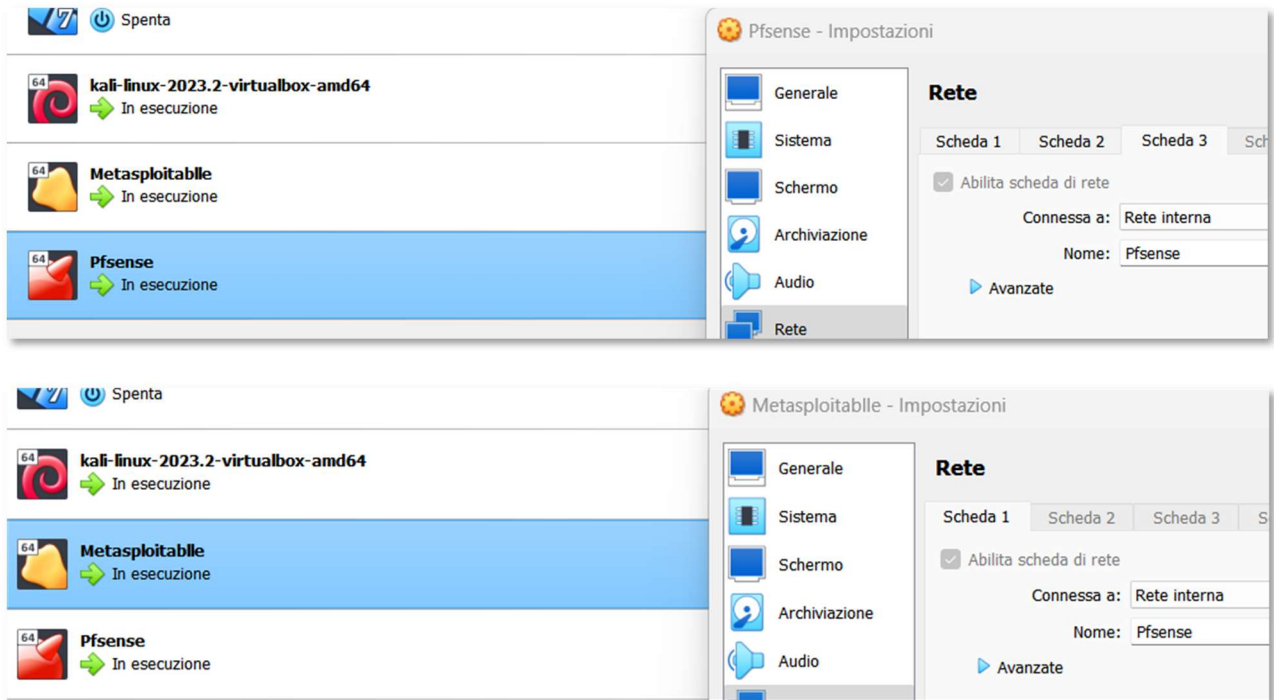


# Configurazione reti su Virtual Box e macchine virtuali

## LAN2 Pfsense (rete di comunicazione Pfsense-Metasploitable)

Rete 192.168.50.0/24



## Abilitazione servizio DHCP per LAN2 PfSense da tool web su Kali

The screenshot shows the PfSense web interface at the URL `https://192.168.1.1/services_dhcp.php?if=opt1`. The breadcrumb navigation is `Services / DHCP Server / LAN2`. There are tabs for `LAN` and `LAN2`, with `LAN2` being the active tab. The `General Options` section is expanded, showing the following configuration:

- Enable:** ☒ Enable DHCP server on LAN2 interface
- BOOTP:** ☐ Ignore BOOTP queries
- Deny unknown clients:**  (Dropdown menu)  
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.
- Ignore denied clients:** ☐ 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:** ☐ Do not record a unique identifier (UID) 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.
- Subnet:** 192.168.50.0
- Subnet mask:** 255.255.255.0
- Available range:** 192.168.50.1 - 192.168.50.254
- Range:** From 192.168.50.100 To 192.168.50.200

## Configurazione IP (statico) su /etc/network/interfaces della macchina Linux

```
GNU nano 2.9.4
# 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
```

