

Esercizi

Sulla base di quanto visto, creare una regola firewall che **blocchi** l'accesso alla DVWA (su metasploitable) dalla macchina Kali Linux e ne impedisca di conseguenza lo scan. Un requisito fondamentale dell'esercizio è che le macchine Kali e Metasploitable siano su reti diverse, potete aggiungere una nuova interfaccia di rete a Pfsense in modo tale da gestire una ulteriore rete.

Connettetevi poi in Web Gui per attivare la nuova interfaccia e configurarla.

1. Creazione di una Rete Interna

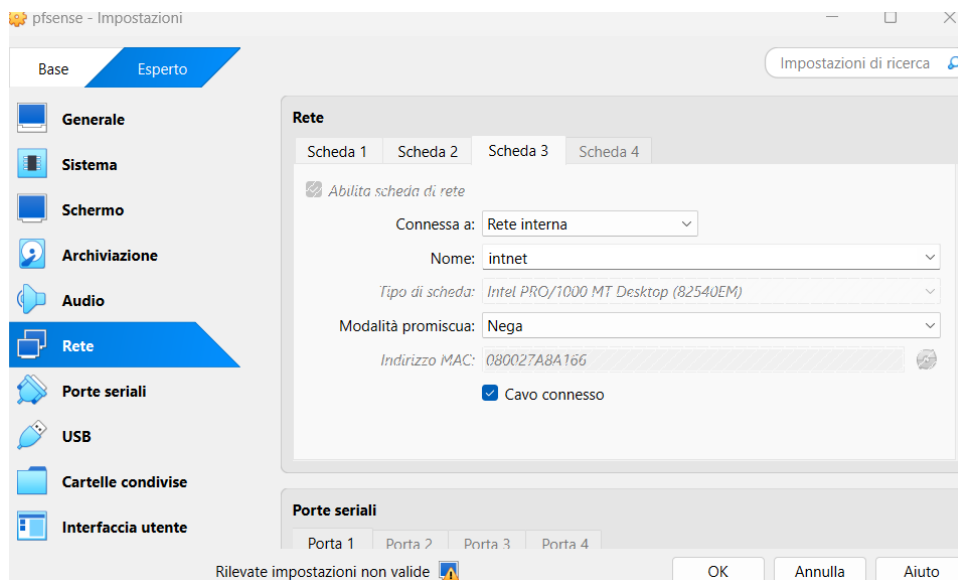
Per configurare una rete interna in pfSense, è necessario aggiungere una scheda di rete dedicata tramite l'interfaccia di amministrazione di pfSense. Una volta creata, la scheda deve essere abilitata e configurata come rete interna per collegare macchine virtuali come Kali e Metasploitable.

Di seguito è mostrata una schermata modificata della configurazione:

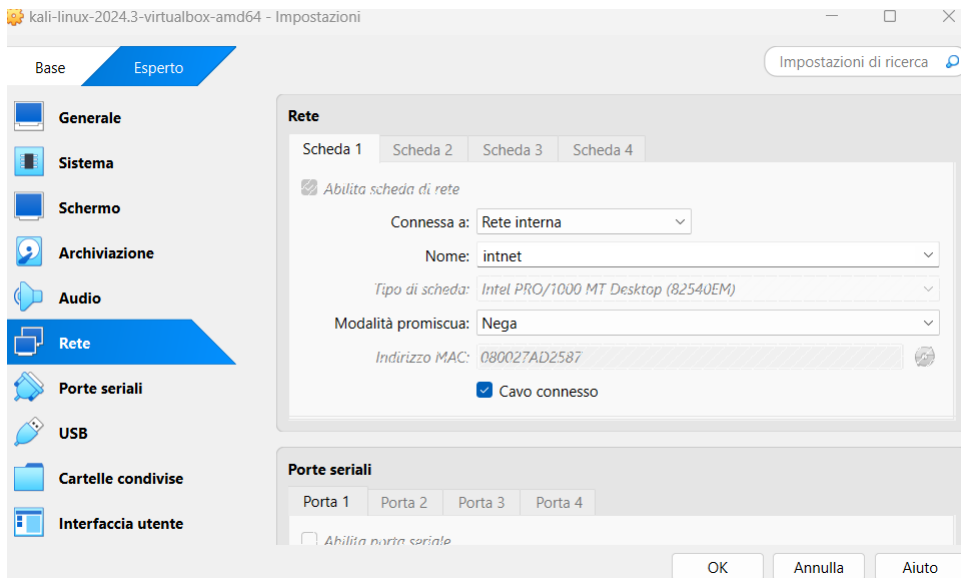
Sulla base di quanto visto, creare una regola firewall che **blocchi** l'accesso alla DVWA (su metasploitable) dalla macchina Kali Linux e ne impedisca di conseguenza lo scan. Un requisito fondamentale dell'esercizio è che le macchine Kali e Metasploitable siano su reti diverse, potete aggiungere una nuova interfaccia di rete a Pfsense in modo tale da gestire una ulteriore rete.

