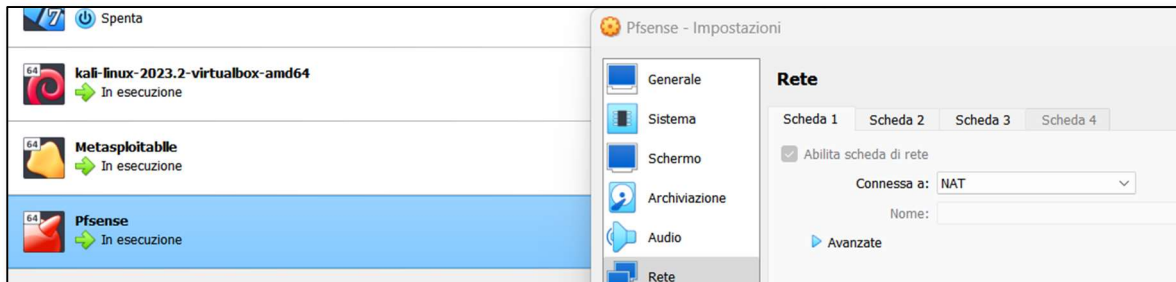


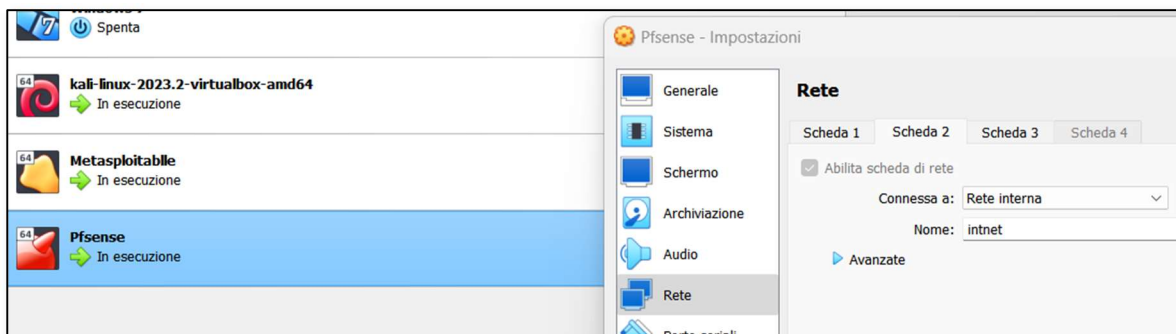
Pfsense

Dopo aver installato la macchina virtuale Pfsense, si abilitano 3 schede di rete da Virtual Box:

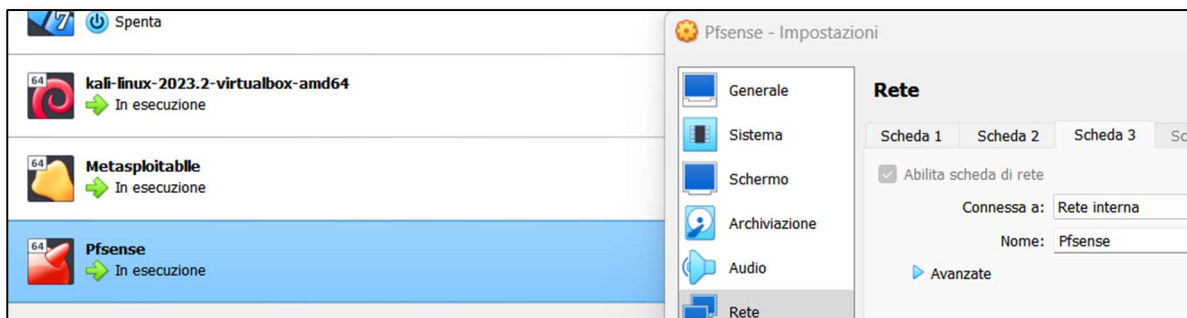
- 1) **NAT** per navigare su web



- 2) **Rete interna Intnet**, che verrà utilizzata per comunicare con Kali Linux



- 3) **Rete interna Pfsense**, che verrà utilizzata per comunicare con Metasploitable



Avviando Pfsense è possibile vedere gli ip della rete WAN e LAN (intnet):

```
WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24
```

Per utilizzare il web tool di configurazione Pfsense da Kali Linux, è necessario configurare Kali sulla stessa rete interna Intnet di Pfsense, quindi sulla rete **192.168.1.0/24**.

