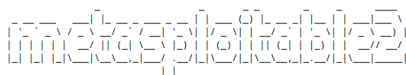
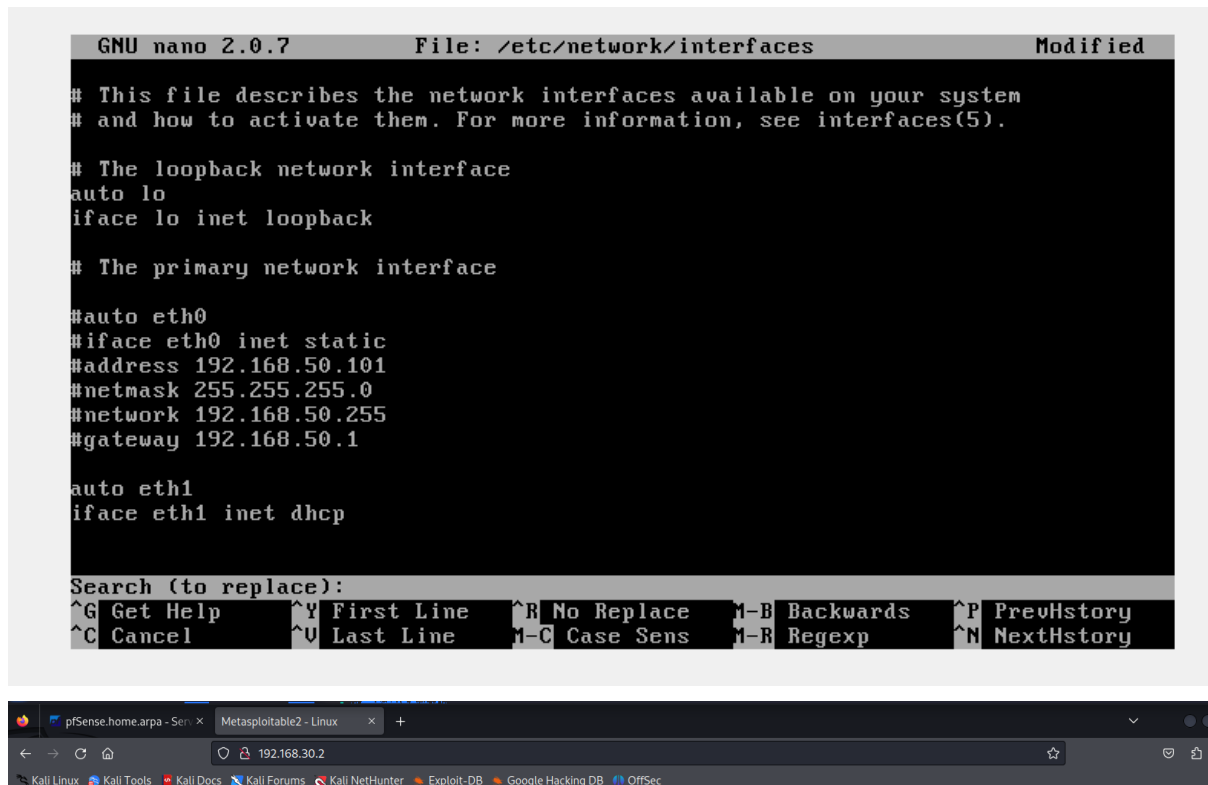


Esercitazione W9D4

Ilaria Pedrelli

# Creazione Policy Pfsense



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](#)

o/sense

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.](#)

Interfaces / LAN2 (em2)

≡

Limit

?

