

REPORT CONFIGURAZIONE MACCHINE VIRTUALI IN LABORATORIO VIRTUALE

Consegna:

creare un laboratorio virtuale, con le seguenti caratteristiche:

1. Installazione di Oracle VirtualBox
2. Installazione e configurazione di Kali Linux
3. Installazione e configurazione di Metasploitable
4. Installazione e configurazione di Windows 7
5. Le macchine virtuali devono essere in grado di comunicare tra di loro su rete interna (evidenze ping tra le macchine)
6. Il sistema host non deve comunicare con l'ambiente virtuale

1

Facoltativo: spazio sul disco permettendo, 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. Al termine dell'attività decidere se tenerla per ulteriori esperimenti oppure eliminarla.

Procedimenti

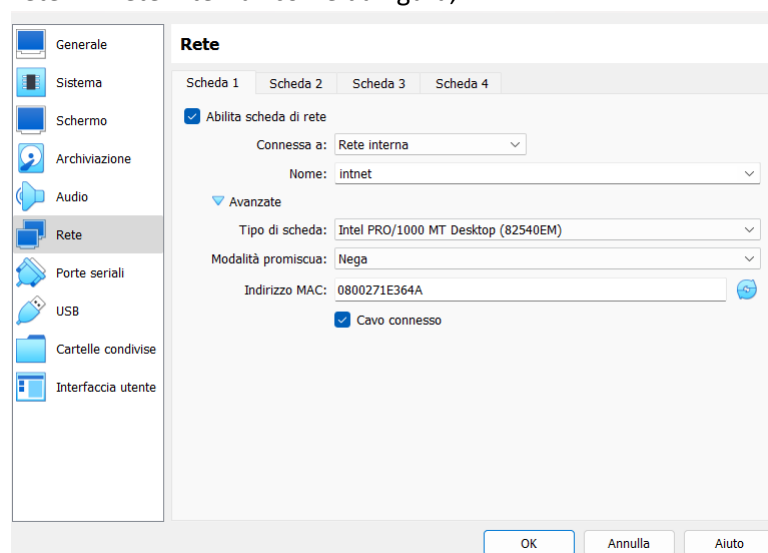
Consegna 1: Installazione di Oracle VirtualBox

Per quanto riguarda il punto 1, la richiesta è stata già completata con i report presenti nelle cartelle M1/W1/D1 e M1/W1/D3.

To Do List – Prima di avviare le macchine virtuali

Prima di avviare le macchine virtuali installate:

- andiamo su "Impostazioni" > "Sistema" > "Scheda Madre" controlliamo la RAM allocata e deseleggiamo Floppy, poi su "Processore" controlliamo quanti "CPU" è stata allocata. **Conoscendo il proprio hardware, con questo controllo si evitano crash dovuti all'indisponibilità di risorse;**
- controlliamo, se non fatto durante l'installazione, andiamo su "Rete" e impostiamo su Scheda 1 "Abilita scheda di rete" > "Rete Interna" come da figura;

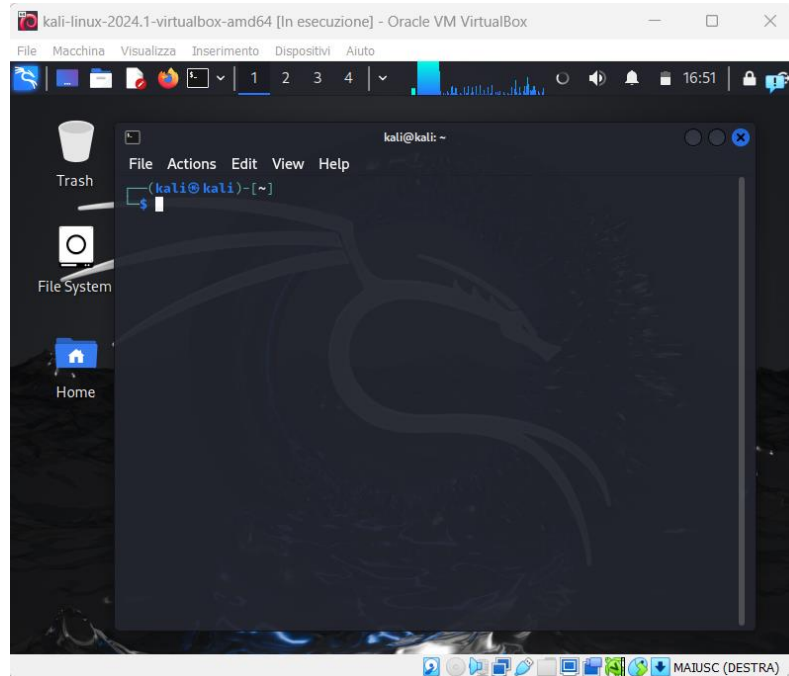


Consegna 2: Installazione e configurazione di Kali Linux

Per quanto riguarda l'installazione si rimanda all'ultimo report in M1/W1/D3.

