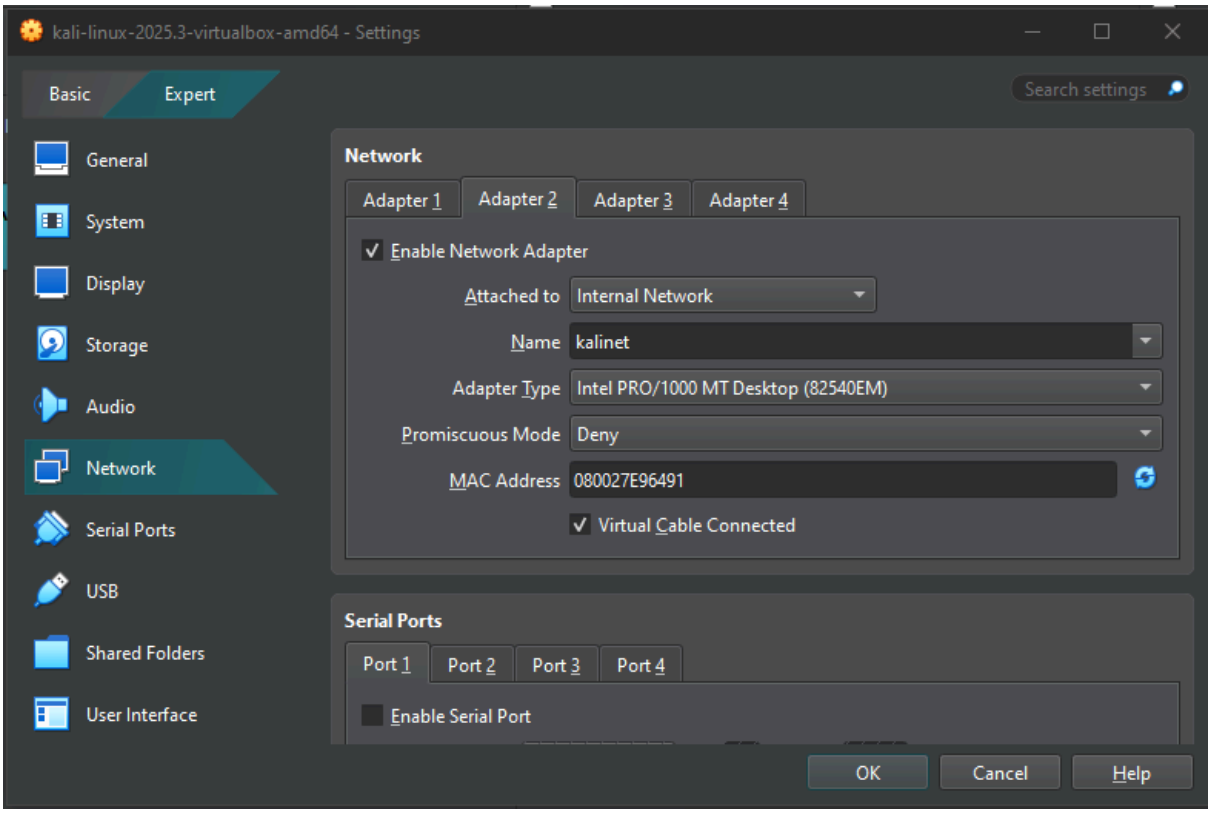
Report S3 L5

Configurazione Firewall

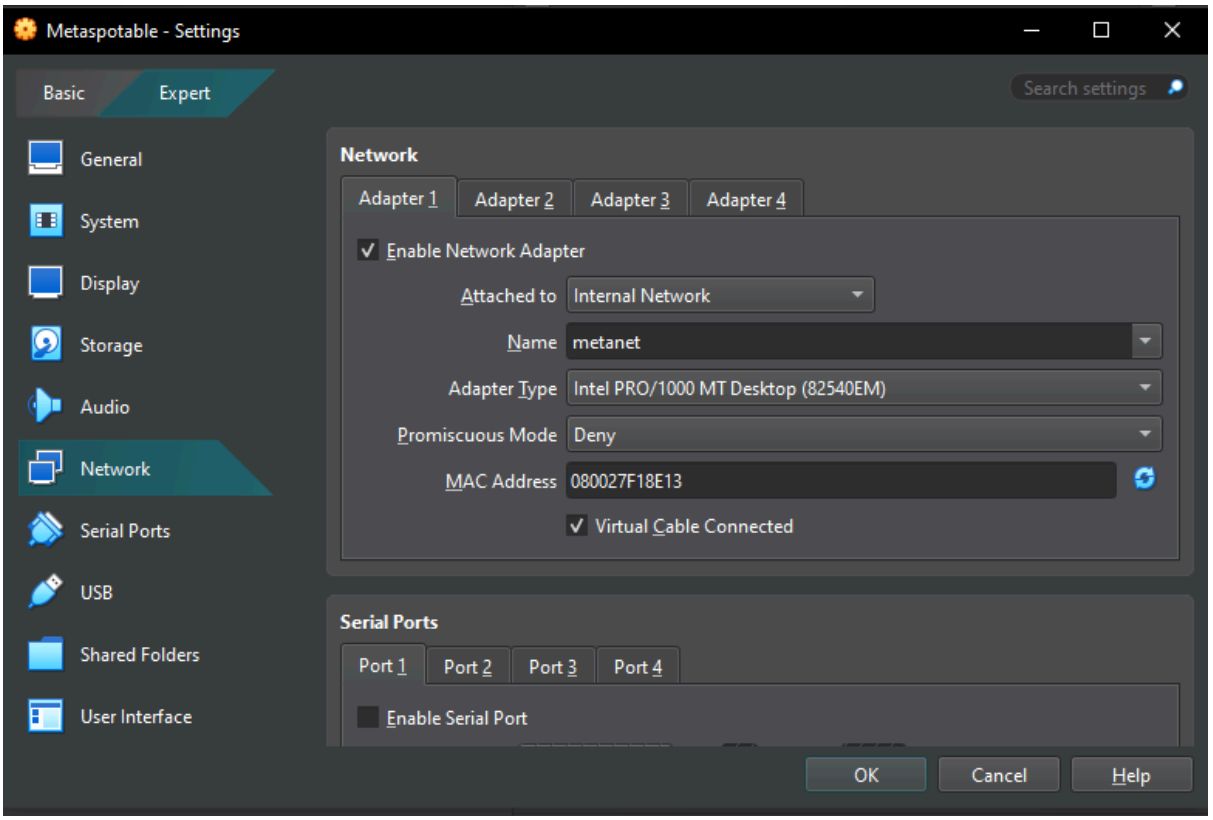
1.0 Configurazione iniziale VM

