

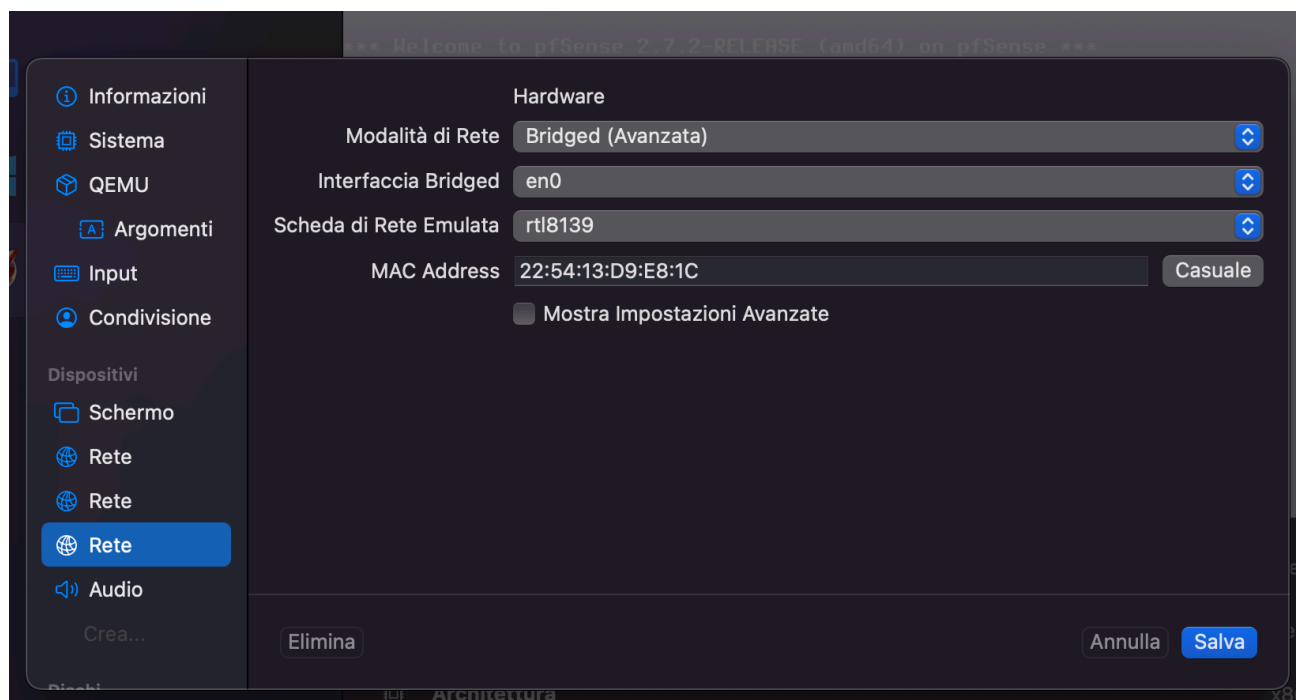
Creare una regola firewall che blocchi l'accesso alla DVWA (su metasploitable) dalla macchina Kali Linux e ne impedisca di conseguenza lo scan.