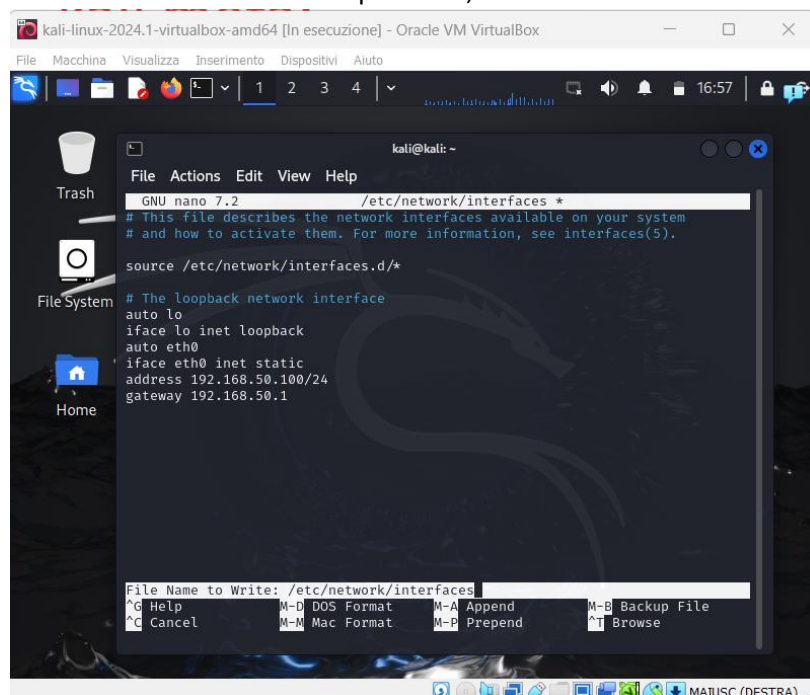
Per la configurazione invece si segue la seguente procedura:

- configurato VirtualBox (Vedi il To Do List sopra) avviamo la macchina virtuale;
- inseriamo le credenziali di Kali Linux "kali:kali";
- apriamo il "Terminal Emulator" in alto a sx;

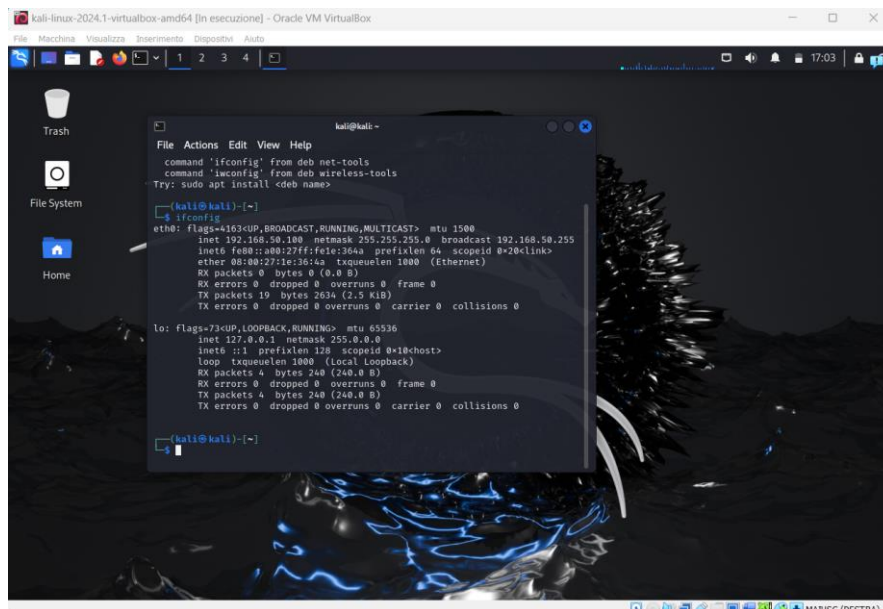


2

- scriviamo il comando "sudo nano /etc/network/interfaces" e inseriamo la password (vedi sopra);
- modifichiamo l'indirizzo IP settandolo l'indirizzo statico a 192.168.50.100 (indirizzo IP deciso dalla consegna) poi premiamo CTRL+O e CTRL+X e poi Enter;



- riavviamo Kali Linux con "sudo reboot"
- una volta riavviato riapriamo il terminale e verifichiamo con il comando "ifconfig" (non IPconfig) che sia come in figura;



