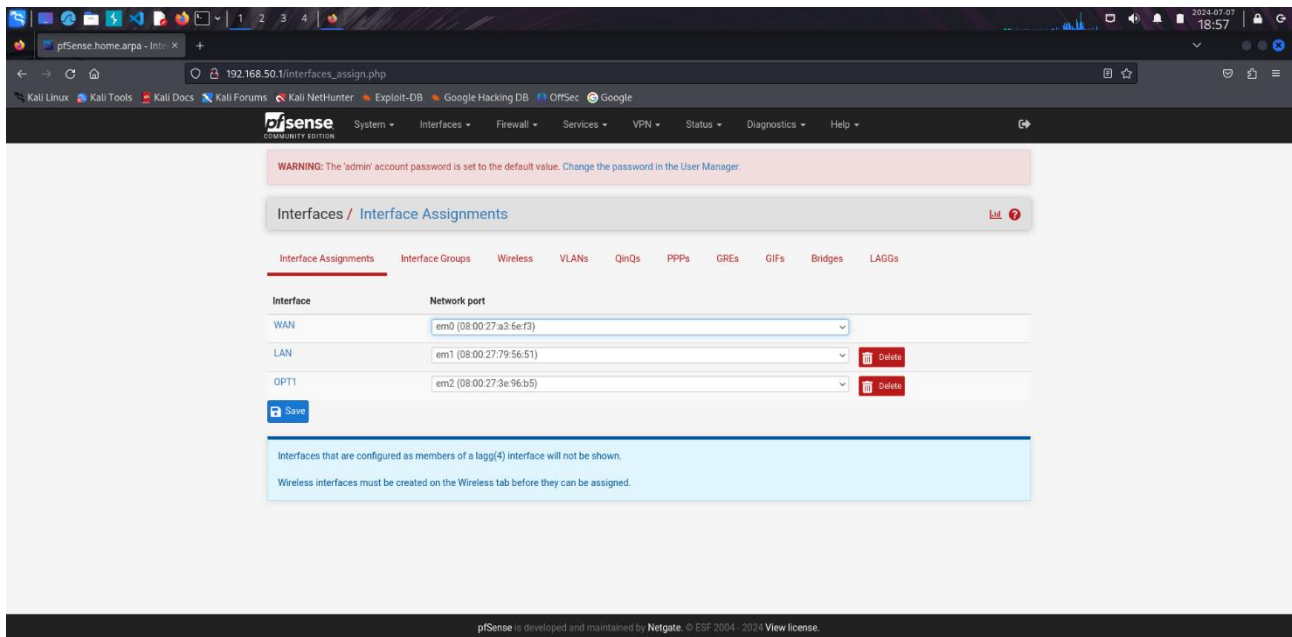


Aggiungo l'interfaccia OPT1, che appartiene alla macchina Metasploitable



La nuova interfaccia compare anche su pfSense mv, che appartiene alla sottorete che abbiamo creato

```
Enter an option:

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: 5d0b35033b9f6c5d2a63