IP KALI: 192.168.50.100

IP METASPOTABLE: 192.168.64.3

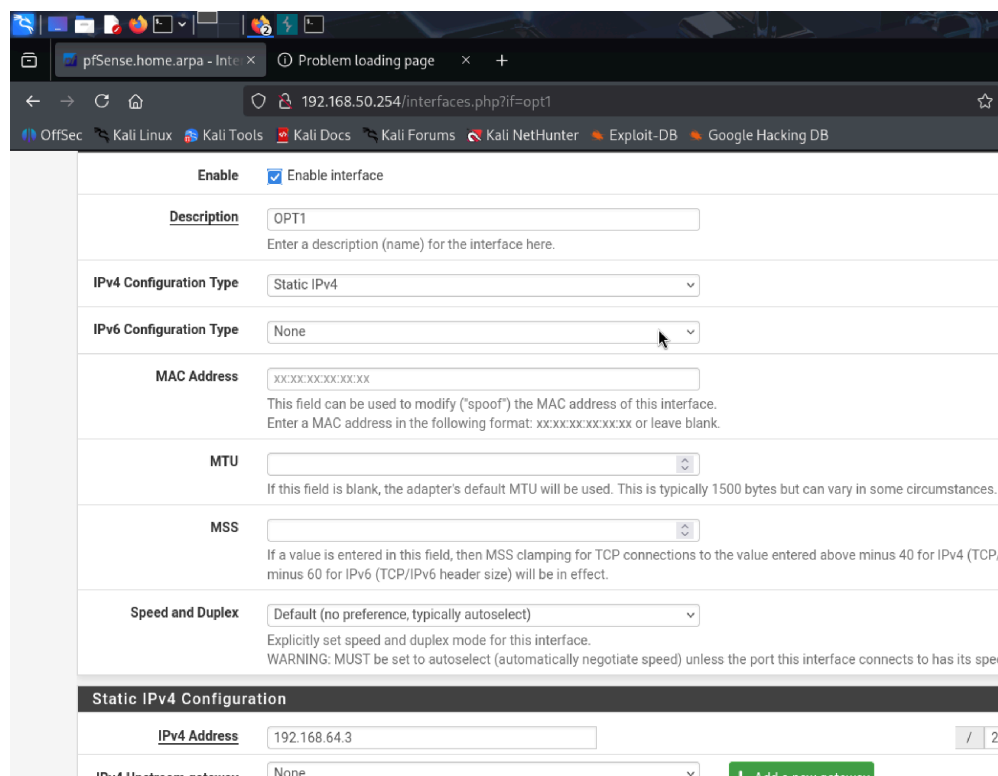
Step1.

Come primo step ho creato una nuova rete su UTM andando su pfsense-modifica-crea rete. Ho creato una rete condivisa.



Step2.

A questo punto sono andato sulla pagina pfsense, dopo di che sono andato su interface/assignments per aggiungere la rete appena creata ed ho inserito i dati della metaspotable.



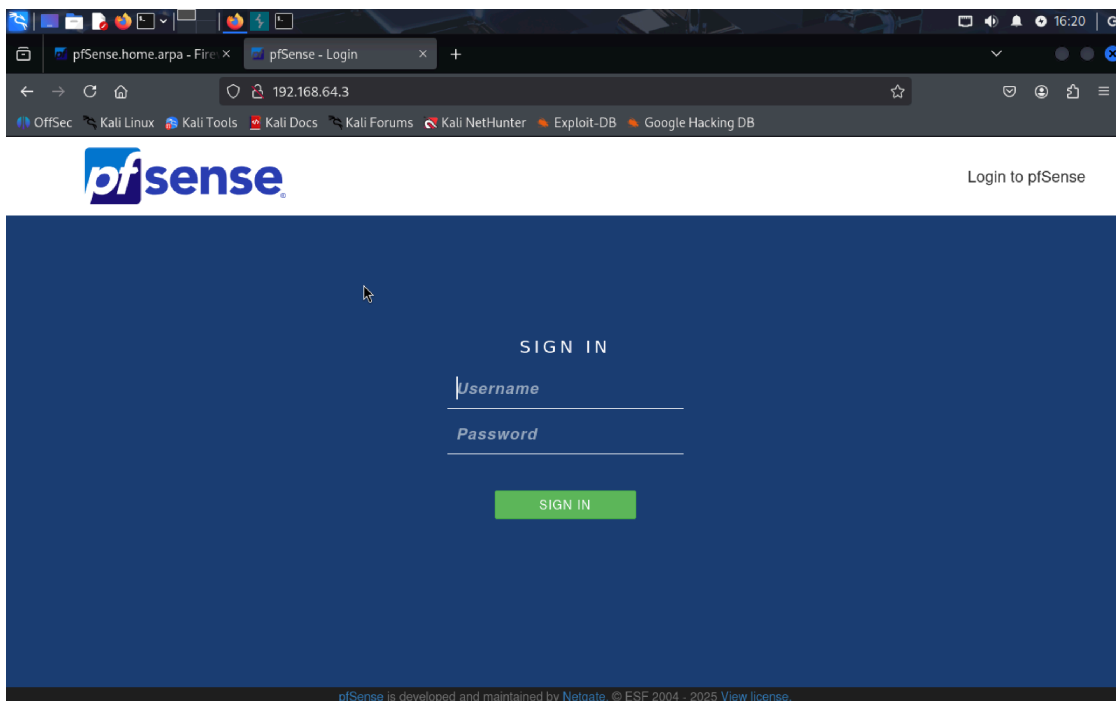
Step3.