Connettetevi poi in Web Gui per attivare la nuova interfaccia e configurarla.

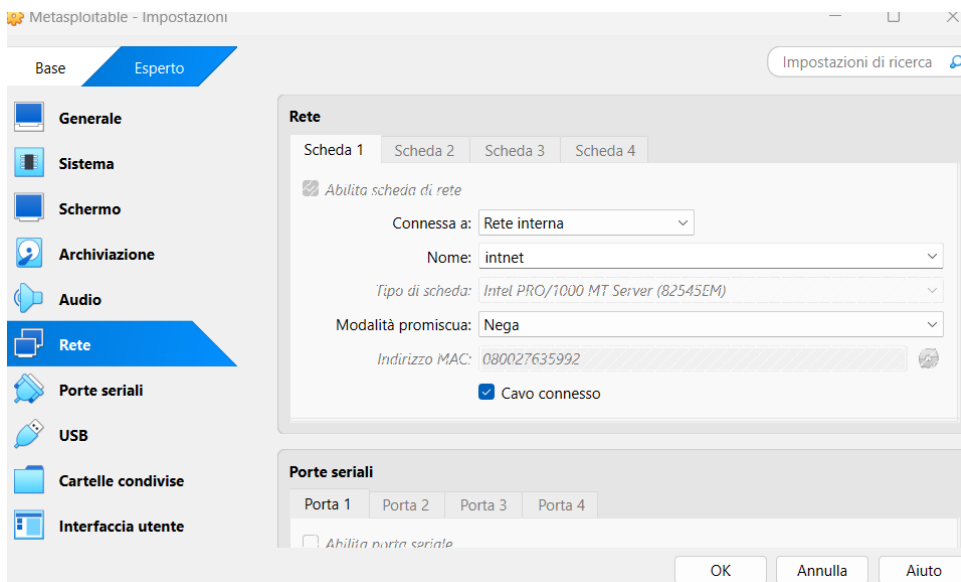
Di seguito è mostrata una schermata modificata della configurazione:



Di seguito è mostrata una schermata modificata della configurazione:



Di seguito è mostrata una schermata modificata della configurazione:



Di seguito è mostrata una schermata modificata della configurazione:

```
sfadmin@metasploitable:~$  
sfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet  HWaddr 08:00:27:63:59:92  
          inet addr:192.168.1.100  Bcast:192.168.1.255  Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:fe63:5992/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:66 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:135 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:12068 (11.7 KB)  TX bytes:31067 (30.3 KB)  
          Base address:0xd240 Memory:f0820000-f0840000  
  
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:270 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:270 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:99545 (97.2 KB)  TX bytes:99545 (97.2 KB)  
sfadmin@metasploitable:~$
```

Di seguito è mostrata una schermata modificata della configurazione:

```
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 static  
address 192.168.1.100  
netmask 255.255.255.0  
network 192.168.1.0  
gateway 192.168.1.1  
broadcast 192.168.1.255
```

Di seguito è mostrata una schermata modificata della configurazione:

