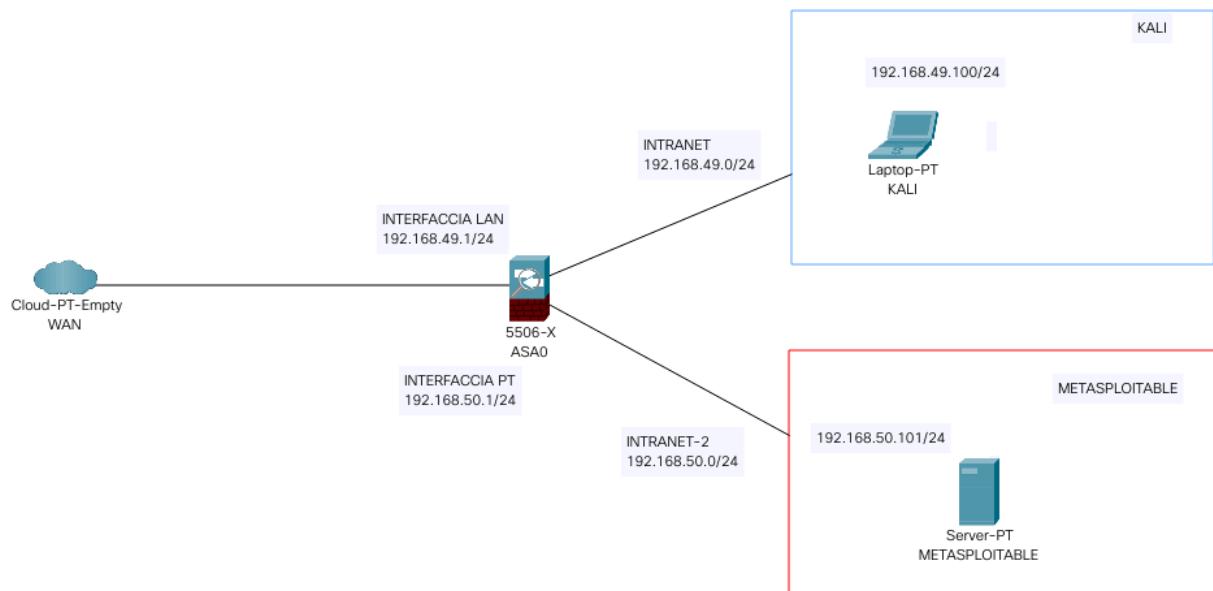


ESERCIZIO S5L1

Traccia: Creare una regola firewall che blocca l'accesso alla DVWA (su metasploitable) dalla macchina Kali Linux e ne impedisca di conseguenza lo scan. Un requisito fondamentale dell'esercizio è che le macchine Kali e Metasploitable siano su reti diverse, potete aggiungere una nuova interfaccia di rete a Pfsense in modo tale da gestire una ulteriore rete. Pfsense è una distribuzione basata su FreeBSD ottimizzata per essere utilizzata come firewall.

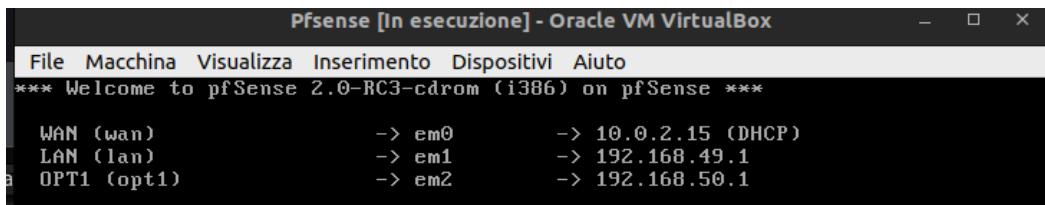
IMPOSTAZIONI AMBIENTE



Inizialmente Pfsense è stata creata sulla macchina virtuale settando 3 schede di rete diverse:

- NAT (interfaccia WAN)
- Rete interna (intnet) (interfaccia LAN)
- Rete interna (pfsense)

La terza scheda di rete è stata creata per aggiungere una nuova interfaccia di rete a Pfsense in modo tale da avere pfsense e metasploitable su una stessa sottorete che chiamiamo "pfsense".



Successivamente si è abilitato il servizio dhcp sull'interfaccia appena creata e sono state modificate le impostazioni di rete di Metasploitable in modo da non utilizzare la configurazione di rete statica, ma quella "dhcp".

TEST FUNZIONAMENTO

Dopo aver settato l'ambiente, si verifica che ci sia connettività tra Kali e Meta, attraverso sia un ping verso Meta (figura a sinistra), che attraverso la DVWA (immagine a destra).

```
(kali㉿kali)-[~] $ ping 192.168.50.101
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data.
64 bytes from 192.168.50.101: icmp_seq=1 ttl=64 time=0.594 ms
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=0.534 ms
64 bytes from 192.168.50.101: icmp_seq=3 ttl=64 time=0.185 ms
64 bytes from 192.168.50.101: icmp_seq=4 ttl=64 time=0.462 ms
64 bytes from 192.168.50.101: icmp_seq=5 ttl=64 time=0.344 ms
64 bytes from 192.168.50.101: icmp_seq=6 ttl=64 time=0.458 ms
^C
--- 192.168.50.101 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5101ms
rtt min/avg/max/mdev = 0.185/0.429/0.594/0.133 ms
(kali㉿kali)-[~] $
```

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

- [TWiki](#)
- [phpMyAdmin](#)
- [Mutilidae](#)
- [DVWA](#)
- [WebDAV](#)

CREAZIONE FIREWALL RULE

Ora, attraverso il sito di Pfsense, si va a creare la regola per bloccare il traffico tra Kali e Meta, in particolare si è bloccato il traffico dalla porta 22 (SSH) alla porta 80 (HTTP). In questo modo si rende inaccessibile la DVWA da Kali.