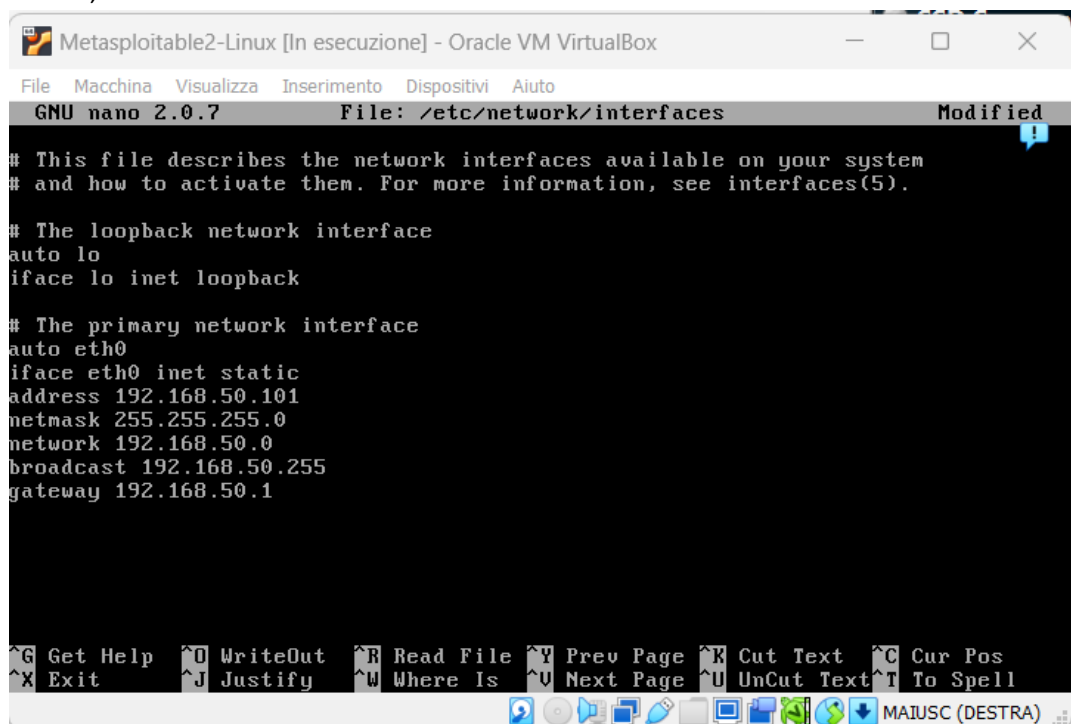
3

Consegna 3: Installazione e configurazione di Metasploitable

Per quanto riguarda l'installazione si rimanda all'ultimo report in M1/W1/D3.

Per quanto riguarda la configurazione eseguiamo i seguenti passaggi:

- controlliamo la configurazione preliminare, lo avviamo, inseriamo le credenziali msfadmin:msfadmin (attenzione quando si digita non appaiono);
- siccome Metasploitable è già un terminale utilizziamo gli stessi comandi per la configurazione dell'indirizzo IP statico a 192.168.50.101 (indirizzo IP deciso dalla consegna) con la stessa procedura di Kali Linux;



- sempre stessi comandi per salvare CTRL+O invio, CTRL+X invio e riavviamo;
- lasciamo "ifconfig" e controlliamo se l'ip sia stato impostato correttamente.

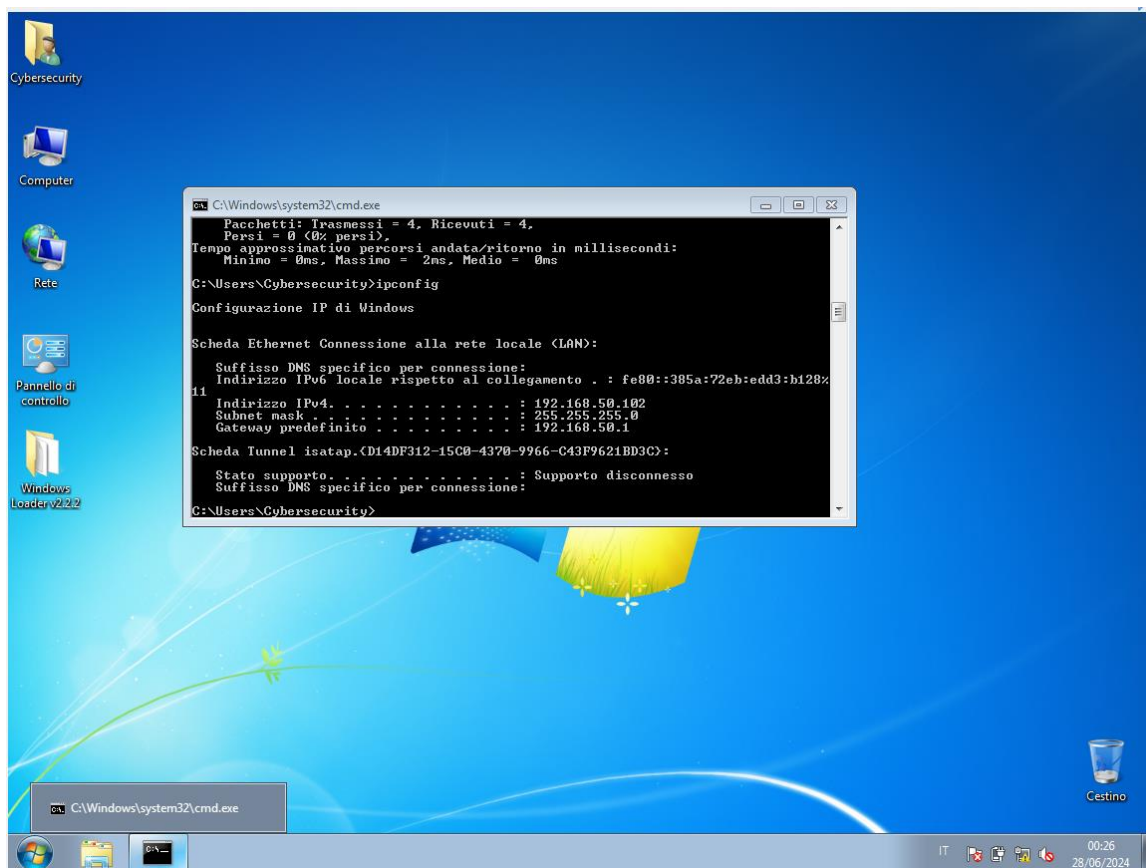
Consegna 4: Installazione e configurazione di Windows 7

