

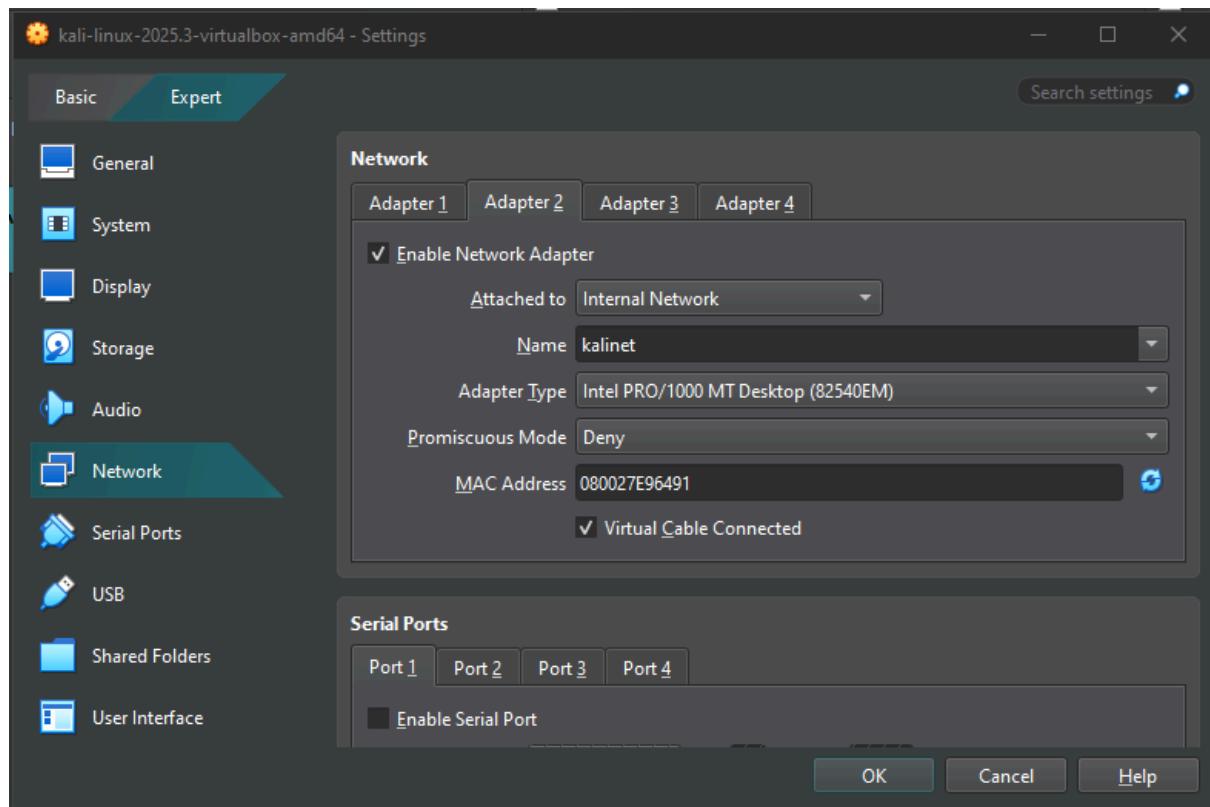
# Report S3 L5

## Configurazione Firewall

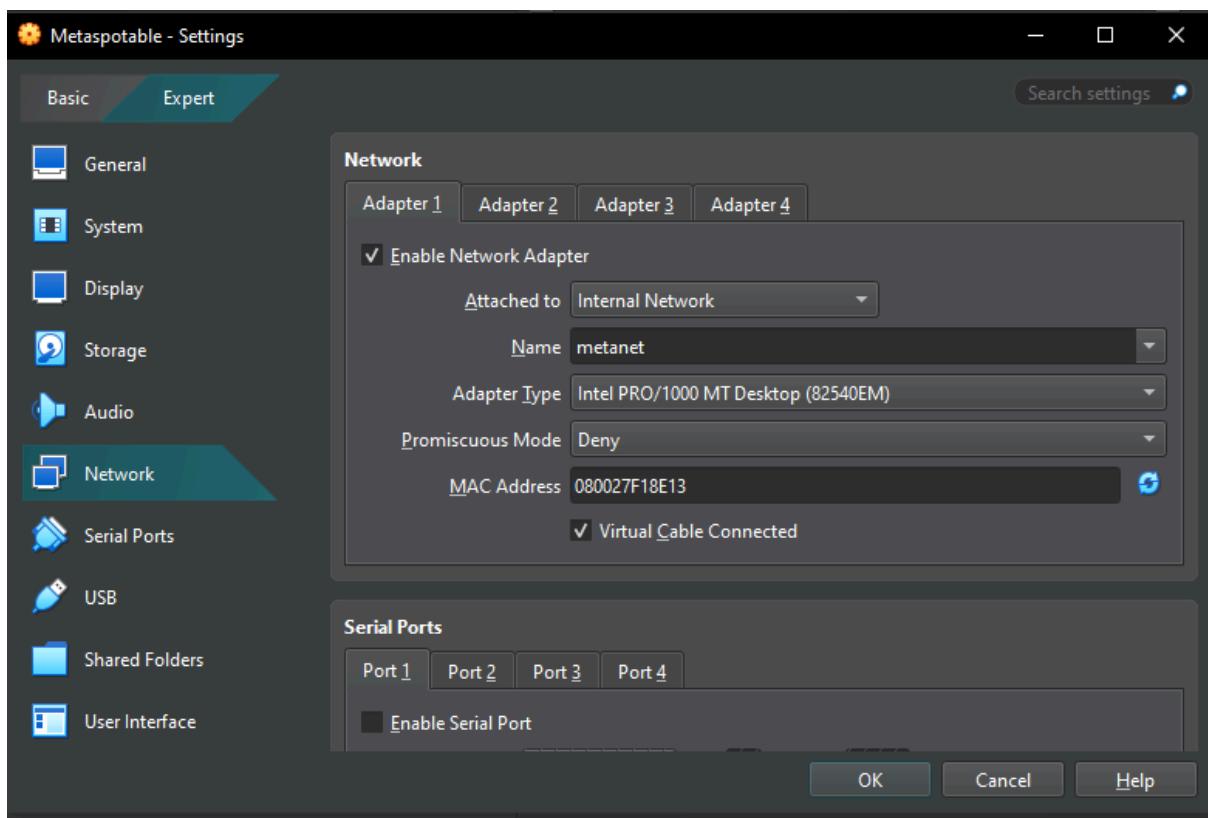
### 1.0 Configurazione iniziale VM

Come primo step andiamo a configurare le **schede di rete** di tutte le **macchine virtuali** che andremo ad utilizzare oggi.