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

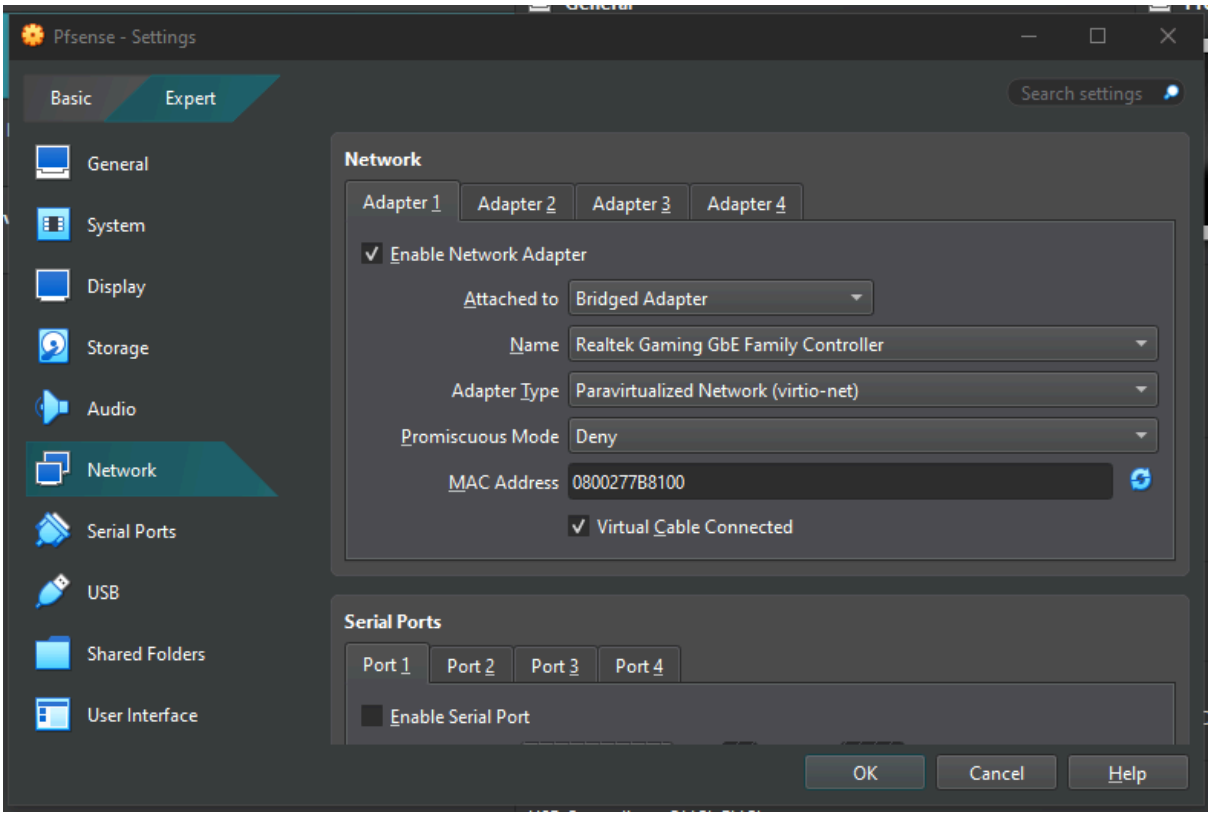
- La kali si troverà sulla rete interna “**kalinet**”