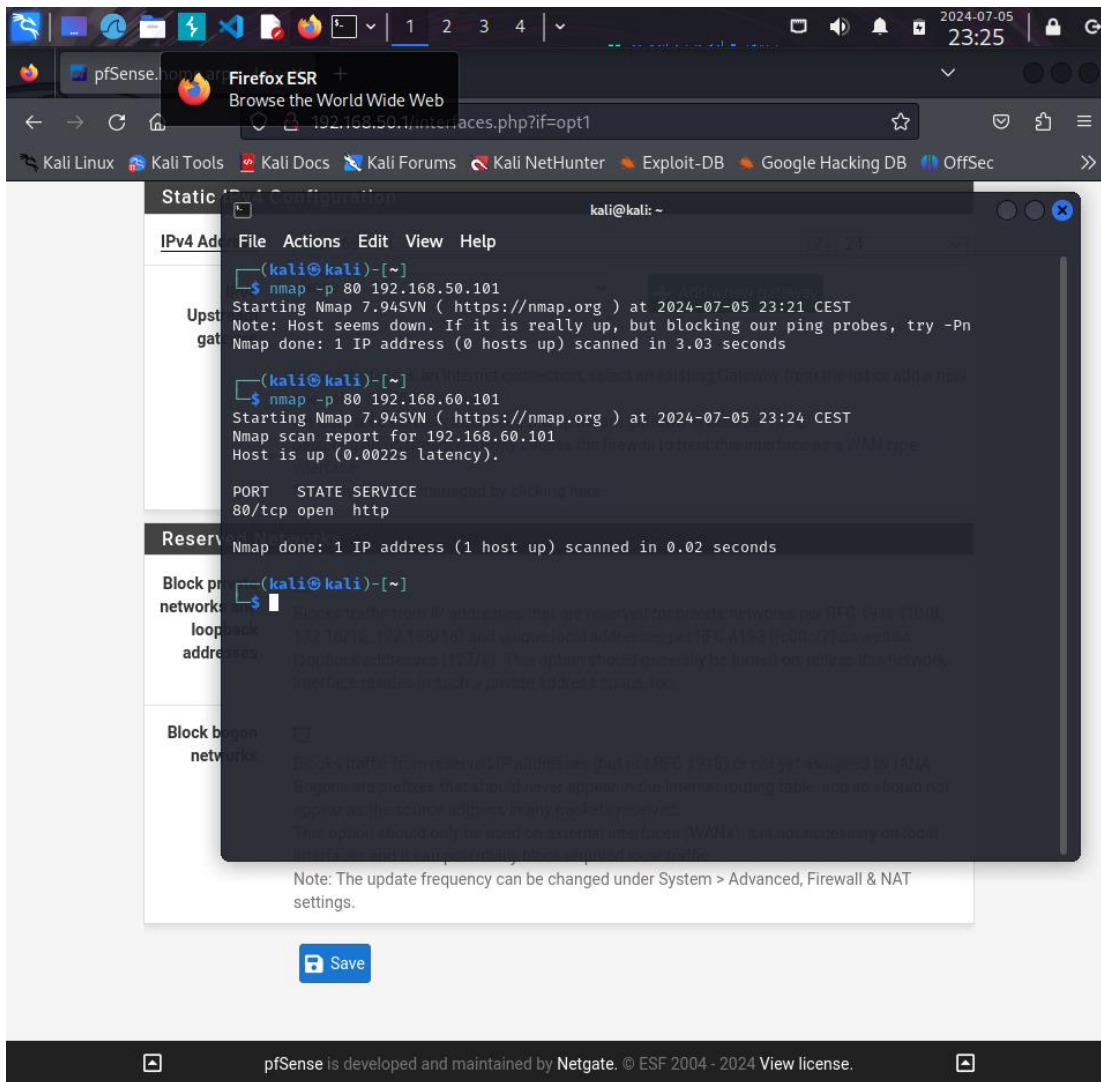
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
LAN (lan)      -> em1      -> v4: 192.168.50.1/24
OPT1 (opt1)    -> em2      -> v4: 192.168.60.1/24

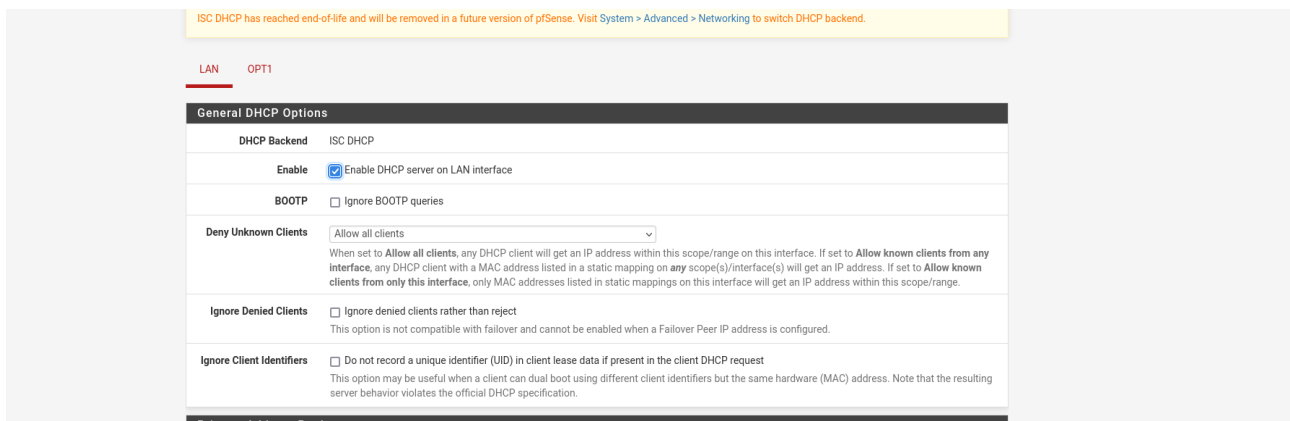
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: 
```