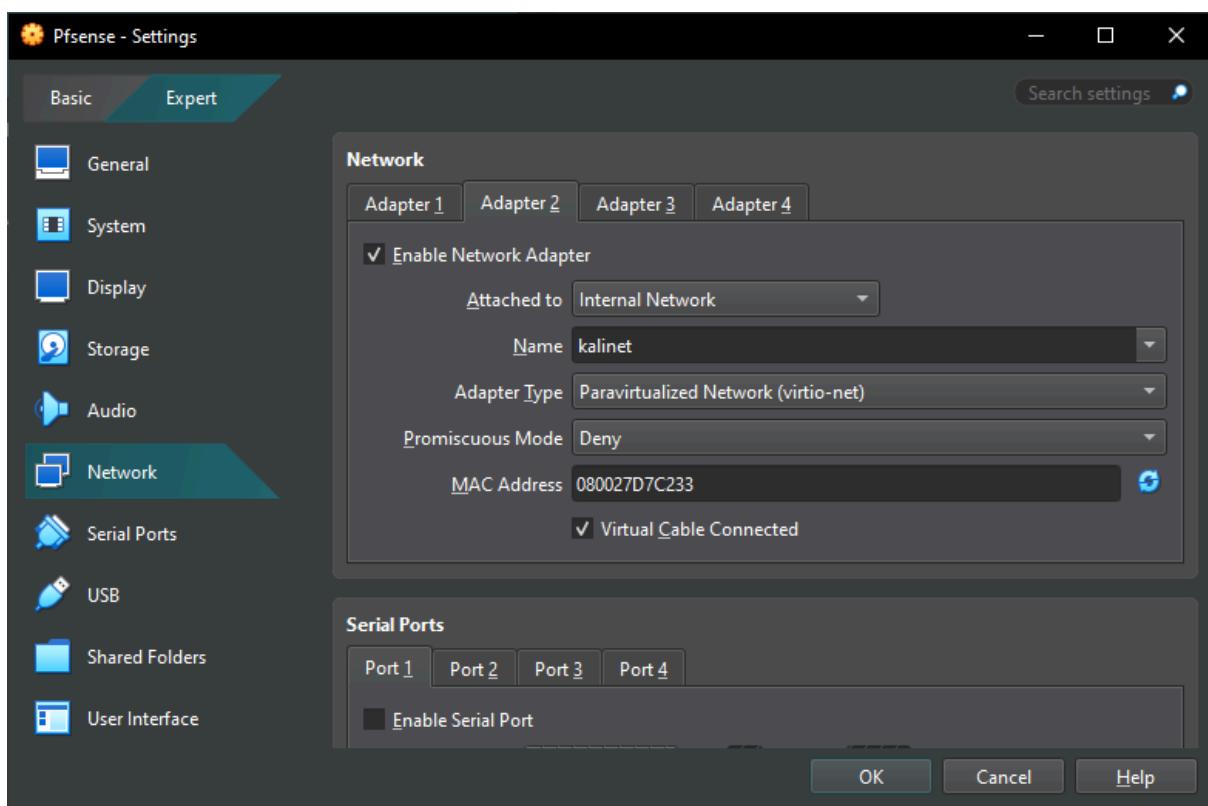
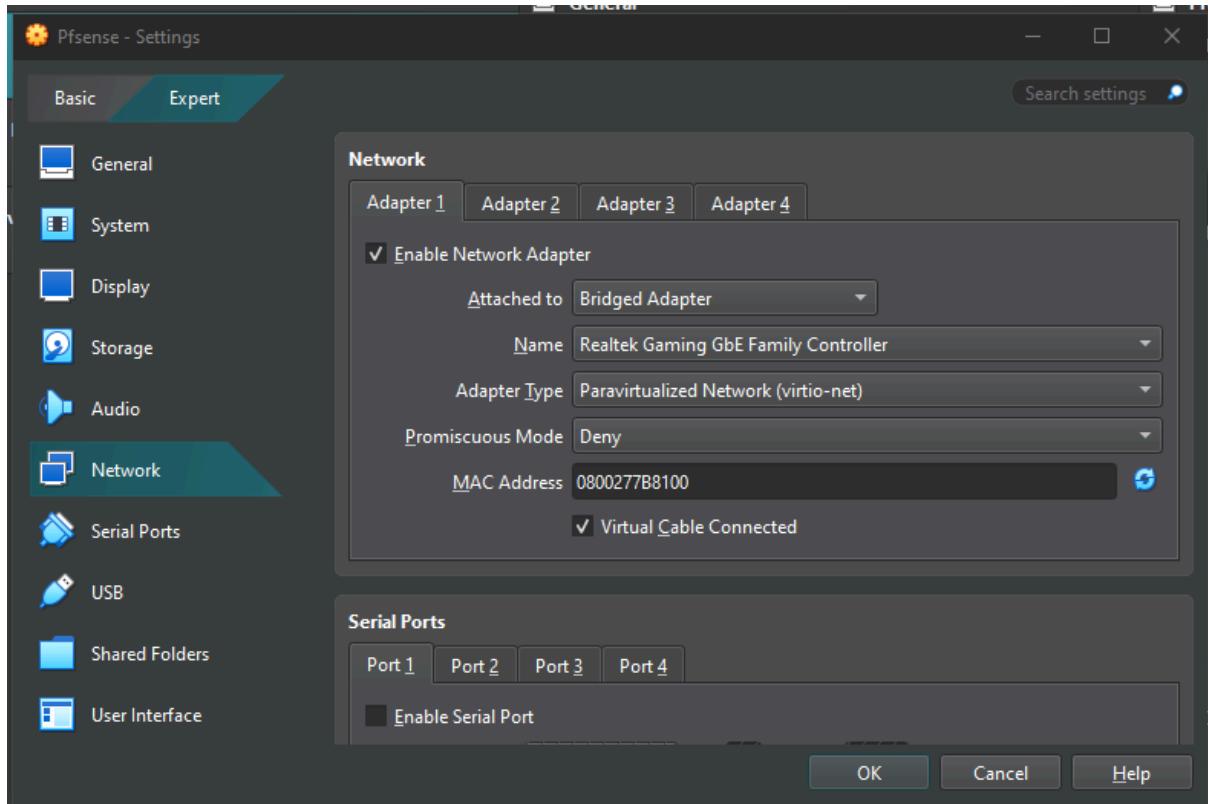
- La kali si troverà sulla rete interna “**kalinet**”