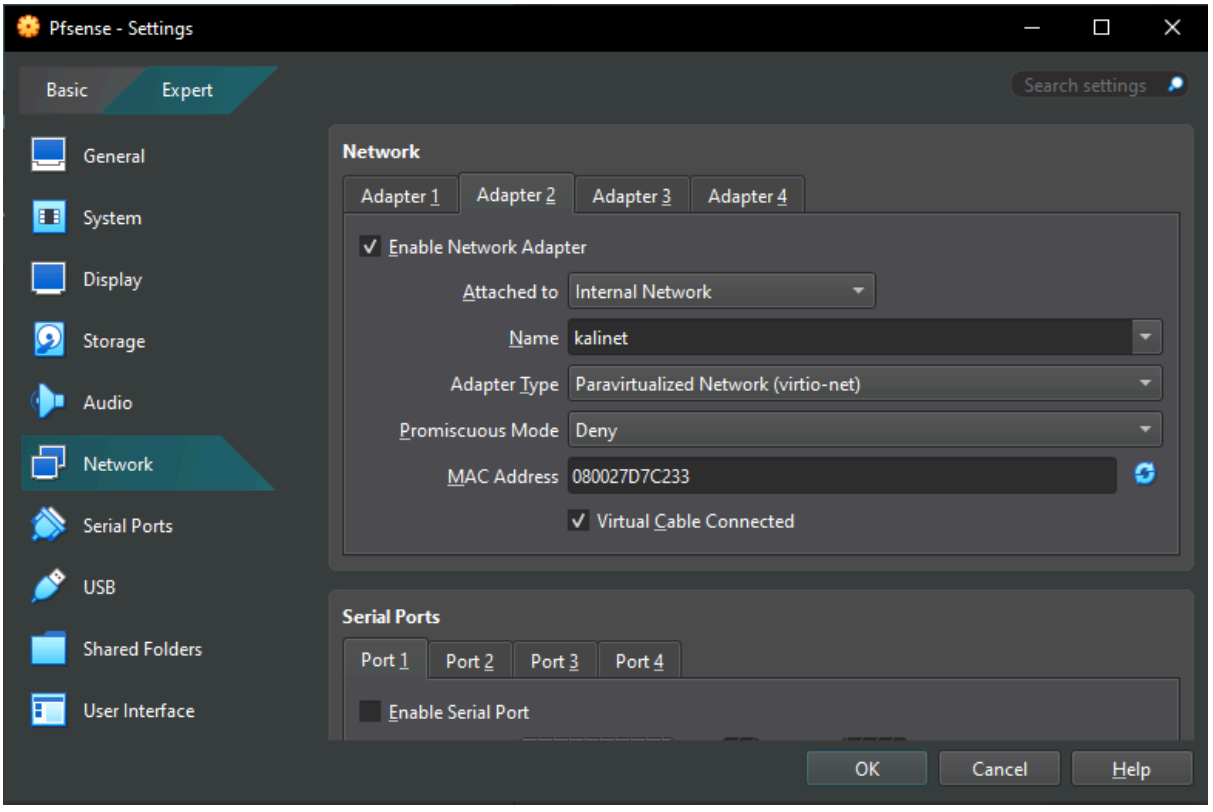


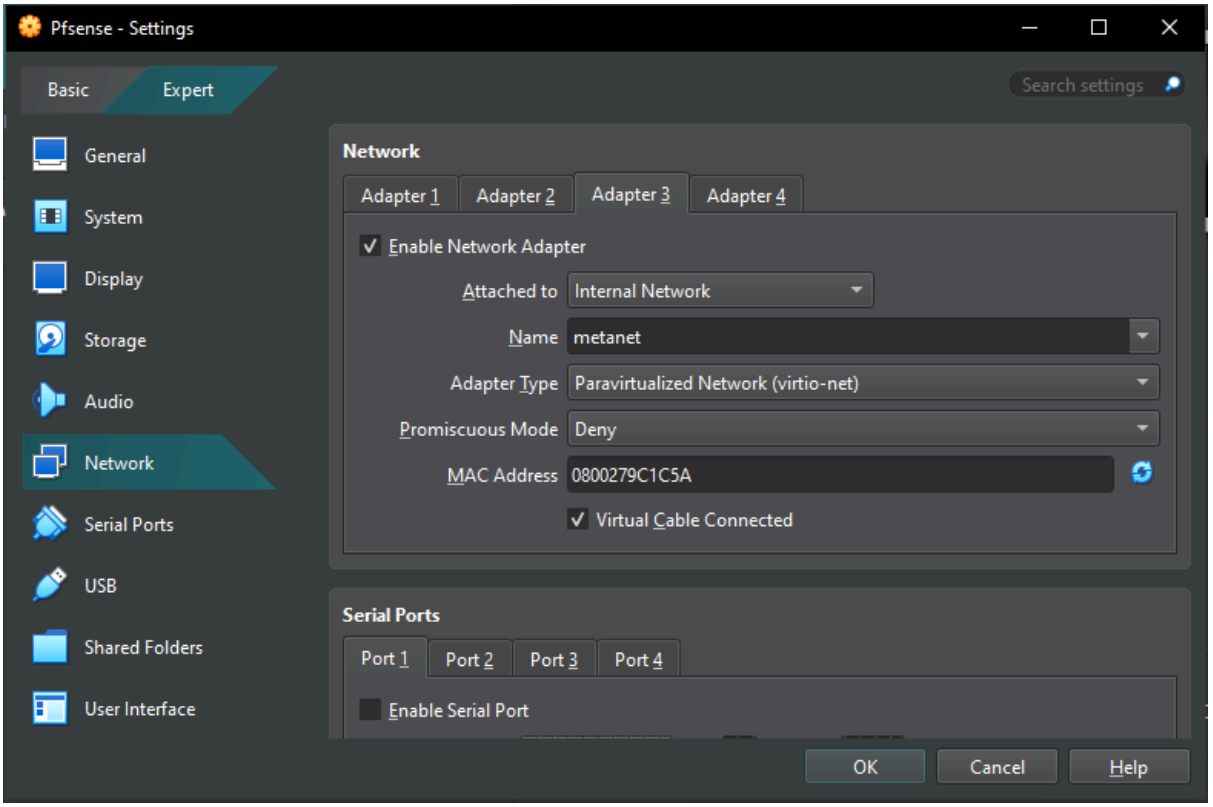
- La metasploitable si troverà sulla rete interna “**metanet**”



