PROGETTO S3/L5 – CREAZIONE POLICY PFSENSE

1. INTRODUZIONE

Nel presente esercizio è stata realizzata la **configurazione di un ambiente virtuale** composto dalle **VM pfSense, Kali Linux e Metasploitable2**, con l'obiettivo di implementare e verificare il **funzionamento di regole firewall su pfSense** in un contesto multi-subnet.
In particolare, l'attività richiedeva di predisporre un'infrastruttura a più subnet, assicurando che la macchina **Kali e** la macchina **Metasploitable2 risiedessero su reti distinte**, in modo da permettere al firewall di svolgere efficacemente funzioni di filtraggio del traffico.

Dopo aver configurato le tre interfacce di pfSense (WAN, LAN e OPT1) e aver assegnato gli indirizzi IP alle relative reti, è stata **verificata la raggiungibilità** della macchina Metasploitable2 da Kali Linux tramite traffico **ICMP** e **HTTP**.

Successivamente, è stata creata una specifica regola firewall con lo scopo di bloccare l'accesso alla web application DVWA ospitata sulla Metasploitable2, impedendo alla macchina Kali di raggiungerne l'homepage.

Il report documenta l'intera procedura attraverso screenshot mirati, mostrando:

- la configurazione iniziale delle interfacce di pfSense;
- la situazione delle regole firewall prima e dopo la modifica;
- il comportamento di Kali Linux nel ping e nell'accesso alla homepage di Metasploitable2, prima e dopo l'applicazione della regola.

L'**obiettivo** finale è dimostrare il **corretto funzionamento del firewall pfSense nel filtraggio del traffico inter-subnet** e la capacità di bloccare selettivamente servizi esposti in rete.

2. CONFIGURAZIONE PRELIMINARE DELL'AMBIENTE VIRTUALE

Prima di procedere con i test di raggiungibilità e con l'applicazione delle regole firewall, è stato necessario **predisporre** correttamente **l'ambiente virtuale** composto da tre VM: **pfSense**, **Kali Linux** e **Metasploitable2**.

L'obiettivo di questa fase era creare una topologia di rete in cui **pfSense agisse come firewall/router tra due subnet distinte**: una dedicata alla Kali Linux (**kalinet**) e una dedicata alla Metasploitable2 (**metanet**).

Al termine di questa fase, la configurazione costituirà la base necessaria per i successivi test di raggiungibilità e per l'implementazione della regola firewall richiesta dall'esercitazione.

2.1 Configurazione delle reti interne in VirtualBox

Sono state create due reti interne separate:

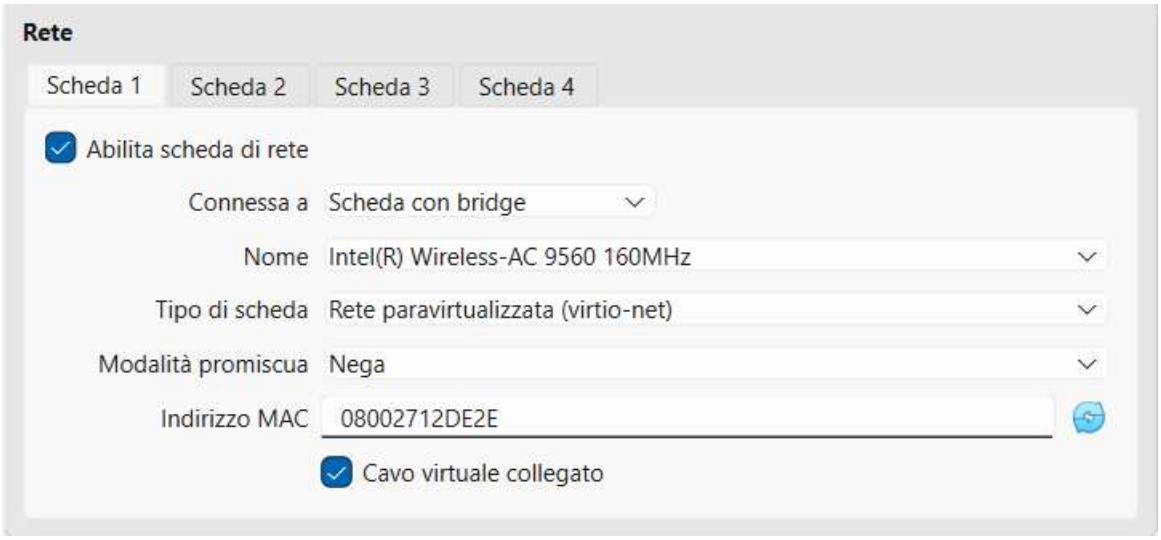
- **kalinet** — rete interna utilizzata per collegare la macchina Kali Linux alla macchina pfSense.
- **metanet** — rete interna dedicata alla comunicazione tra pfSense e Metasploitable2 tramite l'interfaccia OPT1.

Questa suddivisione permette a pfSense di operare come punto di controllo del traffico tra due reti interne distinte.
Per realizzare le suddette internal network, a ogni VM è stata assegnata la scheda di rete corretta.