Firewall: Rules: Edit

Edit Firewall rule

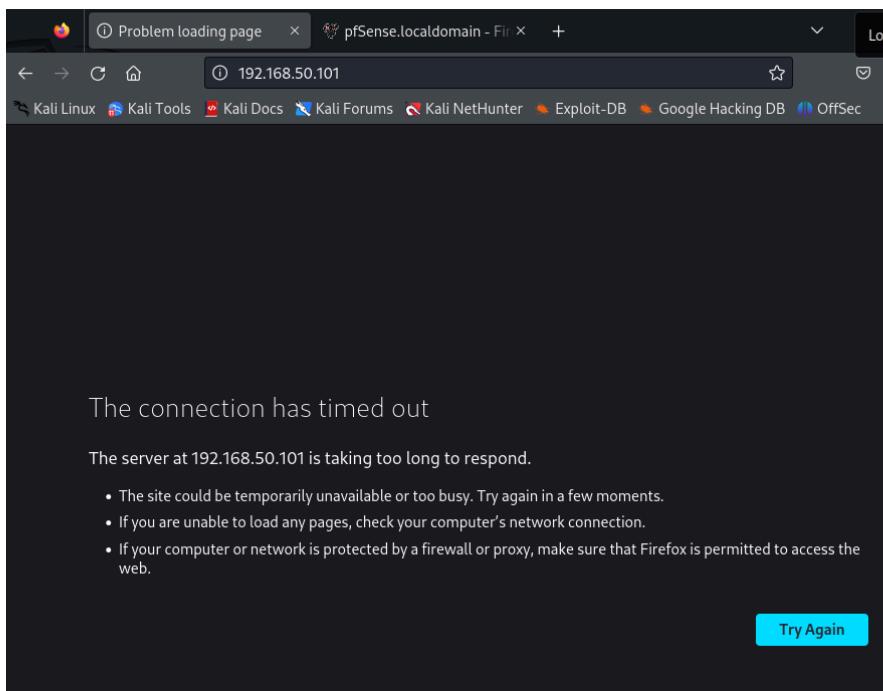
Action	<input type="button" value="Block"/>	Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped 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	<input type="button" value="LAN"/>	Choose on which interface packets must come in to match this rule.
Protocol	<input type="button" value="TCP"/>	Choose which IP protocol this rule should match. Hint: in most cases, you should specify <i>TCP</i> here.
Source	<input type="checkbox"/> not	Use this option to invert the sense of the match. Type: <input type="button" value="Single host or alias"/> Address: <input type="text" value="192.168.49.100"/> / <input type="button"/>
<input type="button" value="Advanced"/> - Show source port range		
Destination	<input type="checkbox"/> not	Use this option to invert the sense of the match. Type: <input type="button" value="Single host or alias"/> Address: <input type="text" value="192.168.50.101"/> / <input type="button"/>
Destination port range	from: <input type="button" value="SSH"/>	<input type="button"/>
	to: <input type="button" value="HTTP"/>	<input type="button"/>
Specify the port or port range for the destination of the packet for this rule. Hint: you can leave the 'to' field empty if you only want to filter a single port		
Log	<input checked="" type="checkbox"/> Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If you want to do a lot of logging, consider using a remote syslog server (see the Diagnostics: System logs: Settings page).	
Description	<input type="button"/> You may enter a description here for your reference.	
<input type="button" value="Save"/> <input type="button" value="Cancel"/>		

Qui di seguito è mostrato uno screen che mostra la regola appena creata, attiva.

	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	*	*	*	*	LAN Address	22 80	*	*		Anti-Lockout Rule	       
<input type="checkbox"/>	*	LAN net	*	*	*	*	*	none		Default allow LAN to any rule	       
<input checked="" type="checkbox"/>	TCP	192.168.49.100	*	192.168.50.101	22 - 80	*	*	none			       

pass pass (disabled) block block (disabled) reject reject (disabled) log log (disabled)

Ora se si prova a raggiungere nuovamente la DVWA, si nota che questa è inaccessibile. In particolare si noti come la risposta del server non sia legata ad un errore 404, ma proprio ad una mancata risposta. Questo comportamento di mancata risposta indica che il firewall Pfsense sia riuscito a bloccare le richieste.



```
(kali㉿kali)-[~]
└$ ping 192.168.50.101
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data.
^C
--- 192.168.50.101 ping statistics ---
32 packets transmitted, 0 received, 100% packet loss, time 31742ms

(kali㉿kali)-[~]
└$
```