

Settimana 2 - Giorno 5 - PRATICA - Relazione - Macchine virtuali

L'esercizio consiste nella creazione e configurazione come da architettura di riferimento (riferendomi alla slide usata per l'esercizio) di un laboratorio virtuale basato su Oracle VirtualBox. La creazione del laboratorio è parte essenziale del lavoro di un Hacker Etico, così come lo è la risoluzione di eventuali problematiche incontrate. Risolvere i problemi nel vostro laboratorio sarà il modo più semplice per acquisire competenze pratiche.

Lasciando sottointeso che tutte e tre le macchine siano già state installate e configurate (lascerò delle immagini in seguito), passo direttamente al terzo punto.

- KALI LINUX: configurazione

```
kali@kali: ~  
File Actions Edit View Help  
(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 08:00:27:34:ea:d1 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::15d0:2587:ea5c:7637/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever  
(kali@kali)-[~]  
$ ip r  
default via 192.168.50.1 dev eth0 proto static metric 100  
192.168.50.0/24 dev eth0 proto kernel scope link src 192.168.50.100 metric 100
```

- METASPLOITABLE 2: configurazione

```
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 08:00:27:8c:7d:26 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:fe8c:7d26/64 scope link  
        valid_lft forever preferred_lft forever  
msfadmin@metasploitable:~$ ip r  
192.168.50.0/24 dev eth0 proto kernel scope link src 192.168.50.101  
default via 192.168.50.1 dev eth0 metric 100
```

- WINDOWS 10 - PRO: configurazione

Seleziona C:\Windows\system32\cmd.exe

```
C:\Users\user>ipconfig
```

```
Configurazione IP di Windows
```

```
Scheda Ethernet Ethernet:
```

```
Suffisso DNS specifico per connessione:
```

```
Indirizzo IPv4. . . . . : 192.168.50.102
```

```
Subnet mask . . . . . : 255.255.255.0
```

```
Gateway predefinito . . . . . : 192.168.50.1
```

3° Le macchine virtuali devono essere in grado di comunicare tra di loro su rete interna (evidenze ping tra la macchine)

- KALI LINUX:

Test di comunicazione da Kali a Metasploitable 2 e da Kali a Windows 10 - PRO

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ ping -c 4 192.168.50.101  
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=1.44 ms  
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=0.491 ms  
64 bytes from 192.168.50.101: icmp_seq=3 ttl=64 time=0.520 ms  
64 bytes from 192.168.50.101: icmp_seq=4 ttl=64 time=1.37 ms  
  
— 192.168.50.101 ping statistics —  
4 packets transmitted, 4 received, 0% packet loss, time 3141ms  
rtt min/avg/max/mdev = 0.491/0.954/1.437/0.449 ms  
  
(kali@kali)-[~]  
$ ping -c 4 192.168.50.102  
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=1.18 ms  
64 bytes from 192.168.50.102: icmp_seq=2 ttl=128 time=0.826 ms  
64 bytes from 192.168.50.102: icmp_seq=3 ttl=128 time=0.622 ms  
64 bytes from 192.168.50.102: icmp_seq=4 ttl=128 time=0.865 ms  
  
— 192.168.50.102 ping statistics —  
4 packets transmitted, 4 received, 0% packet loss, time 4394ms  
rtt min/avg/max/mdev = 0.622/0.874/1.183/0.200 ms
```

- METASPLOITABLE 2:

Test di comunicazione da Metasploitable 2 a Kali Linux e da Metasploitable 2 a Windows 10 - PRO


```
msfadmin@metasploitable:~$ ping -c 4 192.168.50.100
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=0.000 ms
64 bytes from 192.168.50.100: icmp_seq=2 ttl=64 time=0.617 ms
64 bytes from 192.168.50.100: icmp_seq=3 ttl=64 time=0.835 ms
64 bytes from 192.168.50.100: icmp_seq=4 ttl=64 time=0.697 ms

--- 192.168.50.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 0.000/0.537/0.835/0.320 ms
msfadmin@metasploitable:~$ ping -c 4 192.168.50.102
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=9.60 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=0.000 ms
64 bytes from 192.168.50.102: icmp_seq=4 ttl=128 time=0.000 ms

--- 192.168.50.102 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3001ms
rtt min/avg/max/mdev = 0.000/2.655/9.609/4.036 ms
msfadmin@metasploitable:~$
```

- WINDOWS 10 - PRO:

Test di comunicazione da Windows 10 - PRO a Kali Linux e da Windows 10 - PRO Metasploitable 2

 C:\Windows\system32\cmd.exe

```
Microsoft Windows [Versione 10.0.10240]
(c) 2015 Microsoft Corporation. Tutti i diritti sono riservati.