- 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**



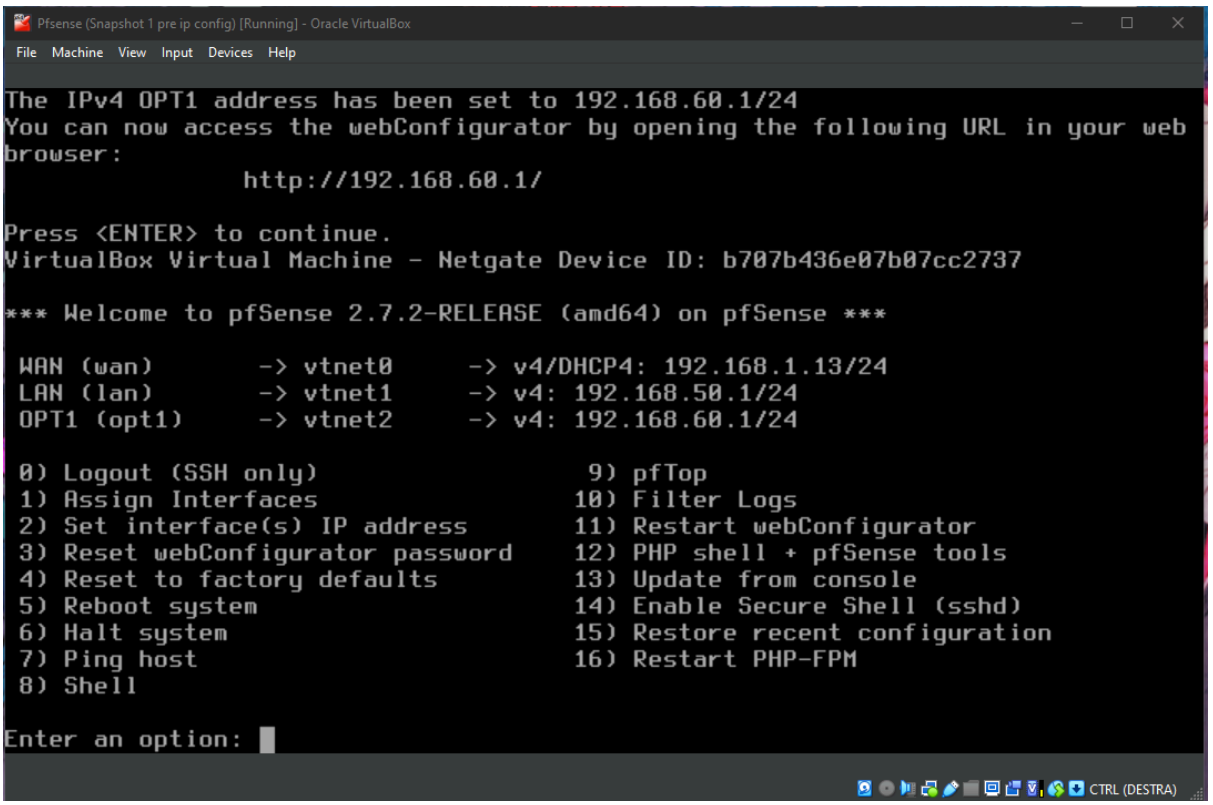



Pfsense - Settings
Basic
Expert
Search settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to
Internal Network
Name
metanet
Adapter Type
Paravirtualized Network (virtio-net)
Promiscuous Mode
Deny
MAC Address
0800279C1C5A
Virtual Cable Connected
Serial Ports
Port 1
Port 2
Port 3
Port 4
Enable Serial Port
OK
Cancel
Help