Faccio nmap sull'indirizzo della Meta prima di applicare la regola, la porta 80 risulta aperta



Abilito il DHCP server sia sull'interfaccia LAN che su OPT1 e creo la regola sull'interfaccia LAN



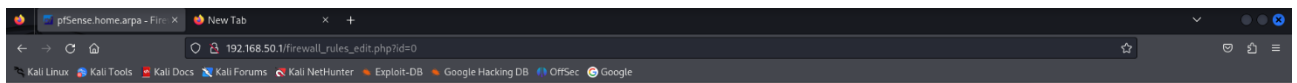
ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit [System > Advanced > Networking](#) to switch DHCP backend.

LAN OPT1

General DHCP Options

DHCP Backend	ISC DHCP
Enable	<input checked="" type="checkbox"/> Enable DHCP server on OPT1 interface
BOOTP	<input type="checkbox"/> Ignore BOOTP queries
Deny Unknown Clients	<div>Allow all clients</div> <div>When set to Allow all clients, any DHCP client will get an IP address within this scope/range on this interface. If set to Allow known clients from any interface, any DHCP client with a MAC address listed in a static mapping on any scope(s)/interface(s) will get an IP address. If set to Allow known clients from only this interface, only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.</div>
Ignore Denied Clients	<input type="checkbox"/> Ignore denied clients rather than reject This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.
Ignore Client Identifiers	<input type="checkbox"/> Do not record a unique identifier (IID) in client lease data if present in the client DHCP request This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.

Primary Address Pool



Firewall / Rules / Edit

Edit Firewall Rule

Action	Block		
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.		
Interface	LAN		
Address Family	IPv4		
Protocol	TCP		
Source	<div><input type="checkbox"/> Invert match</div> <div>Address or Alias</div> <div>192.168.50.100</div>		
Destination	<div><input type="checkbox"/> Invert match</div> <div>Address or Alias</div> <div>192.168.60.101</div>		
Destination Port Range	<div>HTTP (80)</div> <div>HTTP (80)</div>		

Firewall / Rules / Edit

Floating WAN LAN OPT1

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓	1/1.71 MB	*	*	*	LAN Address	80	*	*	Anti-Lockout Rule	
<input type="checkbox"/>	✗	0/2 KIB	IPv4 TCP	192.168.50.100	*	192.168.60.101	80 (HTTP)	*	none	Blocco da Kali -> Metasploitte	
<input type="checkbox"/>	✓	0/501 KIB	IPv4 *	LAN subnets	*	*	*	*	none	Default allow LAN to any rule	
<input type="checkbox"/>	✓	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none	Default allow LAN IPv6 to any rule	