E' importante configurare il gateway con l'indirizzo ip di Pfsense per permettere la comunicazione tra le due macchine.

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

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

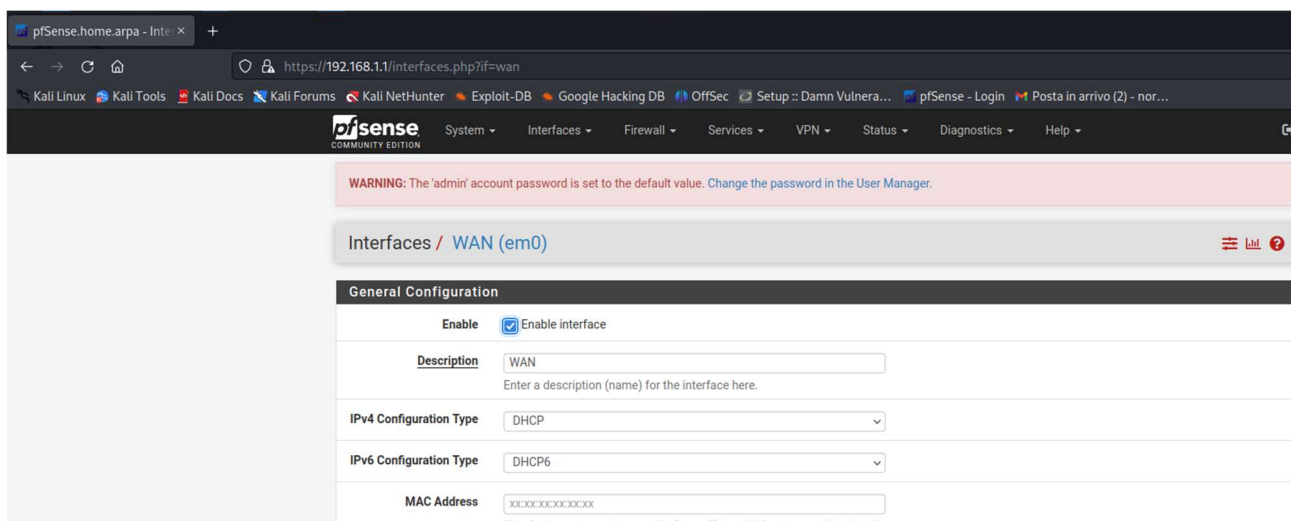
auto eth0
#iface eth0 inet dhcp
iface eth0 inet static
address 192.168.1.10/24
gateway 192.168.1.1
```

Verifichiamo la connettività eseguendo un ping da Kali a Pfsense:




```
(kali㉿kali)-[~]
$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=0.587 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=0.816 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=0.744 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=1.00 ms
64 bytes from 192.168.1.1: icmp_seq=5 ttl=64 time=0.404 ms
64 bytes from 192.168.1.1: icmp_seq=6 ttl=64 time=0.200 ms
```

La comunicazione è verificata e possiamo accedere dal browser in Kali al web tool di Pfsense, dove possiamo vedere e allineare le configurazioni di rete dal menu **"Interfaces"**.

Scheda di rete WAN configurata con DHCP:



Scheda di rete **LAN (em1)** configurata con IP statico **192.168.1.1**:

Interfaces / LAN (em1)   

General Configuration

Enable

☒ Enable interface

Description

LAN

Enter a description (name) for the interface here.

IPv4 Configuration Type

Static IPv4

IPv6 Configuration Type

Track Interface

MAC Address

xx:xx:xx:xx:xx:xx

This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

MTU

If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS

If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Speed and Duplex

Default (no preference, typically autoselect)

Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.




Static IPv4 Configuration

IPv4 Address

192.168.1.1

/ 24

Scheda di rete **LAN2 (em2)** che aggiungiamo e configuriamo con IP statico **192.168.50.1**:

Interfaces / LAN2 (em2)   

General Configuration

Enable

☒ Enable interface

Description

LAN2

Enter a description (name) for the interface here.

IPv4 Configuration Type

Static IPv4

IPv6 Configuration Type

None

MAC Address

xx:xx:xx:xx:xx:xx

This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

MTU

If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS

If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Speed and Duplex

Default (no preference, typically autoselect)

Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Static IPv4 Configuration

IPv4 Address

192.168.50.1

/ 24

Per la LAN2 abilitiamo anche il servizio come server DHCP da menu Services -> DHCP Server in modo da poter assegnare un ip alla macchina Metasploitable:

The screenshot shows the PfSense web interface for configuring the DHCP Server on the LAN2 interface. The breadcrumb trail is 'Services / DHCP Server / LAN2'. The 'LAN2' tab is selected. Under 'General Options', the 'Enable' checkbox is checked, and the 'BOOTP' checkbox is unchecked. The 'Deny unknown clients' dropdown is set to 'Allow all clients'. The 'Ignore denied clients' checkbox is unchecked. The 'Ignore client identifiers' checkbox is unchecked. The 'Subnet' is 192.168.50.0, the 'Subnet mask' is 255.255.255.0, and the 'Available range' is 192.168.50.1 - 192.168.50.254. The 'Range' section shows 'From' 192.168.50.100 and 'To' 192.168.50.200.

General Options	
Enable	<input checked="" type="checkbox"/> Enable DHCP server on LAN2 interface
BOOTP	<input type="checkbox"/> Ignore BOOTP queries
Deny unknown clients	<input type="text" value="Allow all clients"/>
Ignore denied clients	<input type="checkbox"/> Ignore denied clients rather than reject
Ignore client identifiers	<input type="checkbox"/> Do not record a unique identifier (UID) in client lease data if present in the client DHCP request
Subnet	192.168.50.0
Subnet mask	255.255.255.0
Available range	192.168.50.1 - 192.168.50.254
Range	<input type="text" value="192.168.50.100"/> <input type="text" value="192.168.50.200"/>

Riavviando PfSense, vediamo tutti gli ip:

```
WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24
LAN2 (opt1)    -> em2      -> v4: 192.168.50.1/24
```

Adesso modifichiamo la configurazione in Metasploitable in modo da impostare il DHCP:

```
# 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

#iface eth0 inet static
#address 192.168.32.101
#netmask 255.255.255.0
#network 192.168.32.0
#broadcast 192.168.32.255
#gateway 192.168.32.1
```

Riavviando Metasploitable ed eseguendo il comando ifconfig vediamo che l'ip della macchina è **192.168.50.100**:

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:11:6c:88
          inet addr:192.168.50.100  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe11:6c88/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3 errors:0 dropped:0 overruns:0 frame:0
          TX packets:109 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:756 (756.0 B)  TX bytes:26836 (26.2 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:428 errors:0 dropped:0 overruns:0 frame:0
          TX packets:428 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:184385 (180.0 KB)  TX bytes:184385 (180.0 KB)
```