2.0 Configurazione IP Pfsense

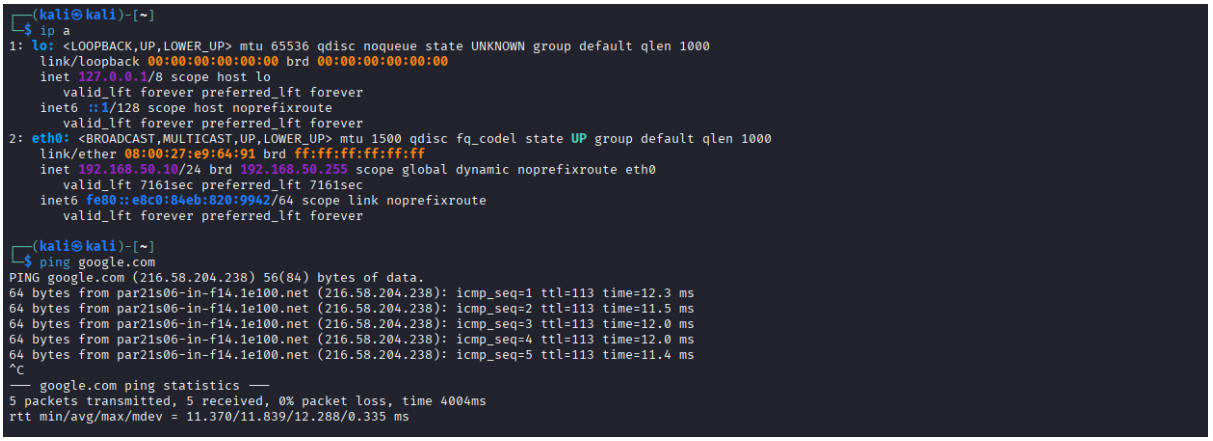
Apriamo Pfsense e andiamo a configurare le 3 interfacce, assegnando i seguenti IP:

- WAN → configurata in **DHCP** tramite il router di casa
- LAN → configurata come ip statico 1**92.168.50.1/24**, fornisce il servizio **DHCP** alle macchine connesse
- OPTI1 → configurata come ip statico 1**92.168.60.1/24**, fornisce il servizio **DHCP** alle macchine connesse