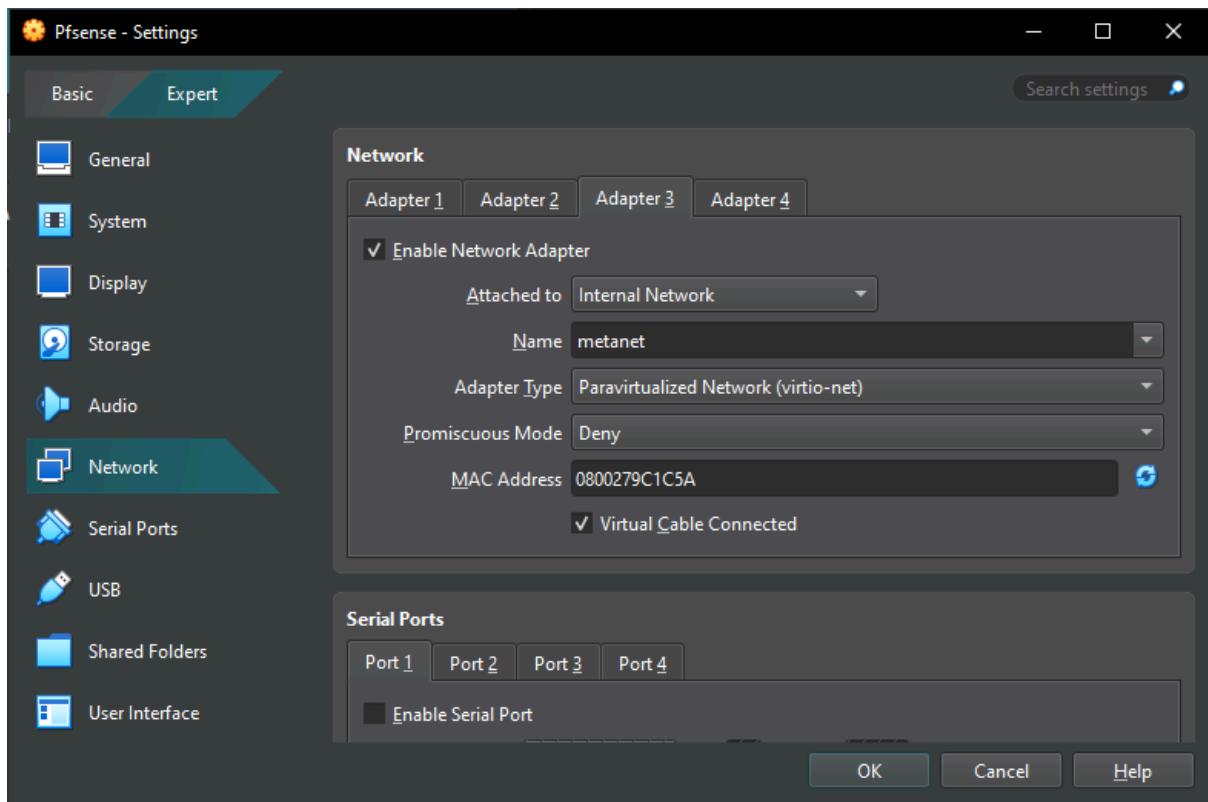


- La metasploitable si troverà sulla rete interna “**metanet**”



- Per la VM Pfsense andiamo ad impostare 3 schede di rete:
  - la scheda **WAN** collegata al nostro router di casa
  - la scheda **LAN** collegata alla rete **kalinet**
  - la scheda **OPT1** collegata alla rete **metanet**