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<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
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 = 0ms, Medio = 0ms

C:\Users\user>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<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
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 = 0ms, Massimo = 0ms, Medio = 0ms
```

4° Il sistema host non deve comunicare con l'ambiente virtuale

```
PS C:\Users\Giuseppe> ping 192.168.50.100

Esecuzione di Ping 192.168.50.100 con 32 byte di dati:
Richiesta scaduta.
Richiesta scaduta.
Richiesta scaduta.
Richiesta scaduta.

Statistiche Ping per 192.168.50.100:
    Pacchetti: Trasmessi = 4, Ricevuti = 0,
    Persi = 4 (100% persi),
PS C:\Users\Giuseppe> 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.

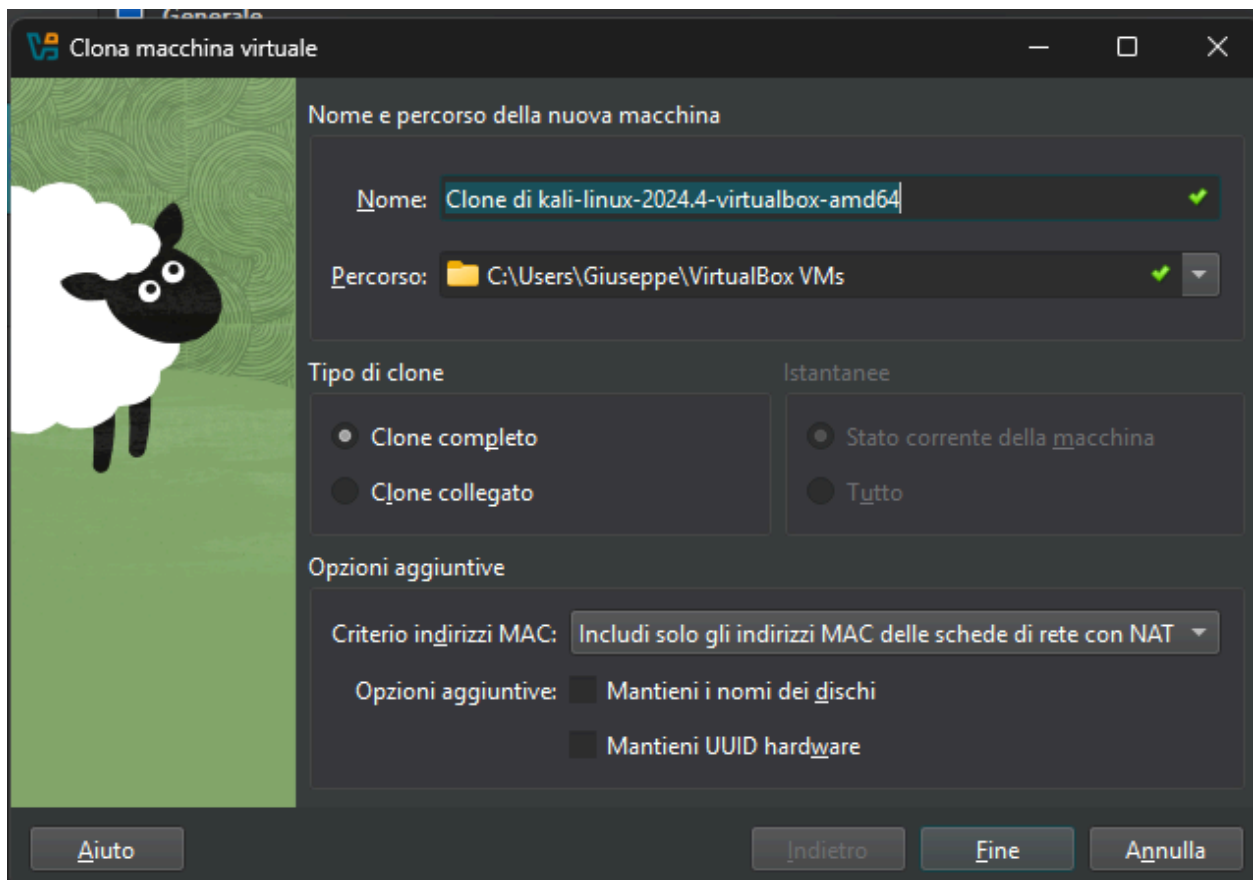
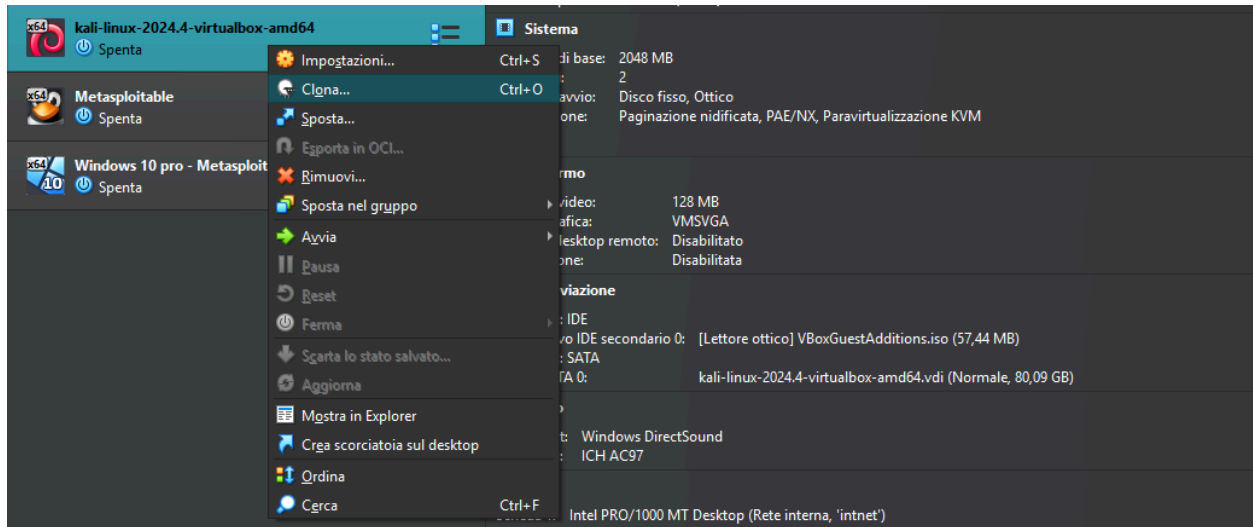
Statistiche Ping per 192.168.50.101:
    Pacchetti: Trasmessi = 4, Ricevuti = 0,
    Persi = 4 (100% persi),
PS C:\Users\Giuseppe> ping 192.168.50.102