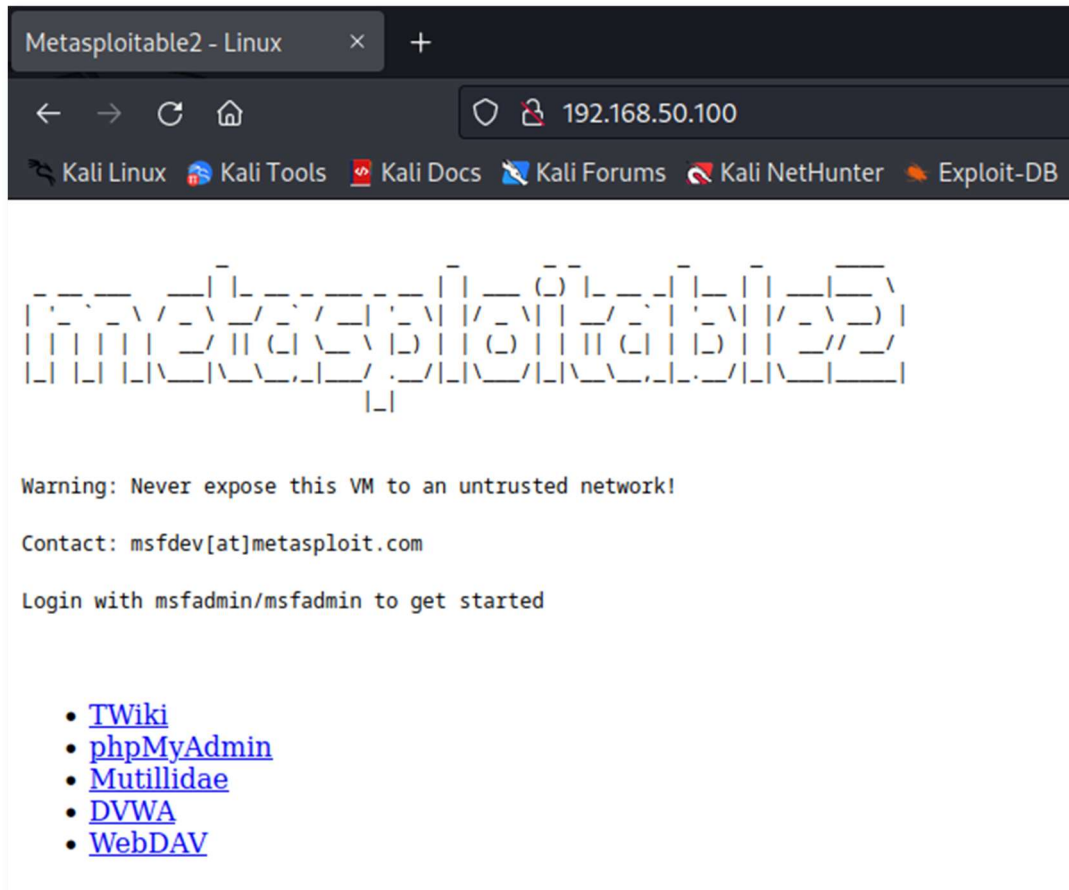
Verifichiamo la connettività eseguendo un ping da Metasploitable a Pfsense (utilizzando ovviamente l'ip dell'interfaccia di rete LAN2):

```
msfadmin@metasploitable:~$ ping 192.168.50.1
PING 192.168.50.1 (192.168.50.1) 56(84) bytes of data.
64 bytes from 192.168.50.1: icmp_seq=1 ttl=64 time=5.84 ms
64 bytes from 192.168.50.1: icmp_seq=2 ttl=64 time=1.06 ms
64 bytes from 192.168.50.1: icmp_seq=3 ttl=64 time=0.950 ms
64 bytes from 192.168.50.1: icmp_seq=4 ttl=64 time=0.865 ms
64 bytes from 192.168.50.1: icmp_seq=5 ttl=64 time=1.01 ms
64 bytes from 192.168.50.1: icmp_seq=6 ttl=64 time=1.34 ms
64 bytes from 192.168.50.1: icmp_seq=7 ttl=64 time=0.988 ms
64 bytes from 192.168.50.1: icmp_seq=8 ttl=64 time=0.986 ms
64 bytes from 192.168.50.1: icmp_seq=9 ttl=64 time=1.12 ms
64 bytes from 192.168.50.1: icmp_seq=10 ttl=64 time=1.06 ms
^X64 bytes from 192.168.50.1: icmp_seq=11 ttl=64 time=0.746 ms
64 bytes from 192.168.50.1: icmp_seq=12 ttl=64 time=0.833 ms
```

Le configurazioni di rete sono adesso completate.