## Configurazione IP DHCP su /etc/network/interfaces della macchina Metasploitable

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

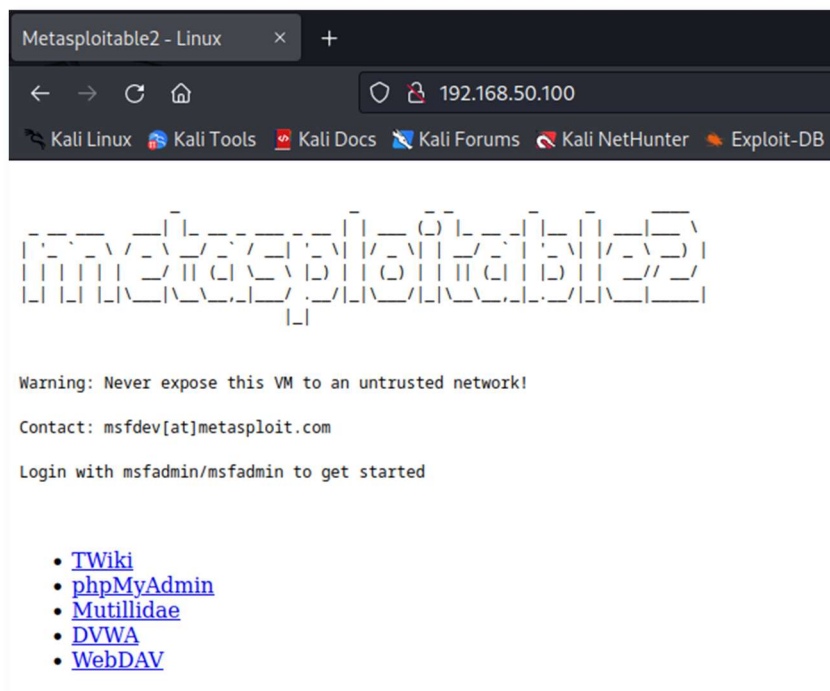
# The loopback network interface
auto lo
iface lo inet loopback

# 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
```

## Verifica connettività da Kali a Metasploitable

```
(kali㉿kali)-[~]
$ ping 192.168.50.100
PING 192.168.50.100 (192.168.50.100) 56(84) bytes of data:
64 bytes from 192.168.50.100: icmp_seq=1 ttl=63 time=2.01 ms
64 bytes from 192.168.50.100: icmp_seq=2 ttl=63 time=1.95 ms
64 bytes from 192.168.50.100: icmp_seq=3 ttl=63 time=1.75 ms
64 bytes from 192.168.50.100: icmp_seq=4 ttl=63 time=1.86 ms
64 bytes from 192.168.50.100: icmp_seq=5 ttl=63 time=1.79 ms
^X64 bytes from 192.168.50.100: icmp_seq=6 ttl=63 time=1.58 ms
64 bytes from 192.168.50.100: icmp_seq=7 ttl=63 time=1.78 ms
64 bytes from 192.168.50.100: icmp_seq=8 ttl=63 time=0.375 ms
```



## Creazione regola su Pfsense (da web tool su Kali) che blocca il traffico sulla porta 80 da Kali a Metasploitable con abilitazione dei log

92.168.1.1/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](#)

## Tentativo di connessione sulla porta 80 da Kali a Metasploitable dopo applicazione regola di firewall e verifica dell'irraggiungibilità da browser web. Analisi dei pacchetti con Wireshark.

The screenshot shows a web browser window with the address bar at 192.168.50.100. The page displays a message: "The connection has timed out. The server at 192.168.50.100 is taking too long to respond." Below this message are three bullet points: "The site could be temporarily unavailable or too busy. Try again in a few moments.", "If you are unable to load any pages, check your computer's network connection.", and "If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web." A "Try Again" button is visible.

Overlaid on the browser is the Wireshark network traffic capture. The packet list shows several TCP retransmissions from 192.168.1.10 to 192.168.50.100 on port 80. The packet details pane shows the selected packet (No. 74) as a TCP segment with the following details:

- 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): 3559837642
- [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	48380 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2543783547 TSecr=0 WS=128
4	12.320606125	192.168.1.10	192.168.50.100	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 48380 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2543788668 TSecr=0 WS=128
5	23.328716648	192.168.1.10	192.168.50.100	TCP	74	[TCP Retransmission] [TCP Port numbers reused] 48380 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=2543793676 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 08:00:27:02:1a:f6



## Verifica dell'applicazione della regola di Firewall anche dai log di pfsense abilitati con la creazione della regola

/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