

Laboratorio Virtuale

In questo esercizio andremo a creare il nostro laboratorio virtuale.

E' necessario aver installato, in questo caso su VirtualBox, i sistemi operativi di Windows 10, Metasploitable2 e Kali Linux.

Una volta aver creato correttamente le macchine virtuali dobbiamo impostarle di Rete Interna, in modo che solo le macchine virtuali possano comunicare tra di loro, ma non abbiano accesso né alla rete esterna, né all'Host. Questo serve a tenere le macchine isolate e creare un ambiente sicuro in cui possiamo lavorare senza pericoli esterni, o creare problemi all'Host. Per farlo dobbiamo andare a cambiare le impostazioni della scheda di rete di ogni Vm, e selezionare su “rete interna”.

Ora andremo ad impostare gli indirizzi Ip in ogni Vm, e lo faremo in questo modo:

Kali: 192.168.50.100/24

Meta: 192.168.50.101/24

Windows: 192.168.50.102/24

Meta:

Prima di iniziare ho impostato la tastiera su lingua italiana. Per farlo ho lanciato il comando `sudo loadkeys it`.

Poi procediamo ad aprire l'interfaccia di rete, tramite il comando:

`sudo nano /etc/network/interfaces`, e si apre questa schermata.

(sudo= permessi di amministratore, nano= aprire come editor di testo).

Andremo a modificare iface eth0 inet Static, e inseriamo le seguenti impostazioni:

address 192.168.50.101

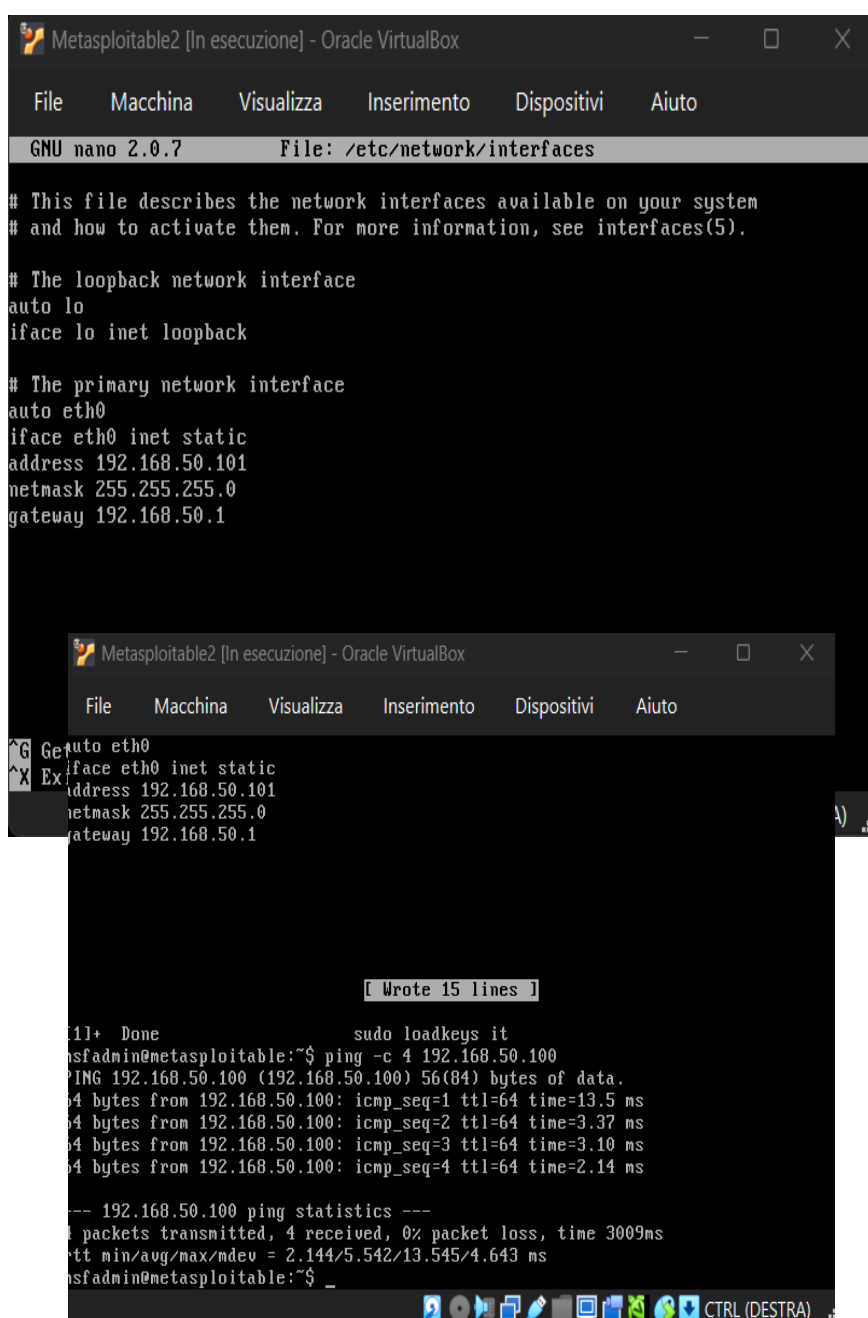
netmask 255.255.255.0

gateway 192.168.50.1

e facciamo Ctrl+X per uscire.

