bytes from 192.168.50.100: icmp_seq=1 ttl=64 time=0.000 ms
54 bytes from 192.168.50.100: icmp_seq=2 ttl=64 time=0.000 ms
54 bytes from 192.168.50.100: icmp_seq=3 ttl=64 time=0.000 ms
54 bytes from 192.168.50.100: icmp_seq=4 ttl=64 time=0.000 ms
54 bytes from 192.168.50.100: icmp_seq=5 ttl=64 time=0.000 ms
54 bytes from 192.168.50.100: icmp_seq=6 ttl=64 time=0.000 ms
54 bytes from 192.168.50.100: icmp_seq=7 ttl=64 time=0.000 ms
54 bytes from 192.168.50.100: icmp_seq=8 ttl=64 time=0.000 ms
54 bytes from 192.168.50.100: icmp_seq=9 ttl=64 time=0.000 ms
54 bytes from 192.168.50.100: icmp_seq=10 ttl=64 time=0.000 ms
54 bytes from 192.168.50.100: icmp_seq=11 ttl=64 time=0.000 ms
54 bytes from 192.168.50.100: icmp_seq=12 ttl=64 time=0.000 ms
54 bytes from 192.168.50.100: icmp_seq=13 ttl=64 time=0.000 ms
54 bytes from 192.168.50.100: icmp_seq=14 ttl=64 time=0.000 ms
54 bytes from 192.168.50.100: icmp_seq=15 ttl=64 time=0.000 ms
54 bytes from 192.168.50.100: icmp_seq=16 ttl=64 time=0.000 ms
54 bytes from 192.168.50.100: icmp_seq=17 ttl=64 time=0.000 ms
`X64 bytes from 192.168.50.100: icmp_seq=18 ttl=64 time=0.000 ms

--- 192.168.50.100 ping statistics ---
18 packets transmitted, 18 received, 0% packet loss, time 17000ms
rtt min/avg/max/mdev = 0.000/0.000/0.000/0.000 ms
nsfadmin@metasploitable:~$
```

2. Metasploitable 2 → Windows



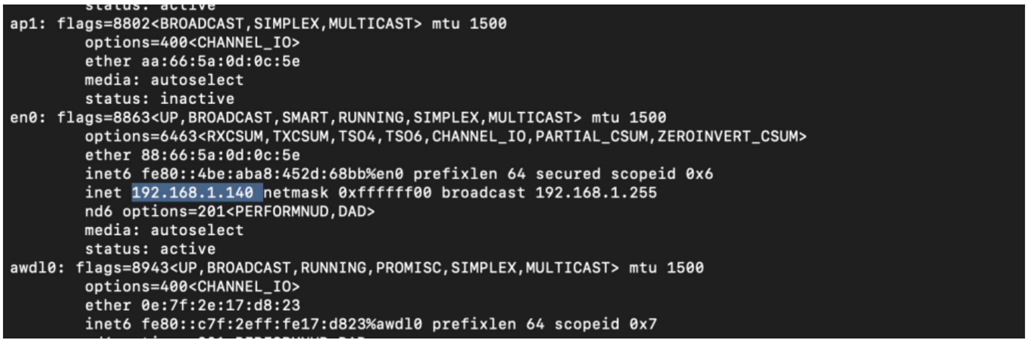
```
--- 192.168.50.100 ping statistics ---
18 packets transmitted, 18 received, 0% packet loss, time 17000ms
rtt min/avg/max/mdev = 0.000/0.000/0.000/0.000 ms
nsfadmin@metasploitable:~$ ping 192.168.50.102
PING 192.168.50.102 (192.168.50.102) 56(84) bytes of data.
54 bytes from 192.168.50.102: icmp_seq=1 ttl=128 time=0.000 ms
54 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=0.000 ms
54 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=0.000 ms
54 bytes from 192.168.50.102: icmp_seq=4 ttl=128 time=0.000 ms
54 bytes from 192.168.50.102: icmp_seq=5 ttl=128 time=0.000 ms
54 bytes from 192.168.50.102: icmp_seq=6 ttl=128 time=0.000 ms
54 bytes from 192.168.50.102: icmp_seq=7 ttl=128 time=0.000 ms
54 bytes from 192.168.50.102: icmp_seq=8 ttl=128 time=0.000 ms
54 bytes from 192.168.50.102: icmp_seq=9 ttl=128 time=0.000 ms
54 bytes from 192.168.50.102: icmp_seq=10 ttl=128 time=0.000 ms
54 bytes from 192.168.50.102: icmp_seq=11 ttl=128 time=0.000 ms
54 bytes from 192.168.50.102: icmp_seq=12 ttl=128 time=0.000 ms
54 bytes from 192.168.50.102: icmp_seq=13 ttl=128 time=0.000 ms
54 bytes from 192.168.50.102: icmp_seq=14 ttl=128 time=0.000 ms

--- 192.168.50.102 ping statistics ---
14 packets transmitted, 14 received, 0% packet loss, time 13000ms
rtt min/avg/max/mdev = 0.000/0.000/0.000/0.000 ms
nsfadmin@metasploitable:~$
```

SISTEMA HOST NON COMUNICA CON LE MACCHINE VIRTUALI

Infine, sono andato a verificare che il sistema **HOST** su cui gira la macchina virtuale “VirtualBox”, quindi anche le macchine virtuali contenuto in essa, non comunichi con le suddette.

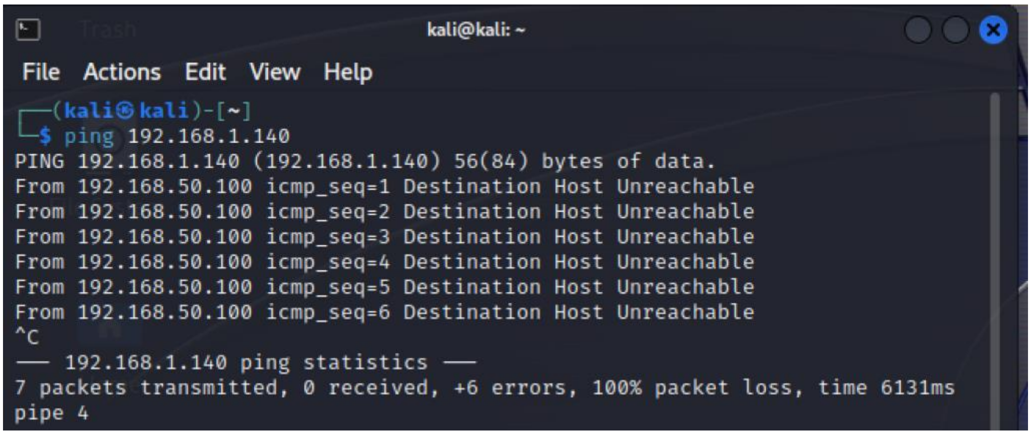
Andando ad effettuare la verifica dei **ping** su terminale delle 3 macchine vistuali e inserendo l’IP dell’host: 192.168.1.140 (in terminale digitando **ifconfig** si può facilmente scoprire).

IP Host



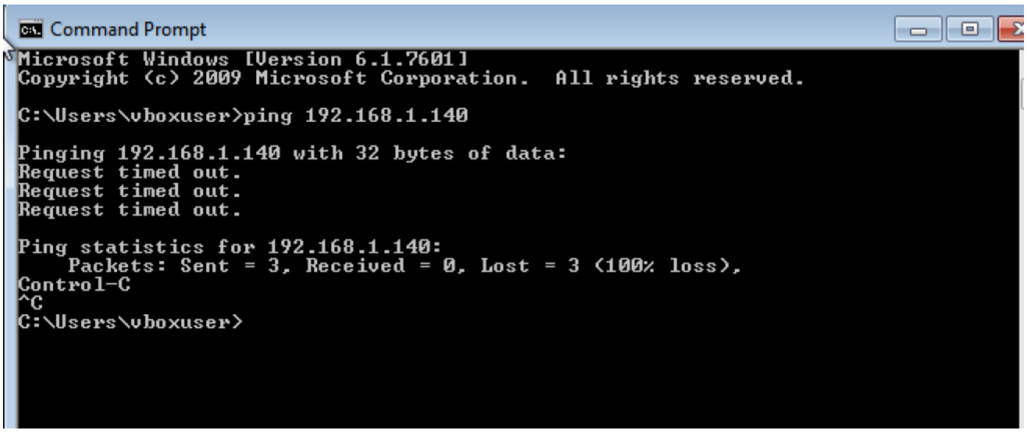
```
        status: active
ap1: flags=8802<BROADCAST,SIMPLEX,MULTICAST> mtu 1500
        options=400<CHANNEL_IO>
        ether aa:66:5a:0d:0c:5e
        media: autoselect
        status: inactive
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
        options=6463<RXCSUM,TXCSUM,TSO4,TSO6,CHANNEL_IO,PARTIAL_CSUM,ZEROINVERT_CSUM>
        ether 88:66:5a:0d:0c:5e
        inet6 fe80::4be:aba8:452d:68bb%en0 prefixlen 64 secured scopeid 0x6
        inet 192.168.1.140 netmask 0xffffff00 broadcast 192.168.1.255
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
awdl0: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
        options=400<CHANNEL_IO>
        ether 0e:7f:2e:17:d8:23
        inet6 fe80::c7f:2eff:fe17:d823%awdl0 prefixlen 64 scopeid 0x7
```

Kali → Host



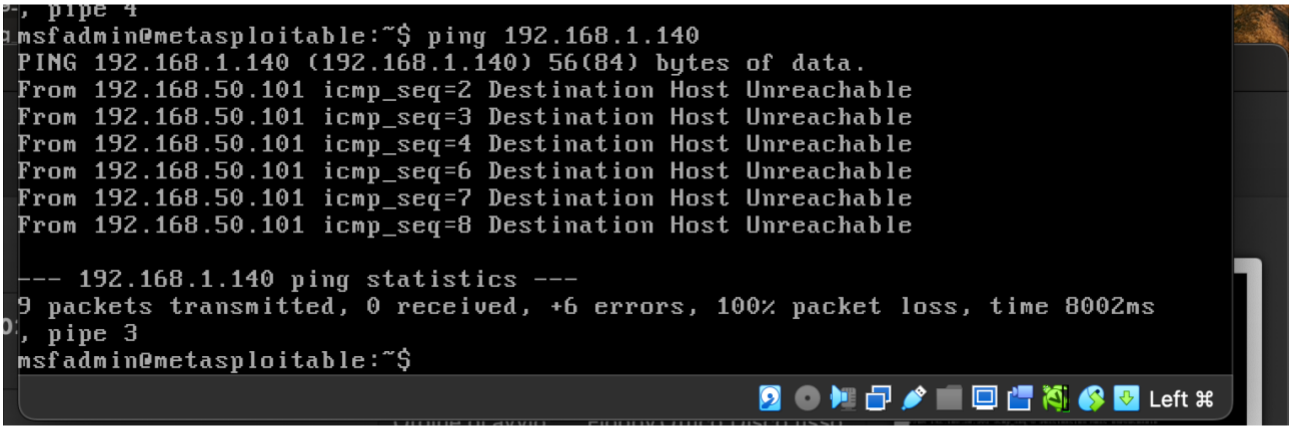
```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.1.140
PING 192.168.1.140 (192.168.1.140) 56(84) bytes of data.