Per quanto riguarda l'installazione si rimanda all'ultimo report in M1/W1/D3. Ricordarsi di verificare le impostazioni di Virtual Box prima dell'avvio della macchina virtuale.

Per quanto riguarda la configurazione seguiamo i seguenti passaggi:

- avvio della macchina virtuale, apriamo l'interfaccia Windows e con i metodi preferiti entrare nell'impostazione della scheda di rete (dal pannello di controllo) per impostare l'IP Statico; è la stessa schermata dove molte guide spiegano come cambiare i DNS;
- impostiamo l'indirizzo IP statico a 192.168.50.102 (indirizzo IP deciso dalla consegna), non sono necessari configurare i DNS;
- riavviamo;
- verifichiamo aprendo il terminale di Windows, cerchiamo CMD e lanciamo il comando "ipconfig" e controlliamo il risultato.

4



```
C:\Windows\system32\cmd.exe
Pacchetti: Trasmessi = 4, Ricevuti = 4,
Persi = 0 (0% persi).
Tempo approssimativo percorsi andata/ritorno in millisecondi:
Minimo = 0ms, Massimo = 2ms, Medio = 0ms

C:\Users\Cybersecurity>ipconfig

Configurazione IP di Windows

Scheda Ethernet Connessione alla rete locale (LAN):
Suffisso DNS specifico per connessione:
Indirizzo IPv6 locale rispetto al collegamento . : fe80::385a:72eb:edd3:b128%11
Indirizzo IPv4. . . . . : 192.168.50.102
Subnet mask . . . . . : 255.255.255.0
Gateway predefinito . . . . . : 192.168.50.1

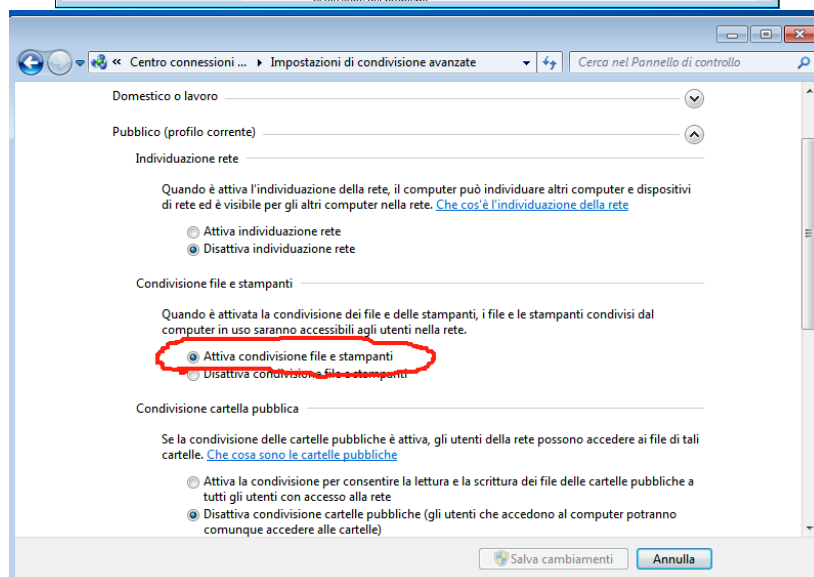
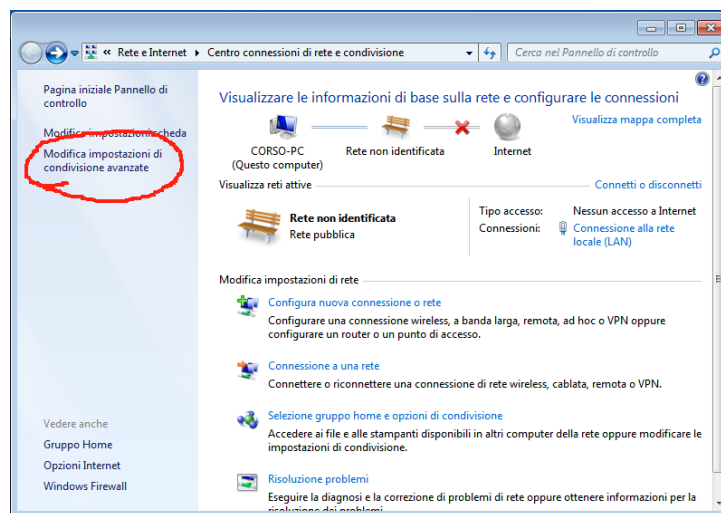
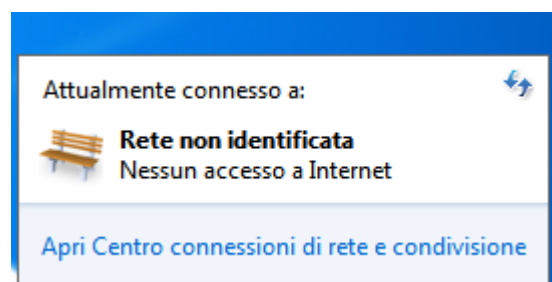
Scheda Tunnel isatap.{D14DF312-15C0-4370-9966-C43F9621BD3C}:
Stato supporto. . . . . : Supporto disconnesso
Suffisso DNS specifico per connessione:

C:\Users\Cybersecurity>
```