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

xxxxxxxxxxxx

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

## Creazione regola

Source

Source

☐ Invert match

Address or Alias ▾

192.168.50.100

/

▾

⚙ 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

Address or Alias ▾

192.168.30.2

/

▾

Destination Port Range

HTTP (80) ▾

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

Risultato: non riesco più a raggiungere la pagina

Cattura da Wireshark

Capturing from eth0						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
Apply a display filter ... <Ctrl-/>						
No.	Time	Source	Destination	Protocol	Length Info	
1	0.000000000	192.168.50.100	192.168.30.2	TCP	74	38092 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1314298728 TSecr=0 WS=128
2	0.261736493	192.168.50.100	192.168.30.2	TCP	74	38106 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1314298990 TSecr=0 WS=128
3	7.422864833	192.168.50.100	192.168.50.1	TCP	60	37450 → 80 [ACK] Seq=1 Ack=1 Win=6482 Len=0 TSval=1041182294 TSecr=58958396
4	7.424278342	192.168.50.1	192.168.50.100	TCP	60	[TCP ACKed unseen segment] 80 → 37450 [ACK] Seq=1 Ack=2 Win=514 Len=0 TSval=58968641 TSecr=
5	8.191135952	192.168.50.100	192.168.30.2	TCP	74	[TCP Retransmission] 38092 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1314298728 TSecr=0 WS=128
6	8.454769292	192.168.50.100	192.168.30.2	TCP	74	47684 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1314307183 TSecr=0 WS=128
7	8.743107091	192.168.50.100	192.168.30.2	TCP	74	47692 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1314307471 TSecr=0 WS=128
8	9.471992142	192.168.50.100	192.168.30.2	TCP	74	[TCP Retransmission] 47684 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1314298728 TSecr=0 WS=128
9	9.772493277	192.168.50.100	192.168.30.2	TCP	74	[TCP Retransmission] 47692 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1314298728 TSecr=0 WS=128
10	10.873883551	192.168.50.1	192.168.50.100	TCP	60	80 → 37450 [FIN, ACK] Seq=1 Ack=2 Win=514 Len=0 TSval=58972092 TSecr=1041110771
11	10.874111242	192.168.50.100	192.168.50.1	TCP	60	[TCP Previous segment not captured] 37450 → 80 [FIN, ACK] Seq=2 Ack=2 Win=6482 Len=0 TSval=1041182294 TSecr=58958396
12	10.874962465	192.168.50.1	192.168.50.100	TCP	60	[TCP ACKed unseen segment] 80 → 37450 [ACK] Seq=2 Ack=3 Win=514 Len=0 TSval=58972092 TSecr=
13	11.491259975	192.168.50.100	192.168.30.2	TCP	74	[TCP Retransmission] 47684 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1314298728 TSecr=0 WS=128
14	11.778720588	192.168.50.100	192.168.30.2	TCP	74	[TCP Retransmission] 47692 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1314298728 TSecr=0 WS=128
15	15.642775470	192.168.50.100	192.168.30.2	TCP	74	[TCP Retransmission] 47684 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1314298728 TSecr=0 WS=128
16	15.875263805	192.168.50.100	192.168.30.2	TCP	74	[TCP Retransmission] 47692 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1314298728 TSecr=0 WS=128
17	20.735076075	PcsCompu_cb:7e:f5	PcsCompu_d9:75:a7	ARP	42	Who has 192.168.50.1? Tell 192.168.50.100
18	20.736074887	PcsCompu_d9:75:a7	PcsCompu_cb:7e:f5	ARP	60	192.168.50.1 is at 08:00:27:d9:75:a7
19	23.891765003	192.168.50.100	192.168.30.2	TCP	74	[TCP Retransmission] 47684 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1314298728 TSecr=0 WS=128
20	24.060696938	192.168.50.100	192.168.30.2	TCP	74	[TCP Retransmission] 47692 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1314298728 TSecr=0 WS=128
21	24.242775470	192.168.50.100	192.168.30.2	TCP	74	[TCP Retransmission] 47684 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=1314298728 TSecr=0 WS=128
Frame 1: 74 bytes on wire (592 bits) captured (74 bytes) on interface eth0						
Ethernet II, Src: PcsCompu_d9:75:a7, Dst: 08:00:27:d9:75:a7, Protocol: TCP						
Internet Protocol Version 4, Src: 192.168.50.100, Destination: 192.168.30.2						

Cattura da Pfsense:

88 Matched Firewall Log Entries. (Maximum 500)						
Action	Time	Interface	Rule	Source	Destination	Protocol
✗	Jan 4 14:32:52	LAN	USER_RULE (1704377847)	192.168.50.100:44556	192.168.30.2:80	TCP:S
✗	Jan 4 14:32:52	LAN	USER_RULE (1704377847)	192.168.50.100:44566	192.168.30.2:80	TCP:S
✗	Jan 4 14:32:53	LAN	USER_RULE (1704377847)	192.168.50.100:44556	192.168.30.2:80	TCP:S
✗	Jan 4 14:32:53	LAN	USER_RULE (1704377847)	192.168.50.100:44566	192.168.30.2:80	TCP:S
✗	Jan 4 14:32:55	LAN	USER_RULE (1704377847)	192.168.50.100:44556	192.168.30.2:80	TCP:S
✗	Jan 4 14:32:55	LAN	USER_RULE (1704377847)	192.168.50.100:44566	192.168.30.2:80	TCP:S
✗	Jan 4 14:32:57	LAN	USER_RULE (1704377847)	192.168.50.100:44576	192.168.30.2:80	TCP:S
✗	Jan 4 14:32:58	LAN	USER_RULE (1704377847)	192.168.50.100:44576	192.168.30.2:80	TCP:S