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),
```

FACOLTATIVO:

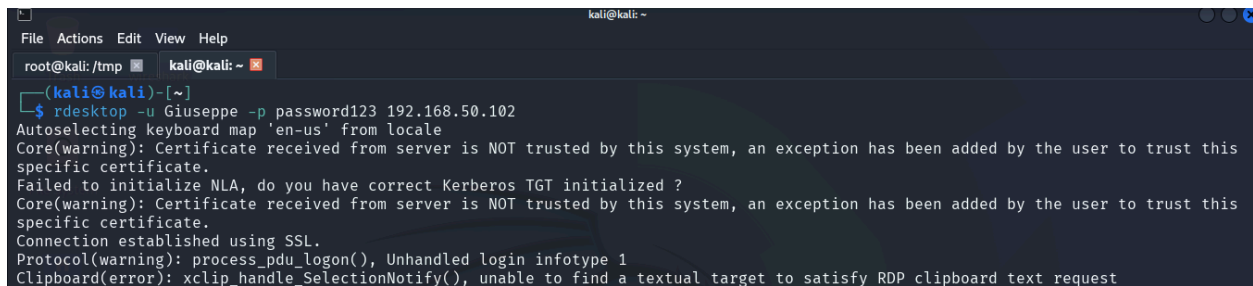
Spazio sul disco permettendo, si richiede di creare una versione di recovery di una delle macchine appena create, come ad esempio l'opzione Clona.



Esercizio alternativo per chi volesse ESAGERARE:

Dalla VM Kali aprire con Remmina (non avendo possibilità di scaricare Remmina su kali userò Xfreerdp) una sessione RDP su Windows nella quale con il browser si deve raggiungere l'IP di Metasploitable.

Dopo “vari” tentativi, non trovano soluzioni di collegamento con xfreerdp sono passato a rdesktop



```
kali@kali: ~  
File Actions Edit View Help  
root@kali: /tmp kali@kali: ~  
(kali@kali)-[~]  
$ rdesktop -u Giuseppe -p password123 192.168.50.102  
Autoselecting keyboard map 'en-us' from locale  
Core(warning): Certificate received from server is NOT trusted by this system, an exception has been added by the user to trust this specific certificate.  
Failed to initialize NLA, do you have correct Kerberos TGT initialized ?  
Core(warning): Certificate received from server is NOT trusted by this system, an exception has been added by the user to trust this specific certificate.  
Connection established using SSL.  
Protocol(warning): process_pdu_logon(), Unhandled login infotype 1  
Clipboard(error): xclip_handle_SelectionNotify(), unable to find a textual target to satisfy RDP clipboard text request
```

Dopo aver utilizzato il comando, cerco semplicemente un browser ed essendo che tutte le macchine sono connesse tramite “rete interna” dalle impostazioni di virtual box, inserisco nella bara di ricerca di microsoft edge l’indirizzo IP della macchina Metasploitable 2. Il risultato è il seguente:

