

S1L1

Traccia:

L'esercizio di oggi consiste nella creazione e configurazione come da architettura di riferimento (sotto in figura) 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. Come detto la priorità sarà kali.

Requisiti:

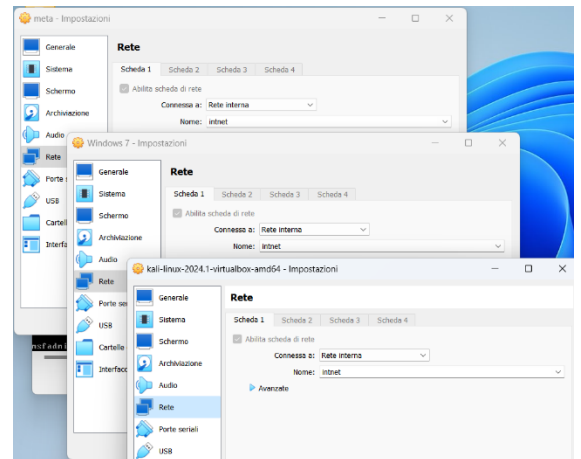
Si richiede allo studente di creare un laboratorio virtuale, con le seguenti caratteristiche:

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

Per la creazione del mio laboratorio virtuale, ho in primo luogo scaricato VirtualBox sul mio pc, o sistema operativo host; VirtualBox è invece il sistema operativo guest, ovvero un virtualizzatore che sarà in grado di leggere i formati .iso delle macchine virtuali Kali Linux, Windows7 e Metasploitable che andremo ad installare e diventeranno il nostro ambiente di test durante tutto il corso.

Kali è uno dei sistemi operativi più famosi ed utilizzati, è una distribuzione Linux creata ad hoc per i penetration testing. Utilizzeremo Kali come macchina attaccante e avremo a disposizione macchine volutamente vulnerabili che faranno da target: Metasploitable e Windows 7.

A destra lo screenshot dell'installazione delle macchine impostate con rete interna in quanto la traccia dell'esercizio richiedeva che le macchine virtuali non comunicassero con il sistema host. Mettere la rete in modalità interna consente la comunicazione tra le macchine virtuali ma non l'interazione con l'ambiente esterno; questo garantisce sicurezza ed evita l'esposizione sulla rete di macchine vulnerabili.



Dopo aver scaricato e installato le 3 vm, sono poi andata a configurare gli indirizzi ip statici ad ognuna di esse.

Per **Kali**, ho utilizzato il comando `sudo nano /etc/network/interfaces` e sono andata a impostare il mio indirizzo ip riavviando poi la macchina. Per controllare che le modifiche fossero state implementate, ho avviato il comando `ifconfig`, che mostra i dettagli dell'indirizzo ip e subnetmask come verificabile negli screen allegati sotto.

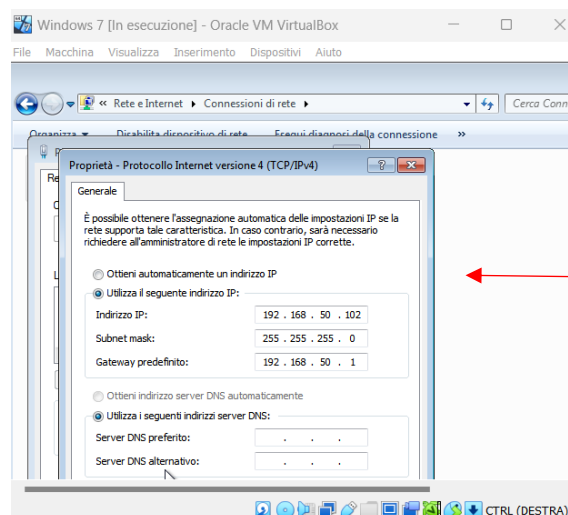
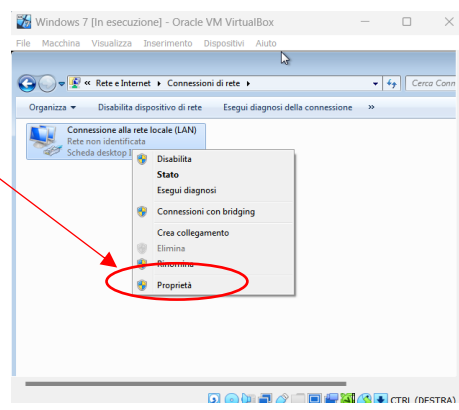
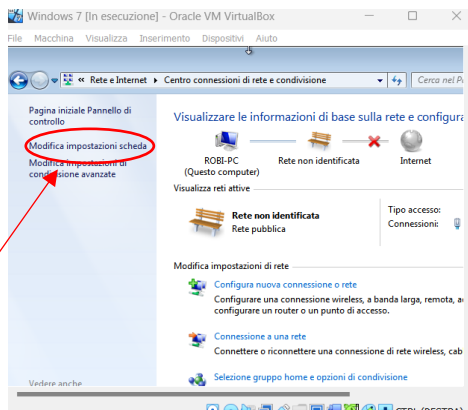
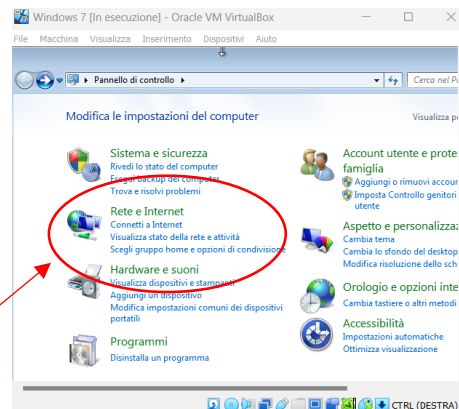
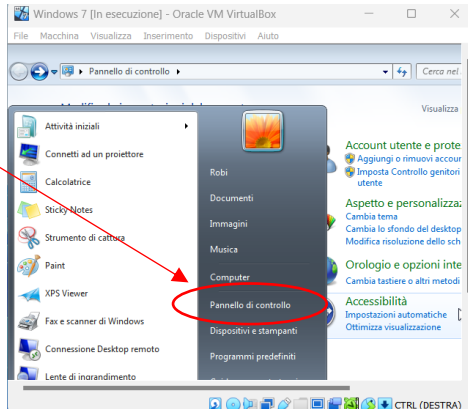
```
kali@kali: ~  
File Actions Edit View Help  
GNU nano 7.2 /etc/network/interfaces  
# This file describes the network interfaces available on your system  
# and how to activate them. For more information, see interfaces(5).  
  
source /etc/network/interfaces.d/*  
  
# The loopback network interface  
auto lo  
iface lo inet loopback  
auto eth0  
iface eth0 inet static  
address 192.168.50.100/24  
gateway 192.168.50.1
```

```
kali@kali: ~  
File Actions Edit View Help  
$ sudo nano /etc/network/interfaces  
[sudo] password for 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:fe1e:364a prefixlen 64 scopeid 0x20<link>  
ether 08:00:27:1e:36:4a txqueuelen 1000 (Ethernet)  
RX packets 296 bytes 31605 (30.8 KiB)  
RX errors 0 dropped 0 overruns 0 frame 0  
TX packets 21 bytes 2774 (2.7 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
```