Poi con il comando “`/etc/init.d/networking restart`” si riavvia scheda di rete.

Una volta fatto possiamo eseguire dei test, facendo “ip a” per verificare la nostra rete, e `ping -c 4 192.168.50.100` per provare a pingare la Vm di Kali con 4 pacchetti.



The image shows two screenshots from a Metasploitable2 virtual machine running in Oracle VM VirtualBox. The top screenshot shows the `/etc/network/interfaces` file being edited with nano. The configuration for `eth0` is set to static with IP 192.168.50.101, netmask 255.255.255.0, and gateway 192.168.50.1. The bottom screenshot shows the terminal output after running `ip a` and `ping -c 4 192.168.50.100`. The `ip a` command shows the `eth0` interface is up and has the correct IP address. The ping command shows successful results with 0% packet loss.

```
Metasploitable2 [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

GNU nano 2.0.7  File: /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.50.101
netmask 255.255.255.0
gateway 192.168.50.1

^G Get auto eth0
^X Ex iface eth0 inet static
address 192.168.50.101
netmask 255.255.255.0
gateway 192.168.50.1

[ Wrote 15 lines ]

11+ Done sudo loadkeys it
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=13.5 ms
64 bytes from 192.168.50.100: icmp_seq=2 ttl=64 time=3.37 ms
64 bytes from 192.168.50.100: icmp_seq=3 ttl=64 time=3.10 ms
64 bytes from 192.168.50.100: icmp_seq=4 ttl=64 time=2.14 ms

--- 192.168.50.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3009ms
rtt min/avg/max/mdev = 2.144/5.542/13.545/4.643 ms
msfadmin@metasploitable:~$
```

Kali:

Anche qui possiamo impostare la tastiera italiana. Avendo Kali un interfaccia grafica è più semplice: si va a cercare sui programmi “Keyboard”, e andiamo ad impostare su Italian.

Per impostare la rete facciamo tasto destro sull'icona di rete nella barra delle applicazioni, e fare “Edit connections”.

Aprire le impostazioni e settarla in questo modo:

Address 192.168.50.100;

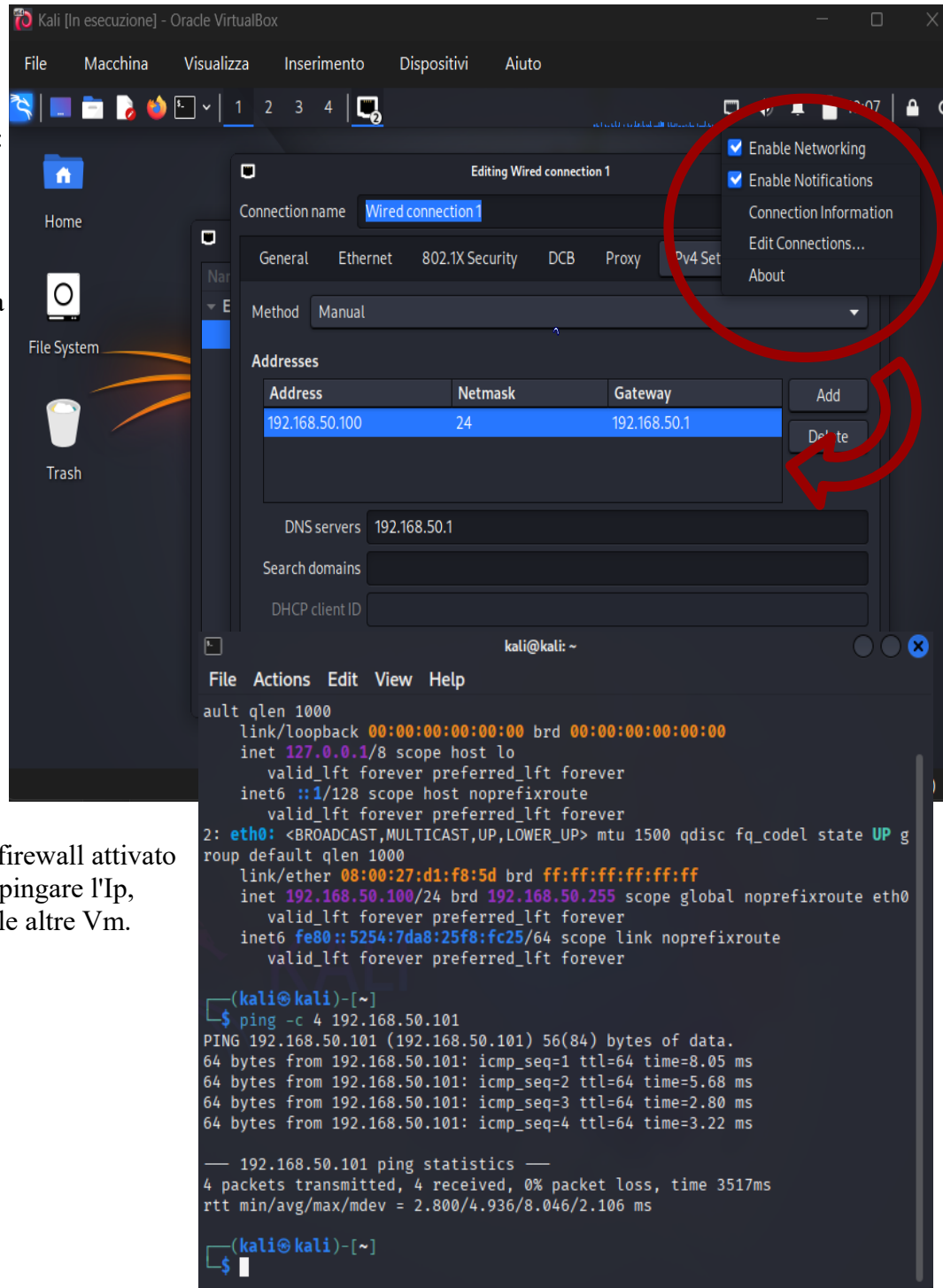
Netmask 24;