Ho verificato che la Kali e la metaspotable comunicassero facendo il comando ping sul terminale.

```
kali@kali: ~  
File Actions Edit View Help  
kali@kali: ~ x kali@kali: ~ x  
(kali@kali)-[~]  
$ ping 192.168.64.3  
PING 192.168.64.3 (192.168.64.3) 56(84) bytes of data.  
64 bytes from 192.168.64.3: icmp_seq=1 ttl=64 time=3.00 ms  
64 bytes from 192.168.64.3: icmp_seq=2 ttl=64 time=2.54 ms  
64 bytes from 192.168.64.3: icmp_seq=3 ttl=64 time=2.75 ms  
^C  
— 192.168.64.3 ping statistics —  
3 packets transmitted, 3 received, 0% packet loss, time 2008ms  
rtt min/avg/max/mdev = 2.542/2.765/3.003/0.188 ms  
(kali@kali)-[~]  
$ ping 192.168.64.3  
PING 192.168.64.3 (192.168.64.3) 56(84) bytes of data.  
64 bytes from 192.168.64.3: icmp_seq=1 ttl=64 time=1.95 ms  
64 bytes from 192.168.64.3: icmp_seq=2 ttl=64 time=2.36 ms  
64 bytes from 192.168.64.3: icmp_seq=3 ttl=64 time=3.09 ms  
64 bytes from 192.168.64.3: icmp_seq=4 ttl=64 time=2.83 ms  
64 bytes from 192.168.64.3: icmp_seq=5 ttl=64 time=2.52 ms  
^C  
— 192.168.64.3 ping statistics —  
5 packets transmitted, 5 received, 0% packet loss, time 4009ms  
rtt min/avg/max/mdev = 1.952/2.548/3.089/0.390 ms  
(kali@kali)-[~]  
$
```

Step4.

Ho verificato che la connessione senza blocco funzionasse.



Step5.

Ora sono andato su firewall-rules-opt1 ed ho creato una regola che dovrebbe impedire l'accesso ad DVWA alla metaspotable.

-Action: Block

- Interface: LAN

Su Source ho inserito l'ip della Kali e su destination l'indirizzo della metaspotable su porta http 80.

← → ↺ 🏠

192.168.50.254/firewall_rules_edit.php?id=0 ☆ 🍷

🔒 OffSec 🐧 Kali Linux 📄 Kali Tools 📄 Kali Docs 🗣️ Kali Forums 🚫 Kali NetHunter 🔍 Exploit-DB 🔍 Google Hacking DB

Action

Block

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled

☐ Disable this rule
Set this option to disable this rule without removing it from the list.

Interface

LAN

Choose the interface from which packets must come to match this rule.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

TCP

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match

Address or Alias

192.168.50.100

/

⚙️ Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination

☐ Invert match
































Address or Alias

192.168.64.3

/

Step6.

Una volta creata la regola la trascino in alto per dargli priorità

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	 1/544 KiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
	 0/0 B	IPv4 TCP	192.168.50.100	*	192.168.64.3	80 (HTTP)	*	none		Blocca DVWA	   
	 0/101 KiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	    
	 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	    
<div> Add  Add  Delete  Toggle  Copy  Save  Separator</div>											

Step7.

Per verificare che il blocco sia funzionante ho provato ad accedere alla DVWA con esito negativo.