Da Kali **192.168.1.10** proviamo adesso ad accedere a Metasploitable **192.168.50.100**.

Riusciamo ad accedere grazie a Pfsense utilizzato come gateway.



Dal tool web di configurazione di PfSense su Kali, accediamo al menu **Firewall -> Rules** e creiamo una nuova regola per bloccare la comunicazione tra ip Kali 192.168.1.10 e ip Metasploitable 192.168.50.100 sulla porta 80 (HTTP):

192.168.1.1/firewall_rules_edit.php?if=lan&after=-1

Kali NetHunter Exploit-DB Google Hacking DB OffSec Setup :: Damn Vulnera... pfSense - Login

pfSense COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Firewall / Rules / Edit

Edit Firewall Rule

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 Single host or alias 192.168.1.10 /

[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 Single host or alias 192.168.50.100 /

Destination Port Range HTTP (80) From Custom To Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log ☒ Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options [Display Advanced](#)

[Save](#)

Dopo l'applicazione della regola, tentiamo di connetterci da Kali a etasplotable da browser web e catturiamo i pacchetti con Wireshark. Verifichiamo che l'indirizzo di destinazione non è raggiungibile.

The screenshot shows a web browser window with the message "The connection has timed out" and "The server at 192.168.50.100 is taking too long to respond." Below this message are several bullet points explaining possible causes: the site might be unavailable, the user's network connection might be the issue, or a firewall/proxy might be blocking access. A "Try Again" button is visible.

Overlaid on the browser is the Wireshark network traffic capture. The packet list shows several TCP SYN packets from 192.168.1.10 to 192.168.50.100. The packet details pane for the selected packet (No. 1) shows the following information:

- Frame 3: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
- Ethernet II, Src: PcsCompu_53:0c:ba (08:00:27:53:0c:ba), Dst: PcsCompu_62:1a:f6 (08:00:27:62:1a:f6)
- Internet Protocol Version 4, Src: 192.168.1.10, Dst: 192.168.50.100
- Transmission Control Protocol, Src Port: 48380, Dst Port: 80
- Source Port: 48380
- Destination Port: 80
- [Stream index: 1]
- [Conversation completeness: Incomplete, SYN_SENT (1)]
- TCP Segment Len: 0
- Sequence Number: 0 (relative sequence number)
- Sequence Number (raw): 359837642
- [Next Sequence Number: 1 (relative sequence number)]
- Acknowledgment Number: 0
- Acknowledgment number (raw): 0
- 1010 = Header Length: 40 bytes (10)
- Flags: 0x002 (SYN)
- Window: 64240
- [Calculated window size: 64240]
- Checksum: 0xb4ed [unverified]
- [Checksum Status: Unverified]

Tentativi di connessione senza risposta:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.1.10	192.168.50.100	TCP	74	48406 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2543776347 TSecr=0 WS=128
2	4.127920813	192.168.1.10	192.168.50.100	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 48406 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2543780475 TSecr=0 WS=128
3	7.199875385	192.168.1.10	192.168.50.100	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 48406 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2543788668 TSecr=0 WS=128
4	12.320666125	192.168.1.10	192.168.50.100	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 48406 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2543799676 TSecr=0 WS=128
5	23.328716648	192.168.1.10	192.168.50.100	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 48406 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2543799676 TSecr=0 WS=128
6	28.448377715	PcsCompu_53:0c:ba	PcsCompu_62:1a:f6	ARP	42	Who has 192.168.1.1? Tell 192.168.1.10
7	28.448489132	192.168.1.10	192.168.50.100	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 48406 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2543804796 TSecr=0 WS=128
8	28.448489132	PcsCompu_62:1a:f6	PcsCompu_53:0c:ba	ARP	60	192.168.1.1 is at 08:00:27:62:1a:f6