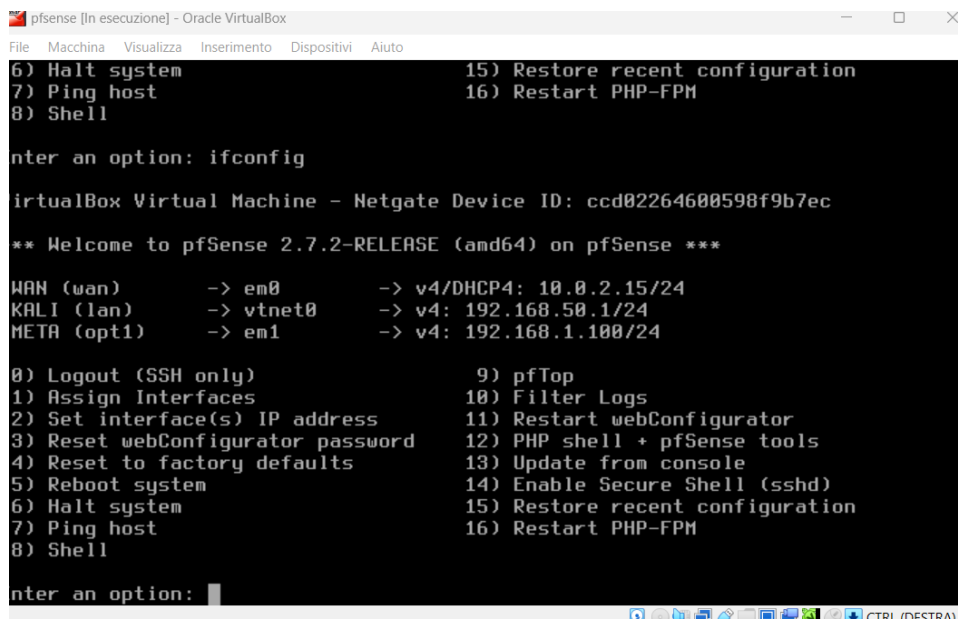
```

(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.50.150 netmask 255.255.255.0 broadcast 192.168.50.255
    inet6 fe80::b055:f33b:4307:7a25 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:ad:25:87 txqueuelen 1000 (Ethernet)
    RX packets 2538 bytes 1176079 (1.1 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1938 bytes 240750 (235.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 480 (480.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 480 (480.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

Di seguito è mostrata una schermata modificata della configurazione:



The screenshot shows a terminal window titled "pfSense [In esecuzione] - Oracle VirtualBox". The menu lists various system and network configuration options. The "WAN (wan)" interface is configured with "em0" and "v4/DHCP4: 10.0.2.15/24". The "KALI (lan)" interface is configured with "vtnet0" and "v4: 192.168.50.1/24". The "META (opt1)" interface is configured with "em1" and "v4: 192.168.1.100/24". The menu also includes options for logging out, assigning interfaces, setting IP addresses, resetting the web configurator password, resetting to factory defaults, rebooting the system, halting the system, pinging the host, running pfTop, filtering logs, restarting the web configurator, running the PHP shell, updating from the console, enabling secure shell, restoring recent configuration, and restarting PHP-FPM.

```

pfSense [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
6) Halt system
7) Ping host
8) Shell

15) Restore recent configuration
16) Restart PHP-FPM

Enter an option: ifconfig

VirtualBox Virtual Machine - Netgate Device ID: ccd02264600598f9b7ec

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

WAN (wan) -> em0 -> v4/DHCP4: 10.0.2.15/24
KALI (lan) -> vtnet0 -> v4: 192.168.50.1/24
META (opt1) -> em1 -> v4: 192.168.1.100/24