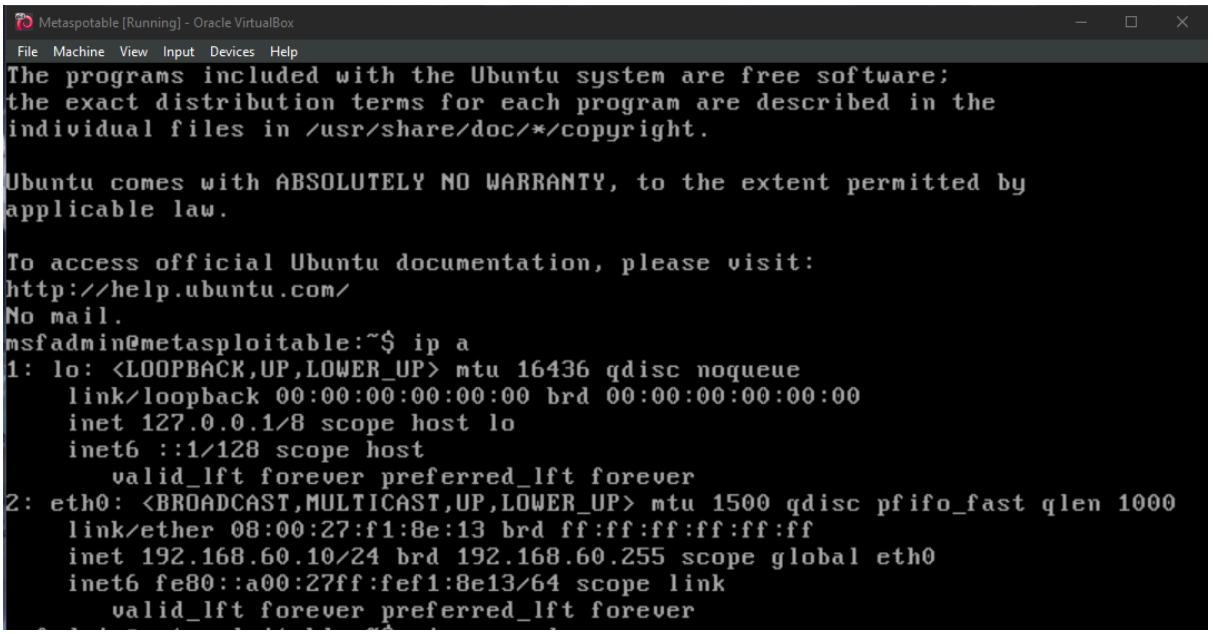


3.0 Controllo connessione

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



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

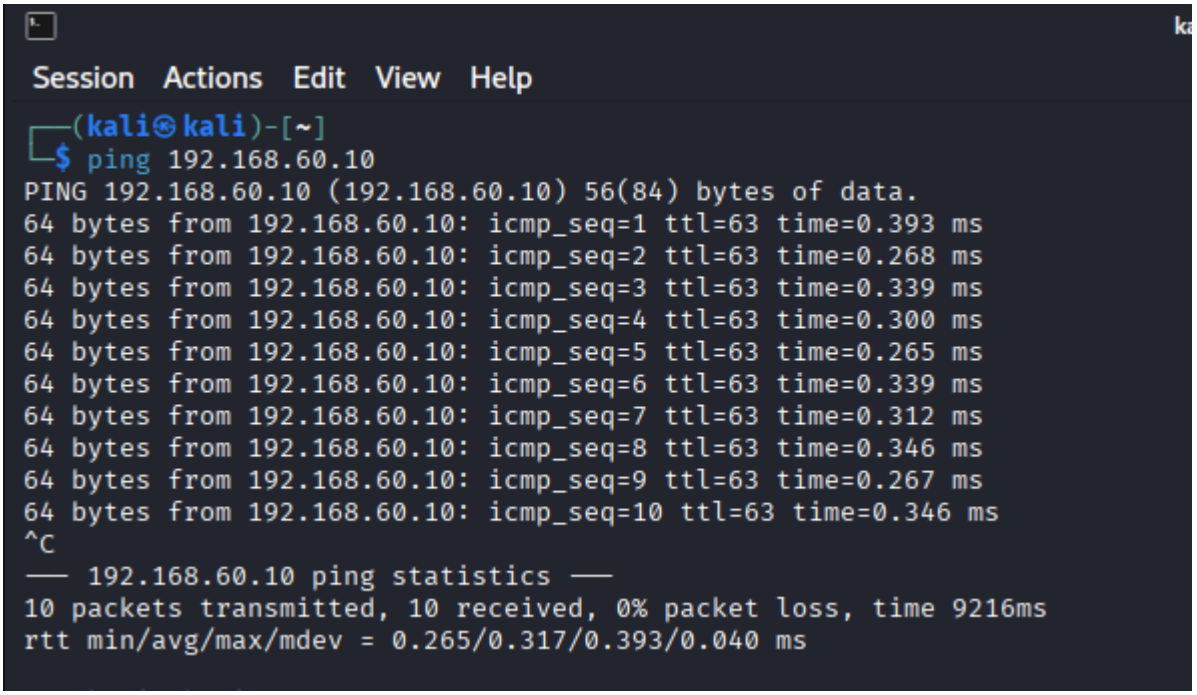


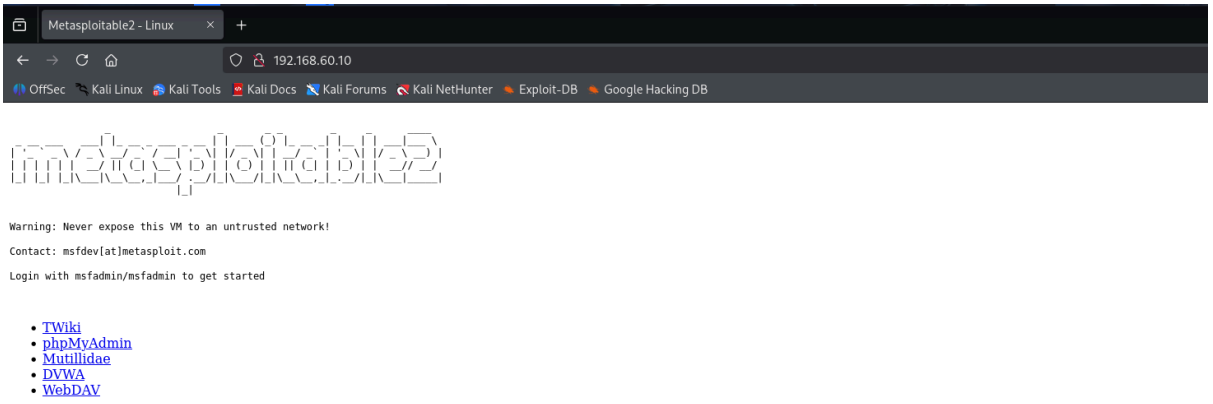
La metasploitable ha ricevuto l’indirizzo IP 192.168.60.10 tramite DHCP