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.1.10	192.168.50.100	TCP	74	48406 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2543776347 TSecr=0 WS=128
2	4.127920813	192.168.1.10	192.168.50.100	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 48406 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2543780475 TSecr=0 WS=128
3	7.199875385	192.168.1.10	192.168.50.100	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 48406 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2543788668 TSecr=0 WS=128
4	12.320666125	192.168.1.10	192.168.50.100	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 48406 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2543799676 TSecr=0 WS=128
5	23.328716648	192.168.1.10	192.168.50.100	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 48406 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2543799676 TSecr=0 WS=128

Length Info
74 48406 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2543776347 TSecr=0 WS=128
74 [TCP Retransmission] [TCP Port numbers reused] 48406 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2543780475 TSecr=0 WS=128
74 48380 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2543783547 TSecr=0 WS=128
74 [TCP Retransmission] [TCP Port numbers reused] 48406 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2543788668 TSecr=0 WS=128
74 [TCP Retransmission] [TCP Port numbers reused] 48380 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2543799676 TSecr=0 WS=128

Verifichiamo dal web tool di Pfsense l'applicazione della regola dal menu Status -> System Logs:

/192.168.1.1/status_logs_filter.php

ms Kali NetHunter Exploit-DB Google Hacking DB OffSec Setup :: Damn Vulnera... pfSense - Login

pfSense
COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Status / System Logs / Firewall / Normal View 🔍 ⚙️ ?

System **Firewall** DHCP Authentication IPsec PPP PPPoE/L2TP Server OpenVPN NTP Packages Settings

Normal View **Dynamic View** Summary View

Last 500 Firewall Log Entries. (Maximum 500)

Action	Time	Interface	Rule	Source	Destination	Protocol
✗	Jul 23 11:55:15	LAN	USER_RULE (1690113252)	192.168.1.10:48380	192.168.50.100:80	TCP:S
✗	Jul 23 11:55:15	LAN	USER_RULE (1690113252)	192.168.1.10:48392	192.168.50.100:80	TCP:S
✗	Jul 23 11:55:16	LAN	USER_RULE (1690113252)	192.168.1.10:48380	192.168.50.100:80	TCP:S
✗	Jul 23 11:55:16	LAN	USER_RULE (1690113252)	192.168.1.10:48392	192.168.50.100:80	TCP:S
✗	Jul 23 11:55:18	LAN	USER_RULE (1690113252)	192.168.1.10:48380	192.168.50.100:80	TCP:S
✗	Jul 23 11:55:18	LAN	USER_RULE (1690113252)	192.168.1.10:48392	192.168.50.100:80	TCP:S
✗	Jul 23 11:55:20	LAN	USER_RULE (1690113252)	192.168.1.10:48406	192.168.50.100:80	TCP:S
✗	Jul 23 11:55:21	LAN	USER_RULE (1690113252)	192.168.1.10:48406	192.168.50.100:80	TCP:S
✗	Jul 23 11:55:22	LAN	USER_RULE (1690113252)	192.168.1.10:48380	192.168.50.100:80	TCP:S
✗	Jul 23 11:55:23	LAN	USER_RULE (1690113252)	192.168.1.10:48406	192.168.50.100:80	TCP:S
✗	Jul 23 11:55:27	LAN	USER_RULE (1690113252)	192.168.1.10:48406	192.168.50.100:80	TCP:S
✗	Jul 23 11:55:30	LAN	USER_RULE (1690113252)	192.168.1.10:48380	192.168.50.100:80	TCP:S
✗	Jul 23 11:55:36	LAN	USER_RULE (1690113252)	192.168.1.10:48406	192.168.50.100:80	TCP:S
✗	Jul 23 11:55:47	LAN	USER_RULE (1690113252)	192.168.1.10:48380	192.168.50.100:80	TCP:S
✗	Jul 23 11:55:52	LAN	USER_RULE (1690113252)	192.168.1.10:48406	192.168.50.100:80	TCP:S
✗	Jul 23 11:56:19	LAN	USER_RULE (1690113252)	192.168.1.10:48380	192.168.50.100:80	TCP:S
✗	Jul 23 11:56:25	LAN	USER_RULE (1690113252)	192.168.1.10:48406	192.168.50.100:80	TCP:S