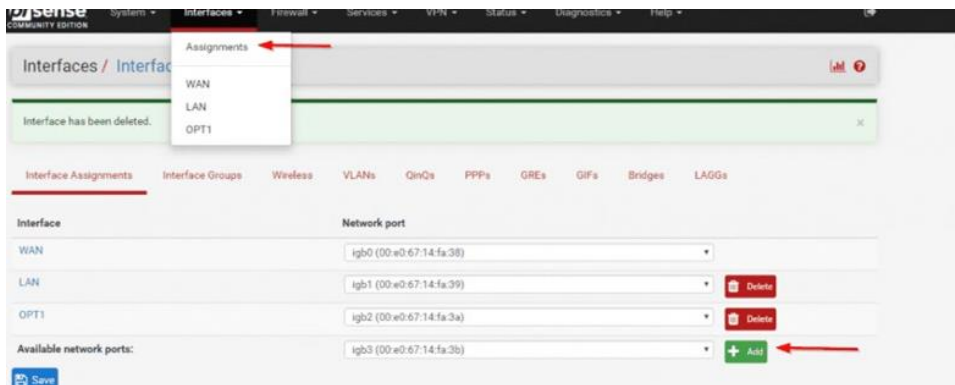
0) Logout (SSH only)
1) Assign Interfaces
2) Set interface(s) IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell

9) pfTop
10) Filter Logs
11) Restart webConfigurator
12) PHP shell + pfSense tools
13) Update from console
14) Enable Secure Shell (sshd)
15) Restore recent configuration
16) Restart PHP-FPM