4.0 Verifica funzionamento firewall

4.1 Pre configurazione Firewall

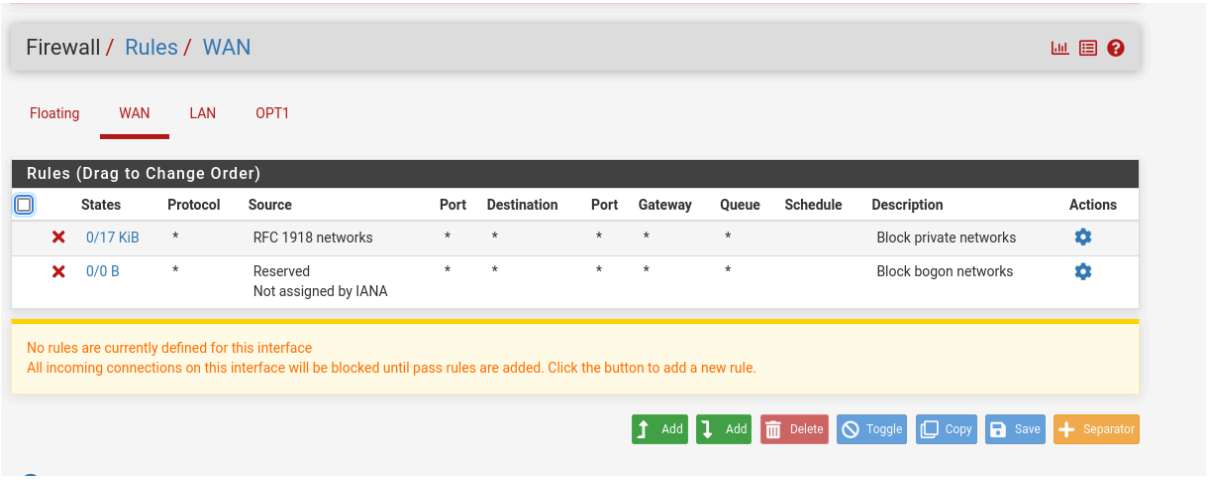
Prima di impostare il firewall andiamo a verificare se le 2 macchine comunicano





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

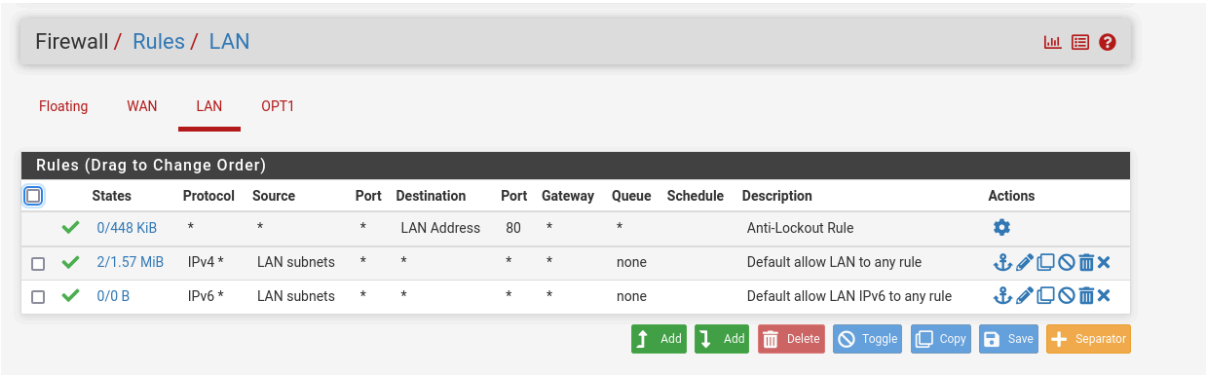
Floating | WAN | LAN | OPT1

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✗	0/17 KiB	*	RFC 1918 networks	*	*	*	*	*		Block private networks	⚙
✗	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