Per quanto riguarda **Metasploitable**, il procedimento è stato lo stesso eseguito con Kali: dsl comando `sudo nano /etc/network/interfaces` sono andata ad inserire l'ip statico, ho riavviato la macchina e controllato che le modifiche fossero state salvate con `ifconfig`.

```
msfadmin@metasploitable:~$ ifconfig  
eth0  
Link encap:Ethernet HWaddr 08:00:27:3a:d6:e0  
inet addr:192.168.50.101 Bcast:192.168.50.255 Mask:255.255.255.0  
inet6 addr: fe80::a00:27ff:fe3a:d6e0/64 Scope:Link  
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1  
RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
TX packets:64 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:1000  
RX bytes:0 (0.0 B) TX bytes:4752 (4.6 KB)  
Base address:0xd010 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:117 errors:0 dropped:0 overruns:0 frame:0  
TX packets:117 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:0  
RX bytes:25129 (24.5 KB) TX bytes:25129 (24.5 KB)  
msfadmin@metasploitable:~$
```

La configurazione dell'ip statico di **Windows 7** invece è stata completamente diversa: in primo luogo ho aperto il pannello di controllo, selezionato Rete e Internet, Modifica impostazioni scheda, proprietà, e da lì si è aperta la finestra per impostare l'ip come verificabile nella sequenza di screenshots allegata sotto.



A seguito della configurazione degli ip su tutte le macchine, ho verificato con il comando `ping indirizzo_ip` che le vm comunicassero tra loro.

```
kali@kali:~  
File Actions Edit View Help  
TX packets 4 bytes 240 (240.0 B)  
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
[kali@kali]~$ ping 192.168.50.101  
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=6.40 ms  
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=2.56 ms  
64 bytes from 192.168.50.101: icmp_seq=3 ttl=64 time=0.730 ms  
64 bytes from 192.168.50.101: icmp_seq=4 ttl=64 time=0.502 ms  
64 bytes from 192.168.50.101: icmp_seq=5 ttl=64 time=12.0 ms  
64 bytes from 192.168.50.101: icmp_seq=6 ttl=64 time=1.09 ms  
64 bytes from 192.168.50.101: icmp_seq=7 ttl=64 time=0.594 ms  
64 bytes from 192.168.50.101: icmp_seq=8 ttl=64 time=1.05 ms  
64 bytes from 192.168.50.101: icmp_seq=9 ttl=64 time=1.34 ms  
64 bytes from 192.168.50.101: icmp_seq=10 ttl=64 time=1.25 ms  
64 bytes from 192.168.50.101: icmp_seq=11 ttl=64 time=1.07 ms  
64 bytes from 192.168.50.101: icmp_seq=12 ttl=64 time=2.87 ms  
64 bytes from 192.168.50.101: icmp_seq=13 ttl=64 time=0.746 ms  
^C  
--- 192.168.50.101 ping statistics ---  
13 packets transmitted, 13 received, 0% packet loss, time 12205ms  
rtt min/avg/max/mdev = 0.502/2.547/12.897/3.354 ms  
[kali@kali]~$
```