From 192.168.50.100 icmp_seq=1 Destination Host Unreachable
From 192.168.50.100 icmp_seq=2 Destination Host Unreachable
From 192.168.50.100 icmp_seq=3 Destination Host Unreachable
From 192.168.50.100 icmp_seq=4 Destination Host Unreachable
From 192.168.50.100 icmp_seq=5 Destination Host Unreachable
From 192.168.50.100 icmp_seq=6 Destination Host Unreachable
^C
── 192.168.1.140 ping statistics ──
7 packets transmitted, 0 received, +6 errors, 100% packet loss, time 6131ms
pipe 4
```

Windows → host



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\vboxuser>ping 192.168.1.140

Pinging 192.168.1.140 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.140:
    Packets: Sent = 3, Received = 0, Lost = 3 (100% loss),
Control-C
^C
C:\Users\vboxuser>
```

Metasploitable 2 → host



```
-, pipe 4
msfadmin@metasploitable:~$ ping 192.168.1.140
PING 192.168.1.140 (192.168.1.140) 56(84) bytes of data.
From 192.168.50.101 icmp_seq=2 Destination Host Unreachable
From 192.168.50.101 icmp_seq=3 Destination Host Unreachable
From 192.168.50.101 icmp_seq=4 Destination Host Unreachable
From 192.168.50.101 icmp_seq=6 Destination Host Unreachable
From 192.168.50.101 icmp_seq=7 Destination Host Unreachable
From 192.168.50.101 icmp_seq=8 Destination Host Unreachable

--- 192.168.1.140 ping statistics ---
9 packets transmitted, 0 received, +6 errors, 100% packet loss, time 8002ms
, pipe 3
msfadmin@metasploitable:~$
```

CONCLUSIONI

Concludendo si può dire che tutte le richieste sono state soddisfatte come da immagini di riferimento. La richiesta iniziale di installare **VirtualBox** è facilmente identificabile nell'utilizzo delle tre macchine virtuali le quali altrimenti non potrebbero girare.