Consegna 5 Le macchine virtuali devono essere in grado di comunicare tra di loro su rete interna (evidenze ping tra le macchine)

Avviamo le macchine virtuali contemporaneamente: Kali Linux, Metasploitable e Windows 7. Per verificare che le macchine siano in grado di comunicare tra di loro usiamo nei rispettivi terminali di ogni macchina il comando “ping” seguito dall’indirizzo IP statico delle altre macchine.

Prima di eseguire i ping test sottoelencate ricordiamo che Windows 7 ha un suo firewall che potrebbe bloccare le connessioni Kali Linux e Metasploitable. Infatti potrebbe rilevare la rete interna di Virtual Box come una Rete Pubblica e di default, la condivisione file e stampanti è disattiva, ciò comporta che lo renderà offline per gli altri dispositivi della rete. Per risolvere basta cambiare il profilo in Rete Aziendale o Domestica, altrimenti basta attivare la condivisione file e stampanti: recarsi al “Pannello di Controllo” “Rete e Internet”, sulla sinistra “Modifica impostazioni di condivisione avanzate” e assicurarsi che sia attiva la condivisione file e stampanti, poi salvare. L’altra alternativa meno sicura è quella di disattivare completamente il firewall.



Ora proviamo a lanciare i comandi e verificare i risultati.

Da Kali Linux lanciamo i comandi:

“ping 192.168.50.101” e “ping 192.168.50.102” CTRL+C per terminare. / Risultato come da richiesta.

```
kali@kali: ~  
File Actions Edit View Help  
$ 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=2.18 ms  
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=0.828 ms  
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=1.10 ms  
64 bytes from 192.168.50.102: icmp_seq=4 ttl=128 time=1.10 ms  
^C  
--- 192.168.50.102 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3003ms  
rtt min/avg/max/mdev = 0.828/1.300/2.177/0.518 ms  
  
$ 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=6.13 ms  
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=1.09 ms  
64 bytes from 192.168.50.101: icmp_seq=3 ttl=64 time=1.42 ms  
64 bytes from 192.168.50.101: icmp_seq=4 ttl=64 time=1.29 ms  
64 bytes from 192.168.50.101: icmp_seq=5 ttl=64 time=1.20 ms  
64 bytes from 192.168.50.101: icmp_seq=6 ttl=64 time=1.08 ms  
^C  
--- 192.168.50.101 ping statistics ---  
6 packets transmitted, 6 received, 0% packet loss, time 5007ms  
rtt min/avg/max/mdev = 1.082/2.035/6.127/1.833 ms  
  
$
```

6

Da Metasploitable lanciamo i comandi:

“ping 192.168.50.100” e “ping 192.168.50.102” CTRL+C per terminare. / Risultato come da richiesta.

```
Metasploitable2-Linux [In esecuzione] - Oracle VM VirtualBox  
File Macchina Visualizza Inserimento Dispositivi Aiuto  
--- 192.168.50.100 ping statistics ---  
7 packets transmitted, 7 received, 0% packet loss, time 6001ms  
rtt min/avg/max/mdev = 1.022/1.115/1.237/0.065 ms  
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=2.72 ms  
64 bytes from 192.168.50.100: icmp_seq=2 ttl=64 time=1.38 ms  
64 bytes from 192.168.50.100: icmp_seq=3 ttl=64 time=1.06 ms  
64 bytes from 192.168.50.100: icmp_seq=4 ttl=64 time=0.965 ms  
--- 192.168.50.100 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3001ms  
rtt min/avg/max/mdev = 0.965/1.535/2.726/0.705 ms  
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=8.83 ms  
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=0.800 ms  
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=0.954 ms  
64 bytes from 192.168.50.102: icmp_seq=4 ttl=128 time=1.33 ms  
--- 192.168.50.102 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 2997ms  
rtt min/avg/max/mdev = 0.800/2.980/8.835/3.385 ms  
msfadmin@metasploitable:~$
```

Da Windows 7 lanciamo i comandi:

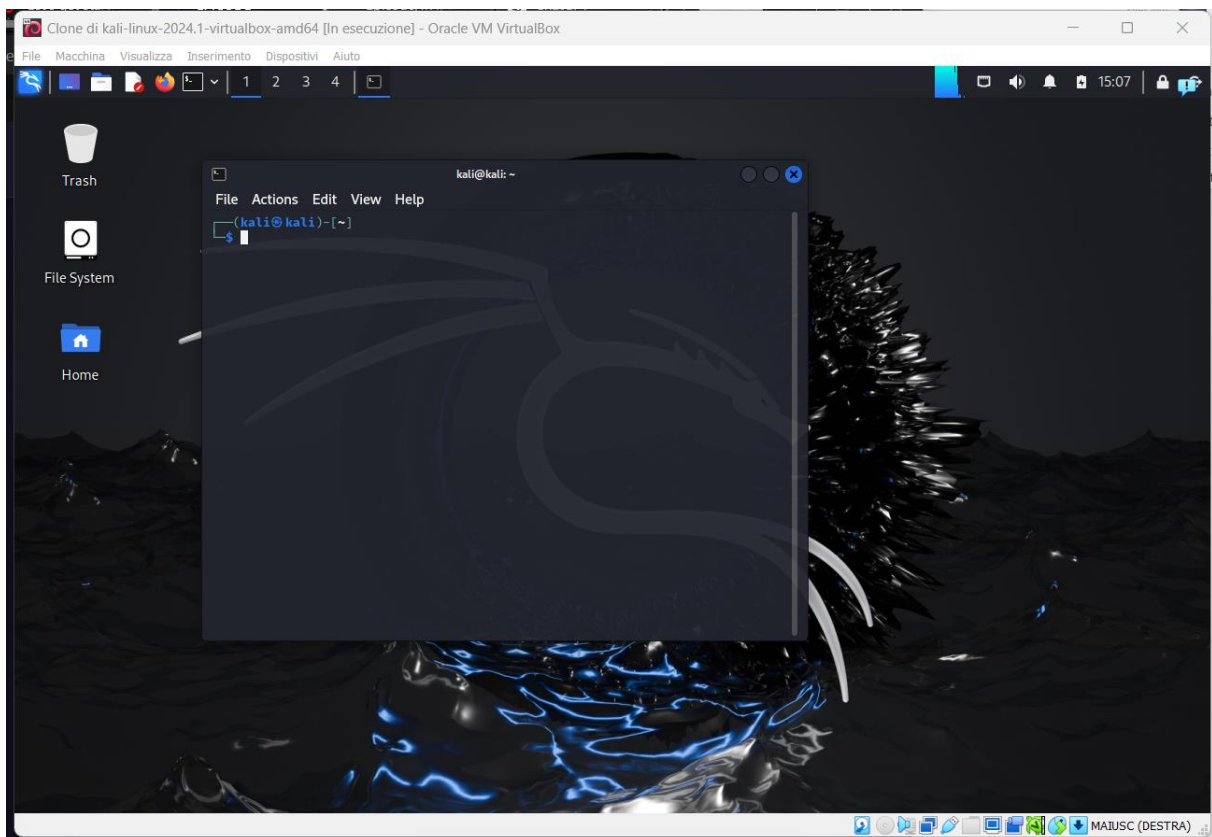
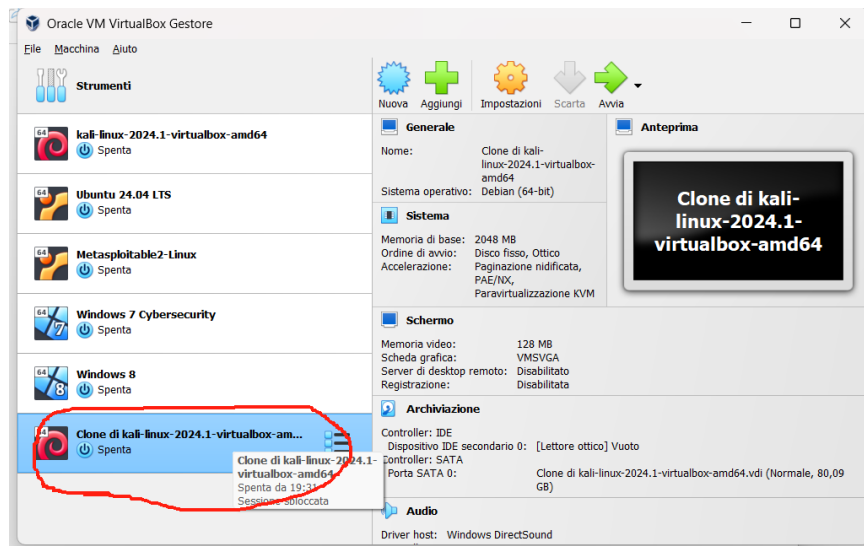
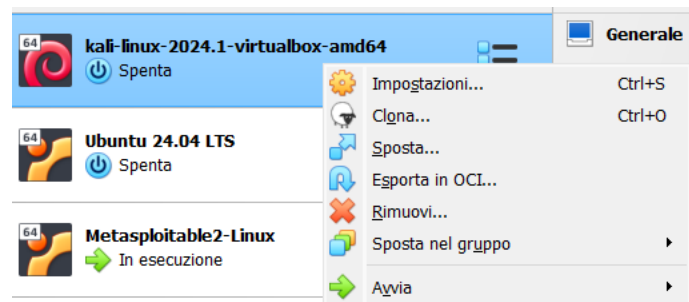
“ping 192.168.50.100” e “ping 192.168.50.101” CTRL+C per terminare. / Risultato come da richiesta.

```
C:\Windows\system32\cmd.exe  
C:\Users\Cybersecurity>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=2ms 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 = 0ms, Massimo = 2ms, Medio = 0ms  
C:\Users\Cybersecurity>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=2ms TTL=64  
Risposta da 192.168.50.101: byte=32 durata<1ms TTL=64  
Risposta da 192.168.50.101: byte=32 durata<1ms 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 = 2ms, Medio = 1ms  
C:\Users\Cybersecurity>
```