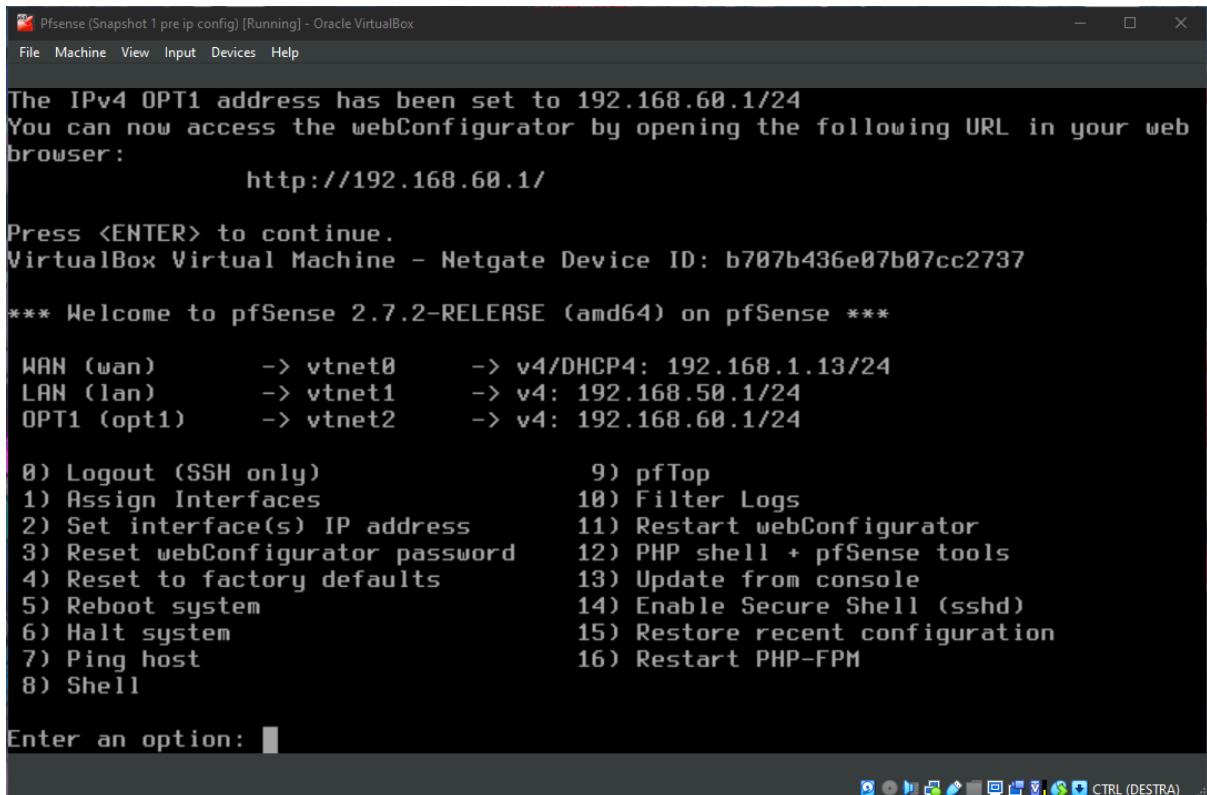




## 2.0 Configurazione IP PfSense

Apriamo PfSense e andiamo a configurare le 3 interfacce, assegnando i seguenti IP:

- WAN → configurata in **DHCP** tramite il router di casa
- LAN → configurata come ip statico **192.168.50.1/24**, fornisce il servizio **DHCP** alle macchine connesse
- OPT1 → configurata come ip statico **192.168.60.1/24**, fornisce il servizio **DHCP** alle macchine connesse



The IPv4 OPT1 address has been set to 192.168.60.1/24  
You can now access the webConfigurator by opening the following URL in your web browser:  
<http://192.168.60.1/>

Press <ENTER> to continue.  
VirtualBox Virtual Machine - Netgate Device ID: b707b436e07b07cc2737

\*\*\* Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense \*\*\*

WAN (wan) -> vtnet0 -> v4/DHCP4: 192.168.1.13/24  
LAN (lan) -> vtnet1 -> v4: 192.168.50.1/24  
OPT1 (opt1) -> vtnet2 -> v4: 192.168.60.1/24