Gateway 192.168.50.1;

DNS servers 192.168.50.1

Anche qui possiamo verificare facendo “ip a”, e provando a pingare Meta.

Nota. se su Windows abbiamo il firewall attivato potremmo non essere in grado di pingare l'Ip, mentre Windows può farlo verso le altre Vm.



Windows 10

Su Windows andiamo tramite il pannello di controllo a modificare le impostazioni della scheda di rete.

Aprendo la schermata del protocollo di rete Ipv4,

andiamo ad impostare la nostra Vm in questo modo:

Ip 192.168.50.102;

Subnet mask 255.255.255.0;

Gateway 192.168.50.1;

DNS predefinito 192.168.50.1

Anche qui, andiamo ad effettuare una prova pingando un'altra Vm

Proprietà - Protocollo Internet versione 4 (TCP/IPv4)

Generale

È possibile ottenere l'assegnazione automatica delle impostazioni IP se la rete supporta tale caratteristica. In caso contrario, sarà necessario richiedere all'amministratore di rete le impostazioni IP corrette.

☐ Ottieni automaticamente un indirizzo IP

☒ Utilizza il seguente indirizzo IP:

Indirizzo IP: 192 . 168 . 50 . 102

Subnet mask: 255 . 255 . 255 . 0

Gateway predefinito: 192 . 168 . 50 . 1

☐ Ottieni indirizzo server DNS automaticamente

☒ Utilizza i seguenti indirizzi server DNS:

DNS preferito: 192 . 168 . 50 . 1

DNS alternativo: . . .

valida impostazioni all'uscita

Avanzate...

OK

Annulla

Seleziona Prompt dei comandi

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=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 = 1ms, Massimo = 2ms, Medio = 1ms

C:\Users\user>_

Eseguendo il comando "nmap" ed inserendo l'intervallo che ci interessa possiamo anche andare a fare una mappatura della rete, andando a verificare quali indirizzi Ip sono attivi in rete.

Kali [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

1 2 3 4

Home

File System

Trash

kali@kali: ~

File Actions Edit View Help

Not shown: 1000 closed tcp ports (reset)

Nmap scan report for 192.168.50.101

Host is up (0.00042s latency).

Not shown: 977 closed tcp ports (reset)

PORT	STATE	SERVICE
21/tcp	open	ftp
22/tcp	open	ssh
23/tcp	open	telnet
25/tcp	open	smtp
53/tcp	open	domain
80/tcp	open	http
111/tcp	open	rpcbind
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds
512/tcp	open	exec
513/tcp	open	login
514/tcp	open	shell
1099/tcp	open	rmiregistry
1524/tcp	open	ingreslock
2049/tcp	open	nfs
2121/tcp	open	ccproxy-ftp
3306/tcp	open	mysql
5432/tcp	open	postgresql
5900/tcp	open	vnc
6000/tcp	open	X11
6667/tcp	open	irc
8009/tcp	open	ajp13
8180/tcp	open	unknown

MAC Address: 08:00:27:4E:32:53 (PCS Systemtechnik/Oracle VM VirtualBox virtual NIC)

Nmap scan report for 192.168.50.102

Host is up (0.00068s latency).

Not shown: 982 closed tcp ports (reset)

PORT	STATE	SERVICE
7/tcp	open	echo
9/tcp	open	discard

CTRL (DESTRA)

E' possibile anche ad andare a creare un “punto di salvataggio” della nostra macchina virtuale, chiamato **recovery**, in cui andiamo a clonare la macchina assicurandoci di avere un backup qualora si verificasse qualche problema con la macchina.

Possiamo anche andare ad effettuare un test creando un file esempio sul desktop, e poi eseguire il clone della Vm. Se poi sulla macchina principale andiamo ad eliminare quel file possiamo vedere come rimanga comunque salvato all'interno della macchina clone, evitando in questo caso la perdita di dati.