Al termine spegniamo le macchine con “Arresta il sistema” o da terminale linux “sudo shutdown now”

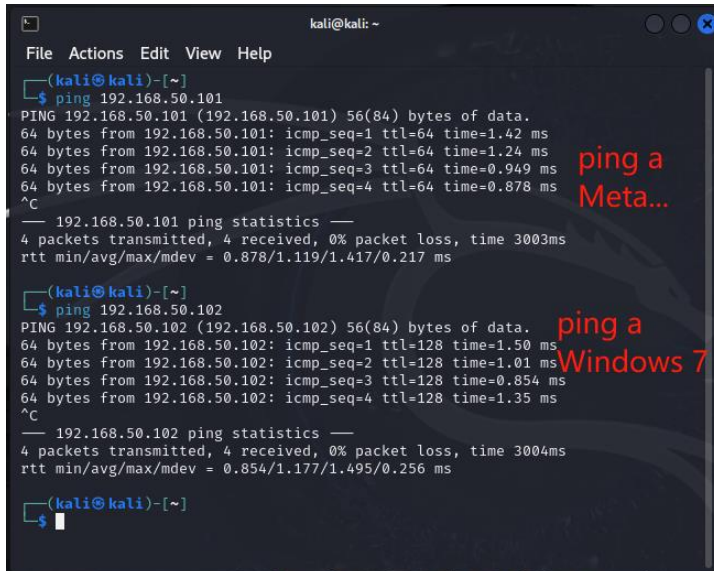
Consegna Facoltativa – Clonare una macchina virtuale e testare le connessioni della rete interna

Creiamo un qualsiasi clone di una macchina virtuale, nel mio caso ho scelto Kali Linux, con la funzione “Clona”.



Eseguiamo gli stessi ping tra le macchine virtuali, come risultati sottostanti, comunicano tra di loro con successo.

