

Creazione Policy Pfsense

Dopo aver installato e configurato la macchina Pfsense su Virtualbox siamo andati a creare la nuova NIC per avere le macchine Kali e Metasploitable su delle rete diverse (avendo come gateway quindi la macchina Pfsense).

Abbiamo poi attivato il servizio di DHCP per la questa interfaccia in modo che la macchina metasploitable potesse usufruirne.



```
metasploitable [Running]
GNU nano 2.0.7 File: /etc/network/interfaces

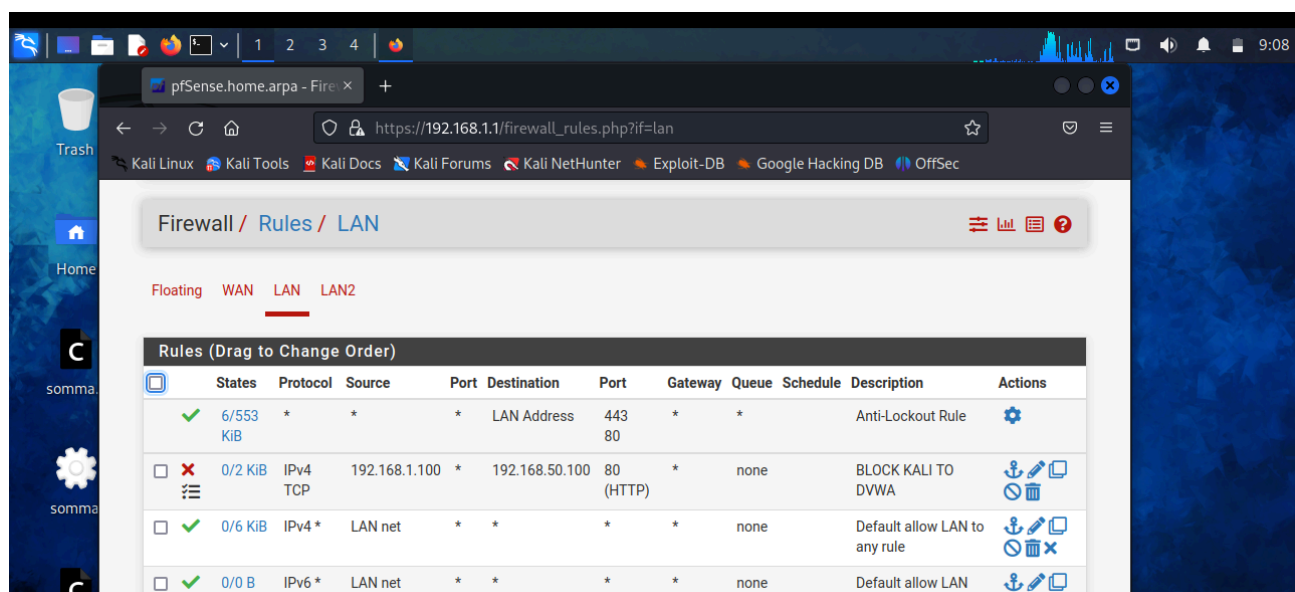
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet dhcp

#auto eth0
#iface eth0 inet static
#address 192.168.50.101
#netmask 255.255.255.0
#network 192.168.50.0
#broadcast 192.168.50.255
#gateway 192.168.50.1
```

Una volta che abbiamo appurato che la macchina Kali avesse connettività con Meta abbiamo creato la regola che bloccasse il traffico verso la porta 80 http.



Abbiamo capito che la regola imposta funziona in quanto l'indirizzo IP di Metasploitable (192.168.50.100 in questo caso) non è più accessibile dal browser. Il blocco si può anche verificare anche dai log di sistema del firewall.

The screenshot shows a Kali Linux terminal window on the left and a web browser window on the right. The terminal displays the output of a ping command to 192.168.50.100, showing successful responses. The web browser displays the pfSense status logs, which show a series of blocked connections from Kali Linux to the DVWA application on the Metasploitable machine.

Terminal Output:

```
(kali@kali)-[~]  
$ ping 192.168.50.100  
PING 192.168.50.100:  
64 bytes from 192.168.50.100: icmp_seq=1 ttl=64 time=0.064 ms  
64 bytes from 192.168.50.100: icmp_seq=2 ttl=64 time=0.064 ms  
64 bytes from 192.168.50.100: icmp_seq=3 ttl=64 time=0.064 ms  
64 bytes from 192.168.50.100: icmp_seq=4 ttl=64 time=0.064 ms  
^C  
--- 192.168.50.100 ping statistics ---  
5 packets transmitted, 5 received, 0% packet loss, time 204ms  
rtt min/avg/max/mdev = 0.064/0.064/0.064/0.000 ms
```

Web Browser Output (pfSense Status Logs):

Time	Source	Destination	Protocol	Action
Jul 22 14:38:36	LAN	BLOCK KALI TO DVWA (1690036478)	TCP:S	Blocked
Jul 22 14:38:37	LAN	BLOCK KALI TO DVWA (1690036478)	TCP:S	Blocked
Jul 22 14:38:38	LAN	BLOCK KALI TO DVWA (1690036478)	TCP:S	Blocked
Jul 22 14:38:40	LAN	BLOCK KALI TO DVWA (1690036478)	TCP:S	Blocked
Jul 22 14:38:41	LAN	BLOCK KALI TO DVWA (1690036478)	TCP:S	Blocked
Jul 22 14:38:42	LAN	BLOCK KALI TO DVWA (1690036478)	TCP:S	Blocked
Jul 22 14:38:43	LAN	BLOCK KALI TO DVWA (1690036478)	TCP:S	Blocked
Jul 22 14:38:47	LAN	BLOCK KALI TO DVWA (1690036478)	TCP:S	Blocked
Jul 22 14:38:50	LAN	BLOCK KALI TO DVWA (1690036478)	TCP:S	Blocked