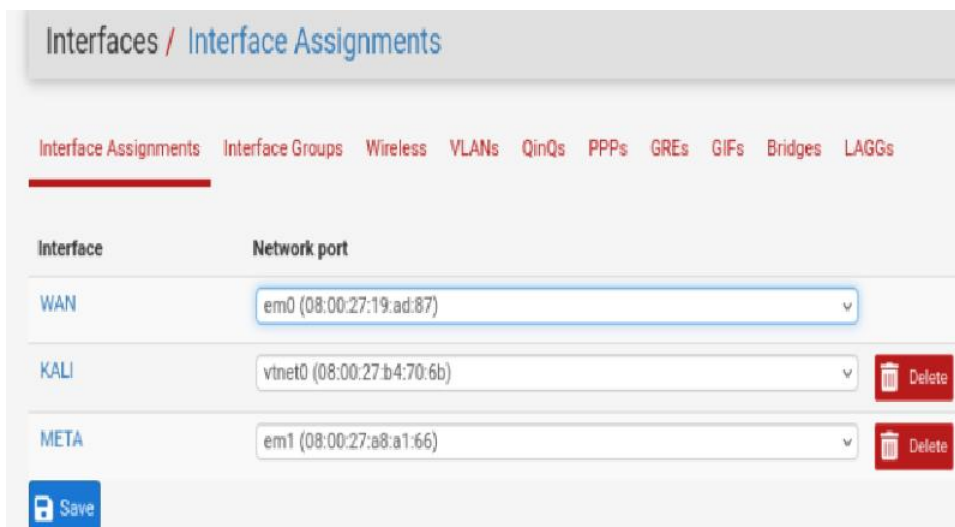
Enter an option:

```



Di seguito è mostrata una schermata modificata della configurazione:



Di seguito è mostrata una schermata modificata della configurazione:



Di seguito è mostrata una schermata modificata della configurazione:

Interfaces / META (em1)  

General Configuration

Enable ☒ Enable interface

Description
Enter a description (name) for the interface here.

IPv4 Configuration Type

IPv6 Configuration Type

MAC Address
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

Di seguito è mostrata una schermata modificata della configurazione:

Static IPv4 Configuration

IPv4 Address /

IPv4 Upstream gateway [+ Add a new gateway](#)

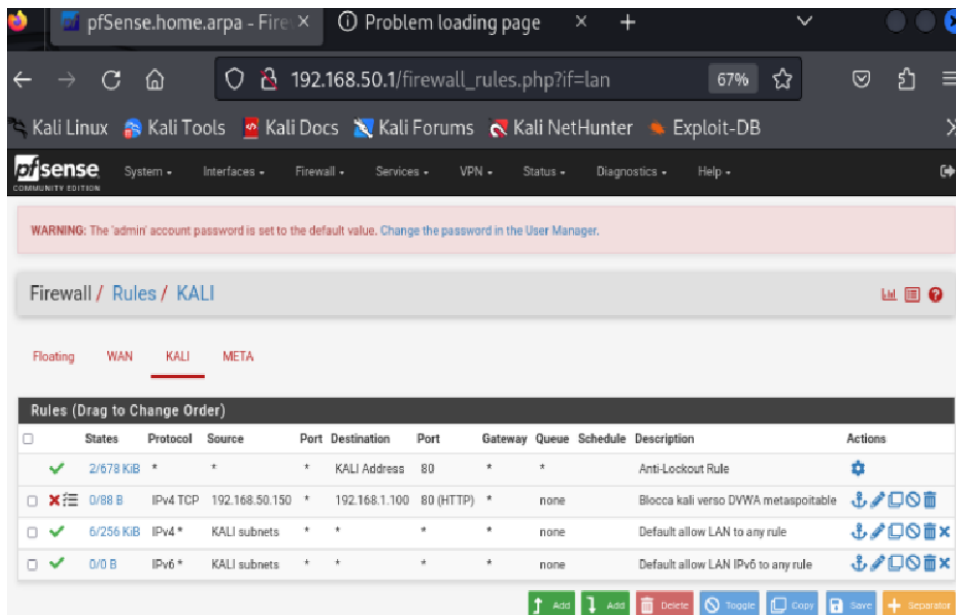
If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button.
On local area network interfaces the upstream gateway should be "none".
Selecting an upstream gateway causes the firewall to treat this interface as a [WAN type interface](#).
Gateways can be managed by [clicking here](#).

Reserved Networks

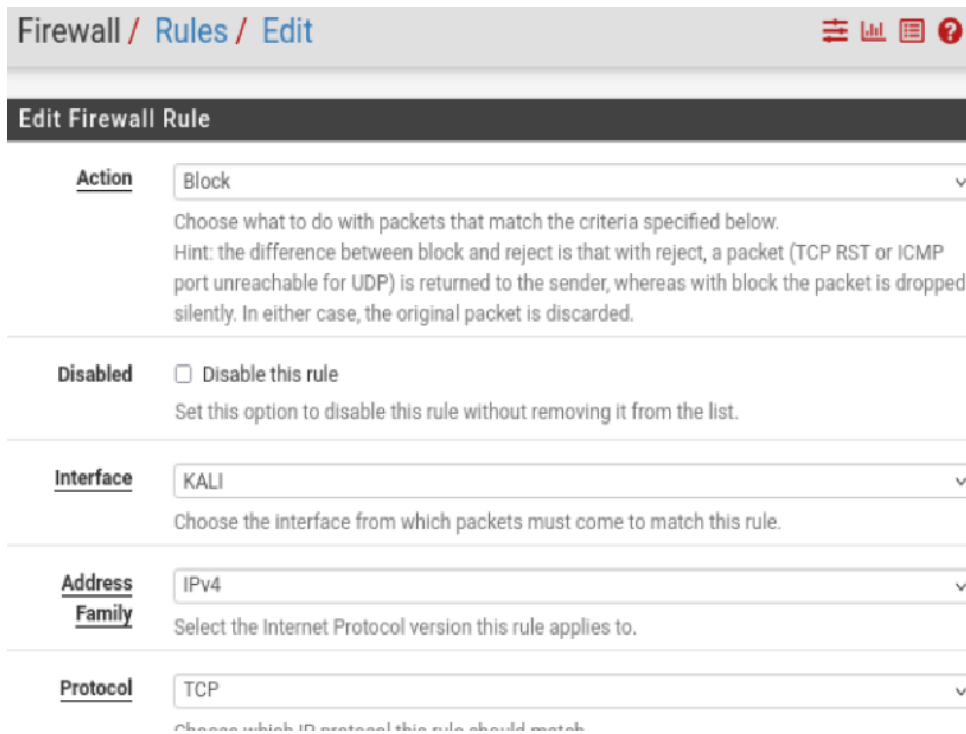
Block private networks and opback addresses ☐
Blocks traffic from IP addresses that are reserved for private networks per RFC 1918 (10/8, 172.16/12, 192.168/16) and unique local addresses per RFC 4193 (fc00::/7) as well as loopback addresses (127/8). This option should generally be turned on, unless this network interface resides in such a private address space, too.

Block bogon networks ☐
Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received.
This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic.
Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

Di seguito è mostrata una schermata modificata della configurazione:



Di seguito è mostrata una schermata modificata della configurazione:



Di seguito è mostrata una schermata modificata della configurazione:

Source

Source

☐ Invert match

Address or Alias
192.168.50.150
/

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
192.168.1.100
/

Destination Port Range

HTTP (80)
From
Custom

HTTP (80)
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

Di seguito è mostrata una schermata modificata della configurazione:

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

Blocca kali verso DVWA metasploitable

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

Di seguito è mostrata una schermata modificata della configurazione:


```
(kali㉿kali)-[~]
└─$ sudo nmap -p 80 192.168.1.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-13 09:56 EST
Nmap scan report for 192.168.1.100
Host is up (0.00098s latency).

PORT      STATE SERVICE
80/tcp    filtered http

Nmap done: 1 IP address (1 host up) scanned in 0.43 seconds
```

Di seguito è mostrata una schermata modificata della configurazione:

| | | | | | | |
|---|-----------------|------|---|------------------------|--------------------|-------|
| ✖ | Dec 13 15:50:01 | KALI | 👤 Blocca kali verso DVWA metasploitable (1734094735) | 🚫 192.168.50.150:39096 | 🔕 192.168.1.100:80 | TCP:S |
| ✖ | Dec 13 15:50:01 | KALI | 👤 Blocca kali verso DVWA metasploitable (1734094735) | 🚫 192.168.50.150:39104 | 🔕 192.168.1.100:80 | TCP:S |
| ✖ | Dec 13 15:50:02 | KALI | 👤 Blocca kali verso DVWA metasploitable (1734094735) | 🚫 192.168.50.150:39096 | 🔕 192.168.1.100:80 | TCP:S |
| ✖ | Dec 13 15:50:02 | KALI | 👤 Blocca kali verso DVWA metasploitable (1734094735) | 🚫 192.168.50.150:39104 | 🔕 192.168.1.100:80 | TCP:S |
| ✖ | Dec 13 15:50:03 | KALI | 👤 Blocca kali verso DVWA metasploitable (1734094735) | 🚫 192.168.50.150:39096 | 🔕 192.168.1.100:80 | TCP:S |
| ✖ | Dec 13 15:50:03 | KALI | 👤 Blocca kali verso DVWA metasploitable (1734094735) | 🚫 192.168.50.150:39104 | 🔕 192.168.1.100:80 | TCP:S |
| ✖ | Dec 13 15:50:04 | KALI | 👤 Blocca kali verso DVWA metasploitable (1734094735) | 🚫 192.168.50.150:39096 | 🔕 192.168.1.100:80 | TCP:S |
| ✖ | Dec 13 15:50:05 | KALI | 👤 Blocca kali verso DVWA metasploitable (1734094735) | 🚫 192.168.50.150:39104 | 🔕 192.168.1.100:80 | TCP:S |
| ✖ | Dec 13 15:50:05 | KALI | 👤 Blocca kali verso DVWA metasploitable (1734094735) | 🚫 192.168.50.150:39096 | 🔕 192.168.1.100:80 | TCP:S |
| ✖ | Dec 13 15:50:06 | KALI | 👤 Blocca kali verso DVWA metasploitable (1734094735) | 🚫 192.168.50.150:39104 | 🔕 192.168.1.100:80 | TCP:S |

2. Configurazione degli Indirizzi IP

Ogni macchina virtuale deve essere configurata con un indirizzo IP statico per garantire una comunicazione stabile all'interno della rete. Di seguito vengono riportati i passaggi per configurare gli IP su Metasploitable e Kali.

3. Creazione di Regole del Firewall

Per proteggere la rete e controllare l'accesso tra le macchine virtuali, vengono create regole specifiche nel firewall di pfSense. È importante salvare i log per monitorare eventuali tentativi di accesso bloccati.

4. Verifica del Funzionamento

Dopo aver configurato il firewall, è possibile testare le regole tramite strumenti come 'nmap'. I log di sistema in pfSense possono fornire ulteriori dettagli sul traffico bloccato.