

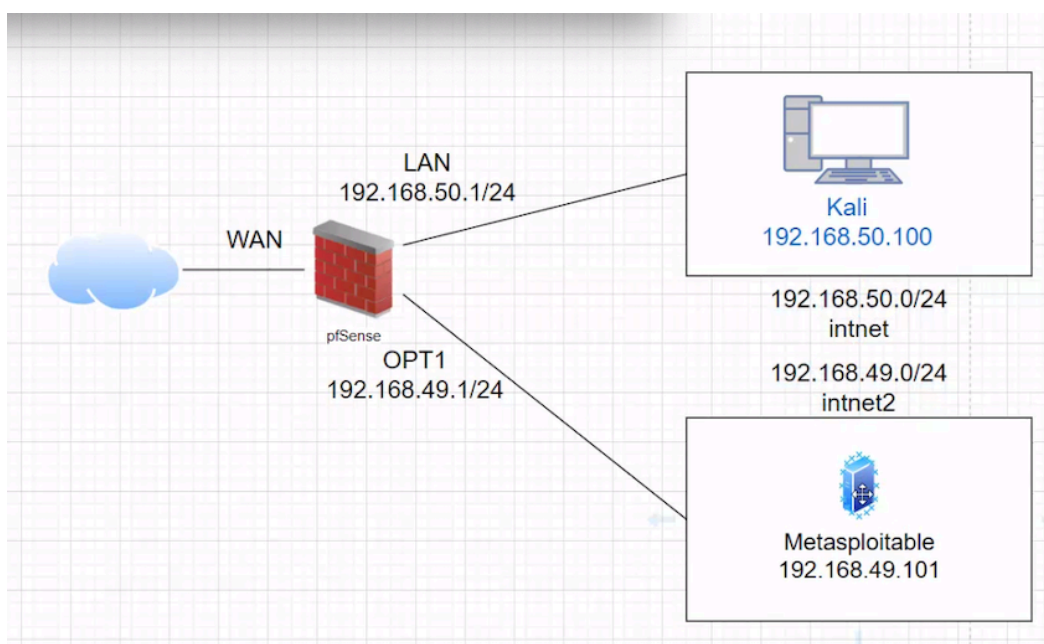
CONSEGNA 19 FEBBRAIO S5L1

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

Dopo aver scaricato ed installato PFSense, dalle impostazioni di virtual box ho configurato tre reti su PFSense: una rete NAT, una rete interna intnet per Kali ed una rete intnet 2 per meta (OPT1).

```
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***  
  
WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24  
LAN (lan)      -> em1      -> v4: 192.168.50.1/24  
OPT1 (opt1)    -> em2      -> v4: 192.168.49.1/24
```

Successivamente ho dovuto cambiare l'indirizzo IP di Meta, nell'immagine allego tutte le configurazioni degli indirizzi IP



Dopo aver settato PFSense, dal browser di Kali, ho impostato le policy del firewall sulla rete LAN, bloccando l'accesso alla pagina DVWA.:80 di meta e quindi i pacchetti in arrivo da Meta. Un'altra opzione possibile era quello di impostare le policy sulla rete OPT1/INTNET2, andando a bloccare quindi i pacchetti in uscita.

Allego sotto l'immagine delle impostazioni della policy su rete LAN.

Da sottolineare che l'azione scelta è stata Block, un'alternativa possibile era l'opzione reject, dove l'utente che tenterà di accedere all'indirizzo bloccato riceverà un messaggio "porta irraggiungibile".

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	<input type="checkbox"/> 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	<input type="checkbox"/> Invert match	Address or Alias	192.168.50.100 /
<div>⚙ Display Advanced</div> <p>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.</p>			
Destination			
Destination	<input type="checkbox"/> Invert match	Address or Alias	192.168.49.101 /
Destination Port Range	From HTTP (80)	To HTTP (80)	

Come richiesto, la porta 80 è stata bloccata dal firewall.

The connection has timed out

The server at 192.168.49.101 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.

```
(kali㉿kali)-[~]  
$ ping 192.168.49.101  
PING 192.168.49.101 (192.168.49.101) 56(84) bytes of data.  
64 bytes from 192.168.49.101: icmp_seq=1 ttl=63 time=7.08 ms  
64 bytes from 192.168.49.101: icmp_seq=2 ttl=63 time=6.78 ms  
64 bytes from 192.168.49.101: icmp_seq=3 ttl=63 time=5.05 ms  
64 bytes from 192.168.49.101: icmp_seq=4 ttl=63 time=17.5 ms  
64 bytes from 192.168.49.101: icmp_seq=5 ttl=63 time=8.82 ms  
64 bytes from 192.168.49.101: icmp_seq=6 ttl=63 time=2.33 ms  
^C  
— 192.168.49.101 ping statistics —  
6 packets transmitted, 6 received, 0% packet loss, time 5011ms  
rtt min/avg/max/mdev = 2.331/7.918/17.455/4.712 ms
```

Allego anche l'immagine del ping da Kali a Meta