0) Logout (SSH only) 9) pfTop  
1) Assign Interfaces 10) Filter Logs  
2) Set interface(s) IP address 11) Restart webConfigurator  
3) Reset webConfigurator password 12) PHP shell + pfSense tools  
4) Reset to factory defaults 13) Update from console  
5) Reboot system 14) Enable Secure Shell (sshd)  
6) Halt system 15) Restore recent configuration  
7) Ping host 16) Restart PHP-FPM  
8) Shell

Enter an option: █

CTRL (DESTRA) █

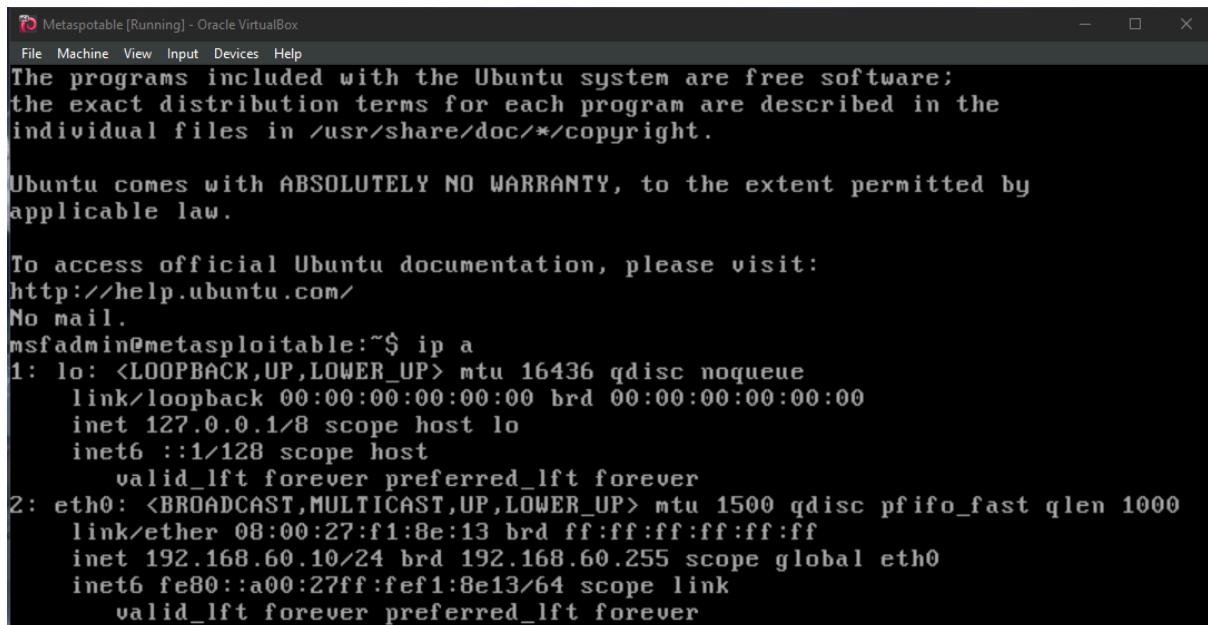
### 3.0 Controllo connessione

Una volta configurato Pfsense apriamo le VM per controllare se sono collegate correttamente

```
(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:e9:64:91 brd ff:ff:ff:ff:ff:ff
        inet 192.168.50.10/24 brd 192.168.50.255 scope global dynamic noprefixroute eth0
            valid_lft 7161sec preferred_lft 7161sec
        inet6 fe80::e8c0:84eb:820:9942/64 scope link noprefixroute
            valid_lft forever preferred_lft forever

(kali㉿kali)-[~]
$ ping google.com
PING google.com (216.58.204.238) 56(84) bytes of data.
64 bytes from par21s06-in-f14.1e100.net (216.58.204.238): icmp_seq=1 ttl=113 time=12.3 ms
64 bytes from par21s06-in-f14.1e100.net (216.58.204.238): icmp_seq=2 ttl=113 time=11.5 ms
64 bytes from par21s06-in-f14.1e100.net (216.58.204.238): icmp_seq=3 ttl=113 time=12.0 ms
64 bytes from par21s06-in-f14.1e100.net (216.58.204.238): icmp_seq=4 ttl=113 time=12.0 ms
64 bytes from par21s06-in-f14.1e100.net (216.58.204.238): icmp_seq=5 ttl=113 time=11.4 ms
^C
--- google.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 11.370/11.839/12.288/0.335 ms
```