1

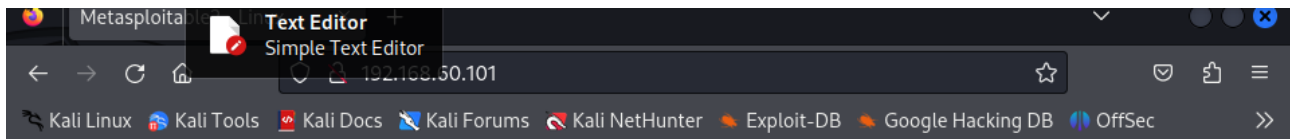
Prima di abilitare la regola controllo da Kali che la Metasploitable sia raggiungibile

```
File Actions Edit View Help
(kali@kali)-[~]
$ ping 192.168.60.101
PING 192.168.60.101 (192.168.60.101) 56(84) bytes of data:
64 bytes from 192.168.60.101: icmp_seq=1 ttl=63 time=1.33 ms
64 bytes from 192.168.60.101: icmp_seq=2 ttl=63 time=4.41 ms
64 bytes from 192.168.60.101: icmp_seq=3 ttl=63 time=2.53 ms
64 bytes from 192.168.60.101: icmp_seq=4 ttl=63 time=5.50 ms
64 bytes from 192.168.60.101: icmp_seq=5 ttl=63 time=2.26 ms
^X64 bytes from 192.168.60.101: icmp_seq=6 ttl=63 time=3.55 ms
64 bytes from 192.168.60.101: icmp_seq=7 ttl=63 time=2.61 ms
^Z
zsh: suspended ping 192.168.60.101

Warning: Never expose this VM to an untrusted network!
(kali@kali)-[~]
$ cat: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

• TWiki
• phpMyAdmin
• Mutillidae
• DVWA
• WebDAV
```



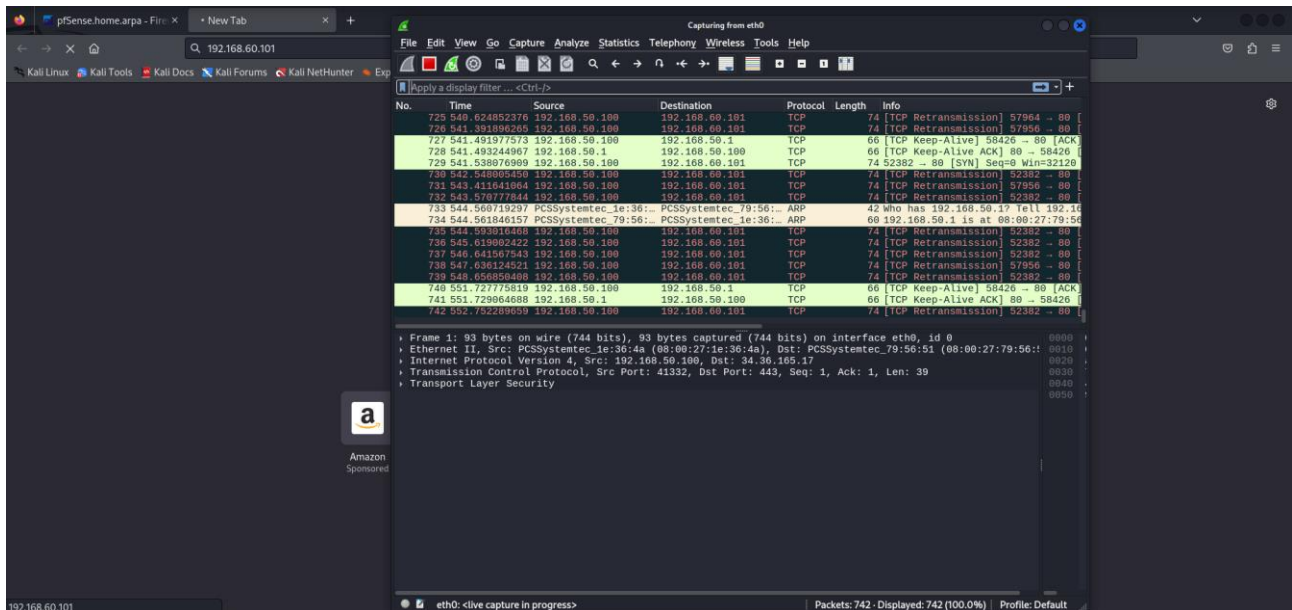
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