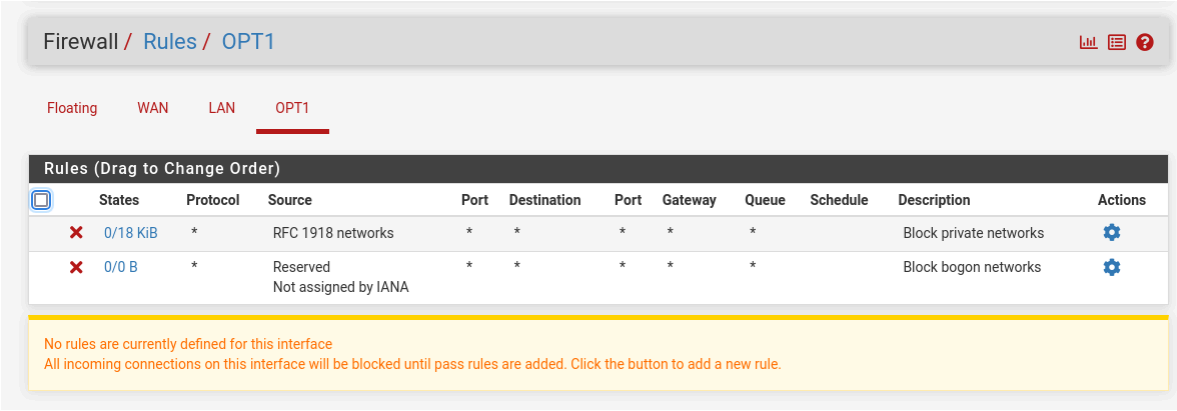
Firewall / Rules / LAN

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

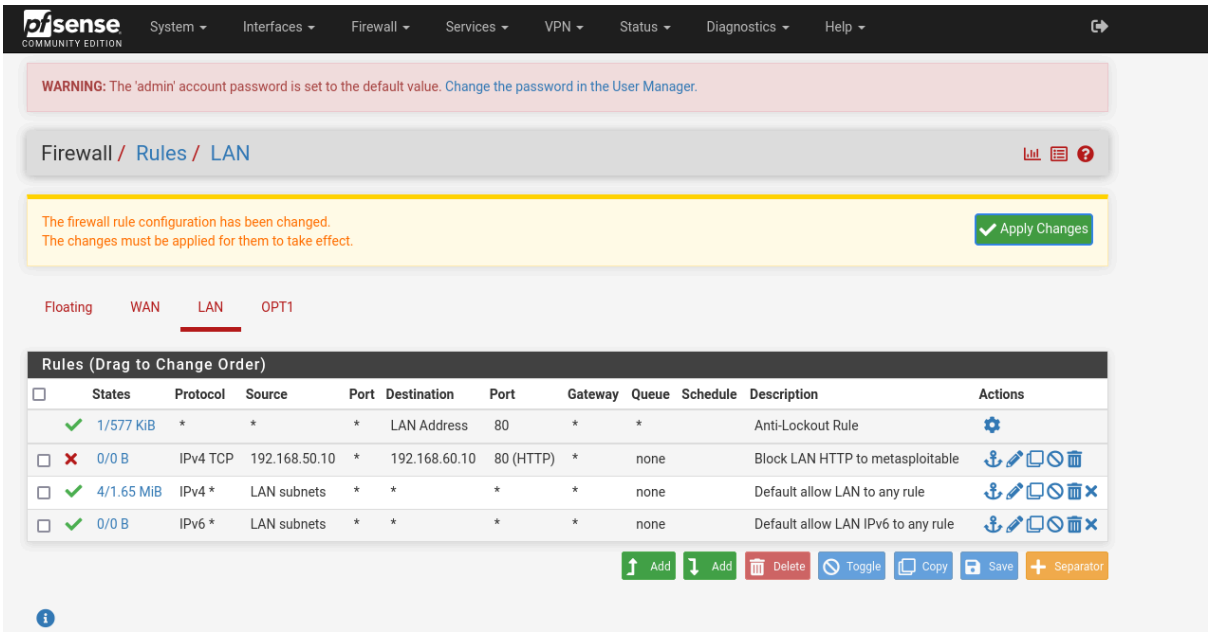
Rules (Drag to Change Order)

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

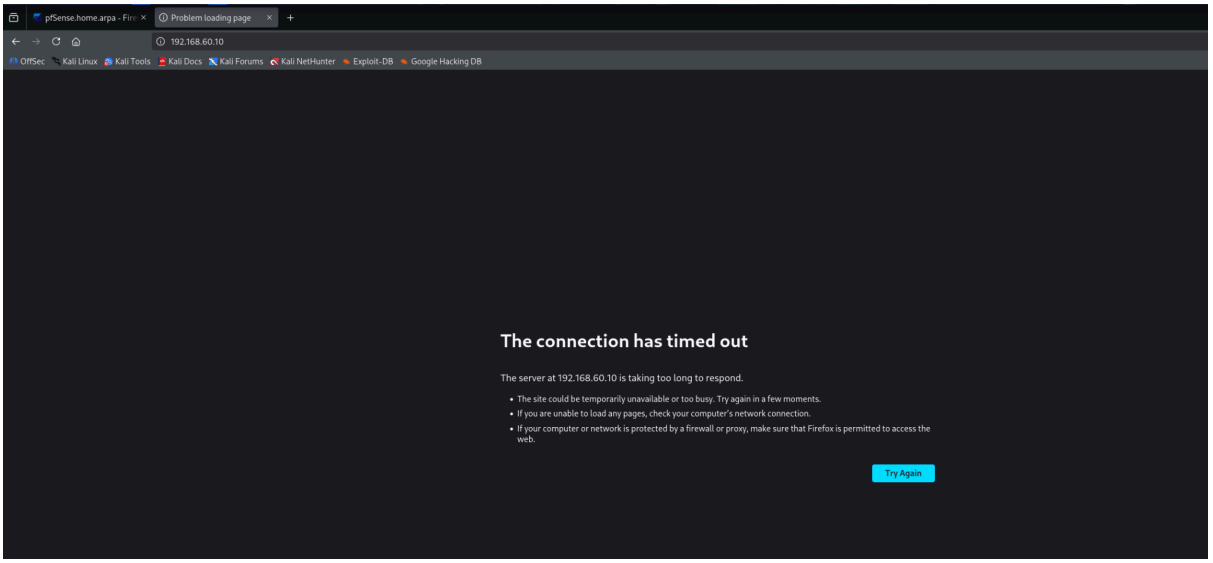
No rules are currently defined for this interface
All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.

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



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



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