La kali ha ricevuto l'indirizzo IP 192.168.50.10 tramite DHCP e pingando google riusciamo a vedere che ha accesso a internet



```
Metasploitable [Running] - Oracle VirtualBox
File Machine View Input Devices Help
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.

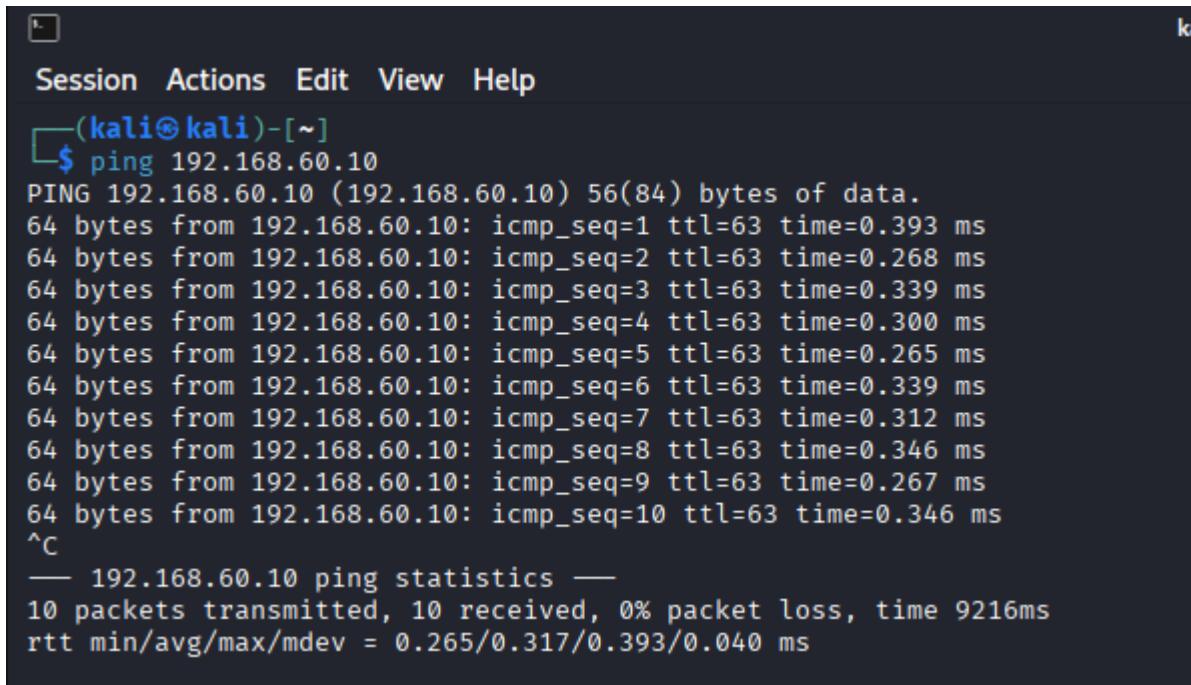
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:f1:8e:13 brd ff:ff:ff:ff:ff:ff
        inet 192.168.60.10/24 brd 192.168.60.255 scope global eth0
            valid_lft forever preferred_lft forever
```