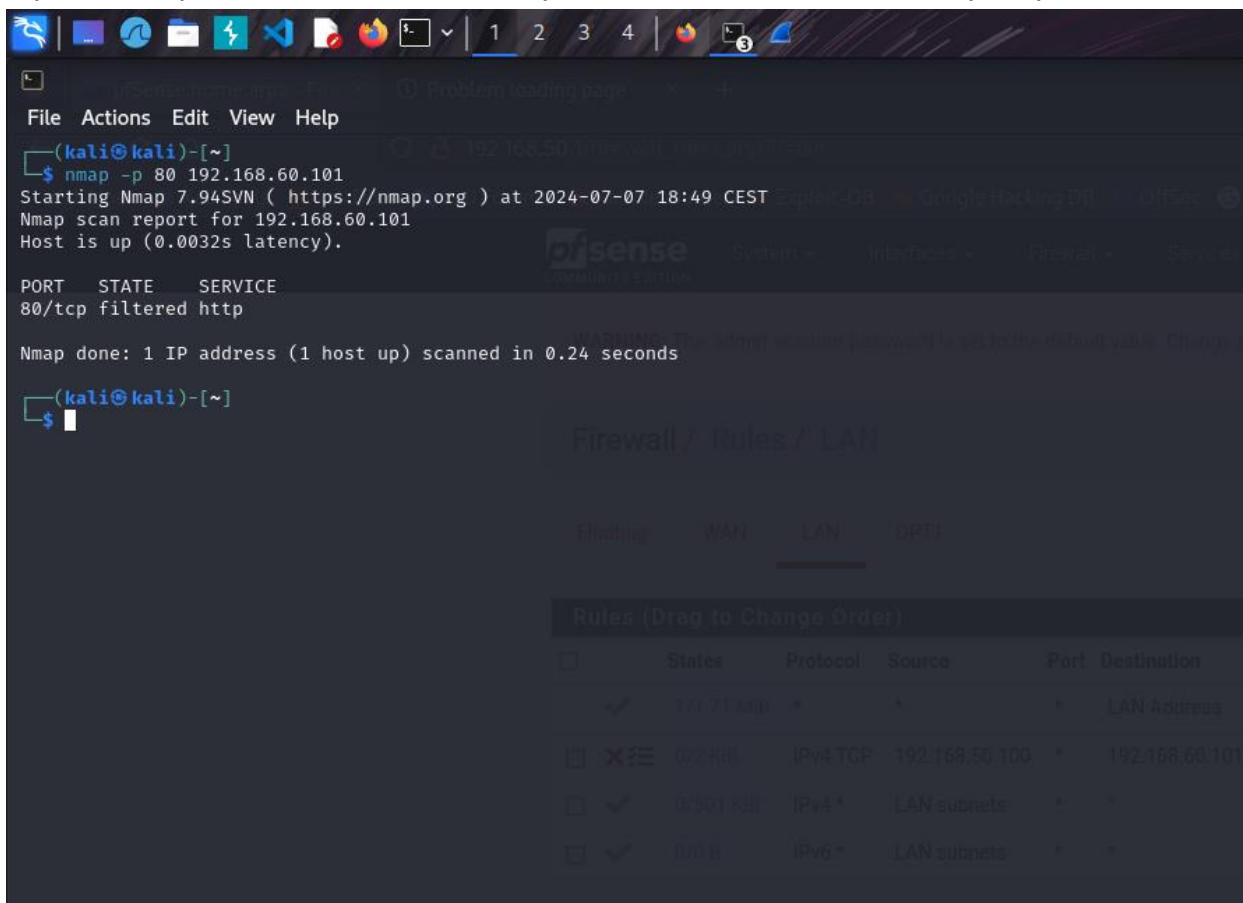
Login with msfadmin/msfadmin to get started

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

Adesso abilito la regola e provo a ricollegarmi sulla DVWA di Metasploitable ma non si collegherà e possiamo vedere, grazie a wireshark, che la connessione con TCP non va a buon fine.