Da Kali Linux



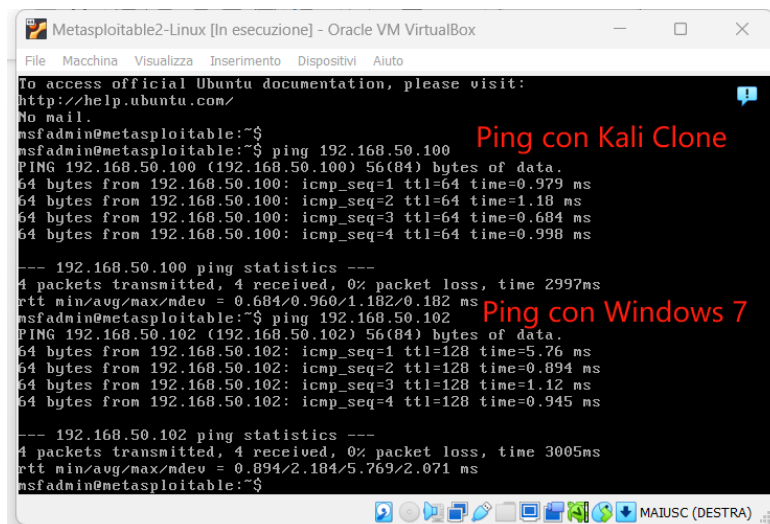
```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)~  
$ ping 192.168.50.101  
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data:  
64 bytes from 192.168.50.101: icmp_seq=1 ttl=64 time=1.42 ms  
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=1.24 ms  
64 bytes from 192.168.50.101: icmp_seq=3 ttl=64 time=0.949 ms  
64 bytes from 192.168.50.101: icmp_seq=4 ttl=64 time=0.878 ms  
^C  
--- 192.168.50.101 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3003ms  
rtt min/avg/max/mdev = 0.878/1.119/1.417/0.217 ms  
  
(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=1.50 ms  
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=1.01 ms  
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=0.854 ms  
64 bytes from 192.168.50.102: icmp_seq=4 ttl=128 time=1.35 ms  
^C  
--- 192.168.50.102 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3004ms  
rtt min/avg/max/mdev = 0.854/1.177/1.495/0.256 ms  
  
(kali@kali)~  
$
```

ping a Meta...

ping a Windows 7

8

Da Metasploitable2

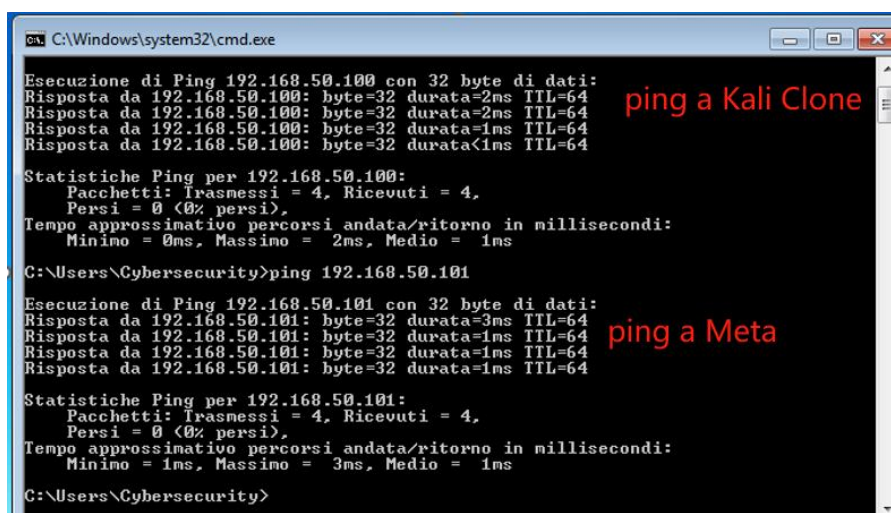


```
Metasploitable2-Linux [In esecuzione] - Oracle VM VirtualBox  
File Macchina Visualizza Inserimento Dispositivi Aiuto  
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
msfadmin@metasploitable:~$  
msfadmin@metasploitable:~$ ping 192.168.50.100  
PING 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=0.979 ms  
64 bytes from 192.168.50.100: icmp_seq=2 ttl=64 time=1.18 ms  
64 bytes from 192.168.50.100: icmp_seq=3 ttl=64 time=0.684 ms  
64 bytes from 192.168.50.100: icmp_seq=4 ttl=64 time=0.998 ms  
--- 192.168.50.100 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 2997ms  
rtt min/avg/max/mdev = 0.684/0.960/1.182/0.182 ms  
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=5.76 ms  
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=0.894 ms  
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=1.12 ms  
64 bytes from 192.168.50.102: icmp_seq=4 ttl=128 time=0.945 ms  
--- 192.168.50.102 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3005ms  
rtt min/avg/max/mdev = 0.894/2.184/5.769/2.071 ms  
msfadmin@metasploitable:~$
```

Ping con Kali Clone

Ping con Windows 7

Da Windows 7



```
C:\Windows\system32\cmd.exe  
Esecuzione di Ping 192.168.50.100 con 32 byte di dati:  
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=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 = 0ms, Massimo = 2ms, Medio = 1ms  
C:\Users\Cybersecurity>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=3ms TTL=64  
Risposta da 192.168.50.101: byte=32 durata=1ms TTL=64  
Risposta da 192.168.50.101: byte=32 durata=1ms 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 = 3ms, Medio = 1ms  
C:\Users\Cybersecurity>
```

ping a Kali Clone

ping a Meta