La metasploitable ha ricevuto l'indirizzo IP 192.168.60.10 tramite DHCP

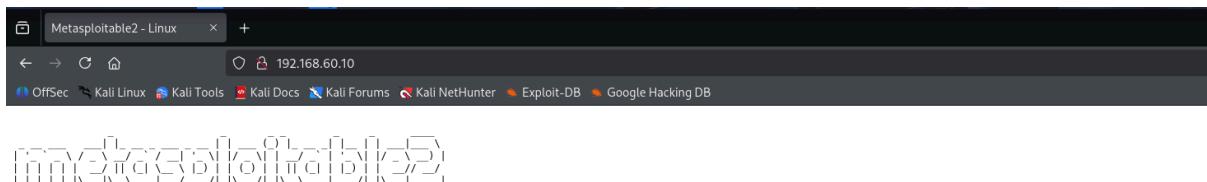
## 4.0 Verifica funzionamento firewall

### 4.1 Pre configurazione Firewall

Prima di impostare il firewall andiamo a verificare se le 2 macchine comunicano



```
(kali㉿kali)-[~]
$ ping 192.168.60.10
PING 192.168.60.10 (192.168.60.10) 56(84) bytes of data.
64 bytes from 192.168.60.10: icmp_seq=1 ttl=63 time=0.393 ms
64 bytes from 192.168.60.10: icmp_seq=2 ttl=63 time=0.268 ms
64 bytes from 192.168.60.10: icmp_seq=3 ttl=63 time=0.339 ms
64 bytes from 192.168.60.10: icmp_seq=4 ttl=63 time=0.300 ms
64 bytes from 192.168.60.10: icmp_seq=5 ttl=63 time=0.265 ms
64 bytes from 192.168.60.10: icmp_seq=6 ttl=63 time=0.339 ms
64 bytes from 192.168.60.10: icmp_seq=7 ttl=63 time=0.312 ms
64 bytes from 192.168.60.10: icmp_seq=8 ttl=63 time=0.346 ms
64 bytes from 192.168.60.10: icmp_seq=9 ttl=63 time=0.267 ms
64 bytes from 192.168.60.10: icmp_seq=10 ttl=63 time=0.346 ms
^C
--- 192.168.60.10 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9216ms
rtt min/avg/max/mdev = 0.265/0.317/0.393/0.040 ms
```



Come possiamo vedere dalle immagini la Kali riesce a pingare e a visitare con successo il sito della metasploitable.

Il firewall ha le seguenti regole per le interfacce:

**Firewall / Rules / WAN**

Floating   WAN   LAN   OPT1

**Rules (Drag to Change Order)**

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
X 0/17 Kib	*	RFC 1918 networks	*	*	*	*	*		Block private networks	
X 0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	

No rules are currently defined for this interface  
All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.

Add Add Delete Toggle Copy Save Separator

**Firewall / Rules / LAN**

Floating   WAN   LAN   OPT1

**Rules (Drag to Change Order)**

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 0/448 Kib	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
✓ 2/1.57 MIB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
✓ 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add Add Delete Toggle Copy Save Separator

**Firewall / Rules / OPT1**

Floating   WAN   LAN   OPT1

**Rules (Drag to Change Order)**

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
X 0/18 Kib	*	RFC 1918 networks	*	*	*	*	*		Block private networks	
X 0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	

No rules are currently defined for this interface  
All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.

## 4.1 Dopo configurazione Firewall

Ora andiamo a inserire la regola sulla **LAN** che non consente più alla kali di visitare il sito sulla metasploitable

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓ 1/577 KIB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✗ 0/0 B	IPv4 TCP	192.168.50.10	*	192.168.60.10	80 (HTTP)	*	none		Block LAN HTTP to metasploitable	
<input type="checkbox"/>	✓ 4/1.65 MIB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	✓ 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

↑ Add ↓ Add Delete Toggle Copy Save + Separator

In questo modo la kali non può più raggiungere il sito della metasploitable, digitando l'IP sul browser la pagina andrà in time out

The connection has timed out

The server at 192.168.60.10 is taking too long to respond.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the web.

Try Again

Per quanto riguarda il **PING** il comando ha successo visto che la nuova regola blocca lo scambio dati sulla porta 80, il protocollo ICMP non utilizza una porta

```
(kali㉿kali)-[~]
$ ping 192.168.60.10
PING 192.168.60.10 (192.168.60.10) 56(84) bytes of data.
64 bytes from 192.168.60.10: icmp_seq=1 ttl=63 time=0.370 ms
64 bytes from 192.168.60.10: icmp_seq=2 ttl=63 time=0.315 ms
64 bytes from 192.168.60.10: icmp_seq=3 ttl=63 time=0.299 ms
64 bytes from 192.168.60.10: icmp_seq=4 ttl=63 time=0.307 ms
64 bytes from 192.168.60.10: icmp_seq=5 ttl=63 time=0.346 ms
^C
--- 192.168.60.10 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4100ms
rtt min/avg/max/mdev = 0.299/0.327/0.370/0.026 ms

(kali㉿kali)-[~]
$
```