Riprovo nmap e vedo che lo stato della porta 80 risulterà 'filtered' e non più open



Ispezione dei log del Firewall

pfSense home.arpa - Sta x New Tab x +

192.168.50.1/status_logs_filter.php

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Google

Normal View Dynamic View Summary View

Last 500 Firewall Log Entries. (Maximum 500)

Action	Time	Interface	Rule	Source	Destination	Protocol
✗	Jul 7 16:46:42	LAN	Blocco da Kali -> Metasploite (1720369407)	192.168.50.100:38988	192.168.60.101:80	TCP-S
✗	Jul 7 16:46:36	LAN	Blocco da Kali -> Metasploite (1720369407)	192.168.50.100:33406	192.168.60.101:80	TCP-S
✗	Jul 7 16:46:34	LAN	Blocco da Kali -> Metasploite (1720369407)	192.168.50.100:38988	192.168.60.101:80	TCP-S
✗	Jul 7 16:46:29	LAN	Blocco da Kali -> Metasploite (1720369407)	192.168.50.100:38988	192.168.60.101:80	TCP-S
✗	Jul 7 16:46:28	LAN	Blocco da Kali -> Metasploite (1720369407)	192.168.50.100:33406	192.168.60.101:80	TCP-S
✗	Jul 7 16:46:27	LAN	Blocco da Kali -> Metasploite (1720369407)	192.168.50.100:38988	192.168.60.101:80	TCP-S
✗	Jul 7 16:46:26	LAN	Blocco da Kali -> Metasploite (1720369407)	192.168.50.100:38988	192.168.60.101:80	TCP-S
✗	Jul 7 16:46:25	LAN	Blocco da Kali -> Metasploite (1720369407)	192.168.50.100:38988	192.168.60.101:80	TCP-S
✗	Jul 7 16:46:24	LAN	Blocco da Kali -> Metasploite (1720369407)	192.168.50.100:38988	192.168.60.101:80	TCP-S
✗	Jul 7 16:46:24	LAN	Blocco da Kali -> Metasploite (1720369407)	192.168.50.100:33406	192.168.60.101:80	TCP-S
✗	Jul 7 16:46:23	LAN	Blocco da Kali -> Metasploite (1720369407)	192.168.50.100:38988	192.168.60.101:80	TCP-S
✗	Jul 7 16:46:22	LAN	Blocco da Kali -> Metasploite (1720369407)	192.168.50.100:38988	192.168.60.101:80	TCP-S
✗	Jul 7 16:46:22	LAN	Blocco da Kali -> Metasploite (1720369407)	192.168.50.100:33406	192.168.60.101:80	TCP-S
✗	Jul 7 16:46:21	LAN	Blocco da Kali -> Metasploite (1720369407)	192.168.50.100:33410	192.168.60.101:80	TCP-S
✗	Jul 7 16:46:21	LAN	Blocco da Kali -> Metasploite (1720369407)	192.168.50.100:33406	192.168.60.101:80	TCP-S
✗	Jul 7 16:46:20	LAN	Blocco da Kali -> Metasploite (1720369407)	192.168.50.100:33410	192.168.60.101:80	TCP-S
✗	Jul 7 16:46:20	LAN	Blocco da Kali -> Metasploite (1720369407)	192.168.50.100:33406	192.168.60.101:80	TCP-S
✗	Jul 7 16:46:19	LAN	Blocco da Kali -> Metasploite (1720369407)	192.168.50.100:33410	192.168.60.101:80	TCP-S