2.1.1 Configurazione delle schede di rete della VM Pfsense

Alla macchina virtuale pfSense sono state assegnate tre schede di rete, configurate come segue:

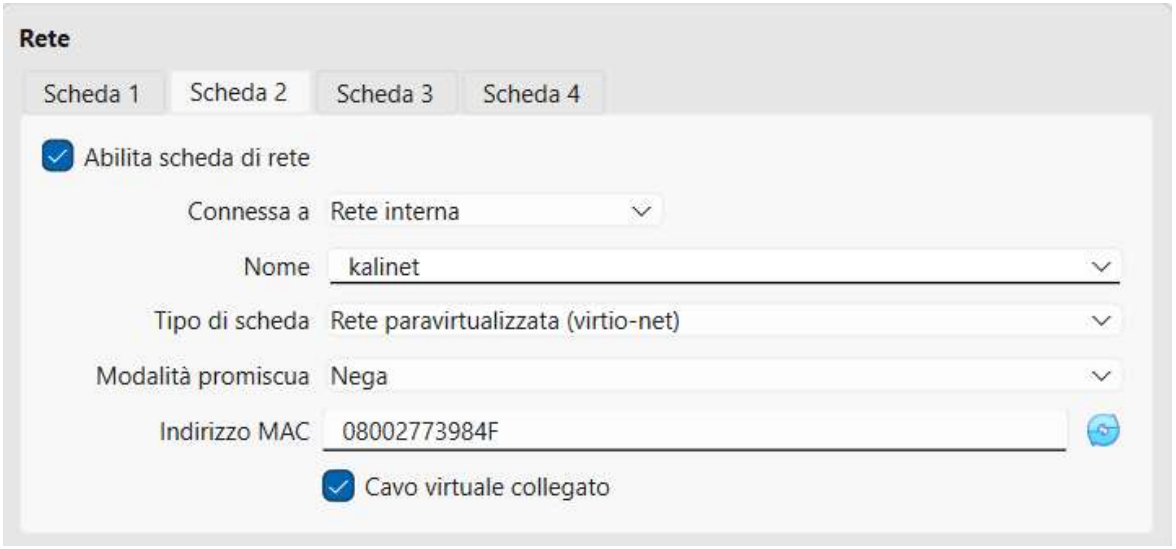
- **Scheda 1 (WAN)**
  - Connessa a: Scheda con bridge
  - Funzione: collegamento alla rete esterna (router domestico)



Impostazione della Scheda 1 nella sezione Rete della VM Pfsense

■ Scheda 2 (LAN)

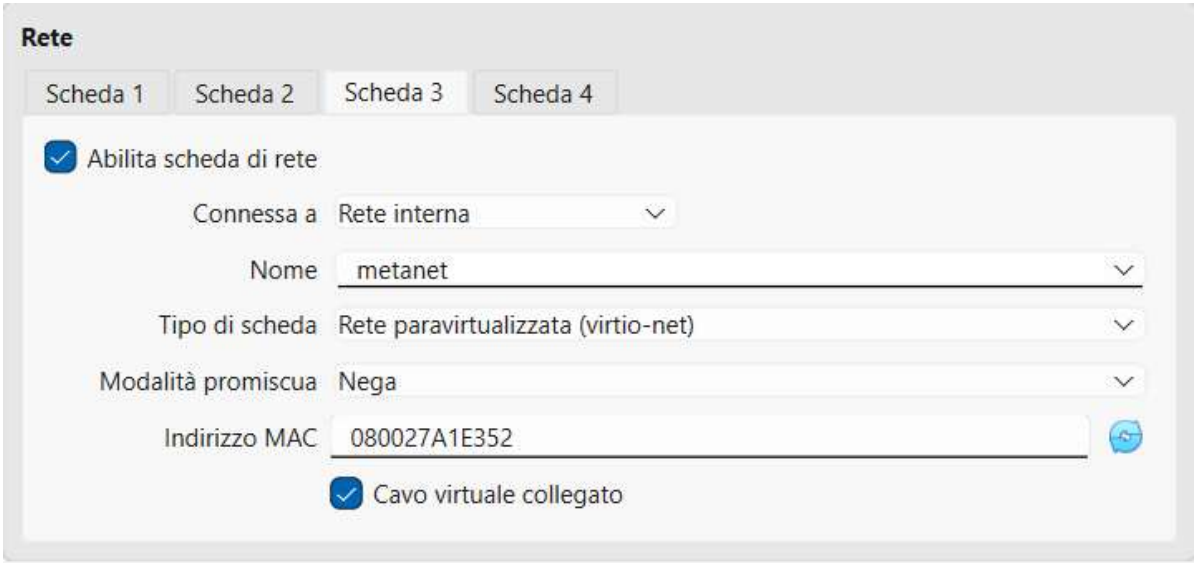
- Connessa a: Rete interna
- Nome rete: Kalinet
- Funzione: collegamento alla macchina Kali Linux



Impostazione della Scheda 2 nella sezione Rete della VM Pfsense

■ Scheda 3 (OPT1)

- Connessa a: Rete interna
- Nome Rete: Metanet
- Funzione: collegamento alla macchina Metasploitable2



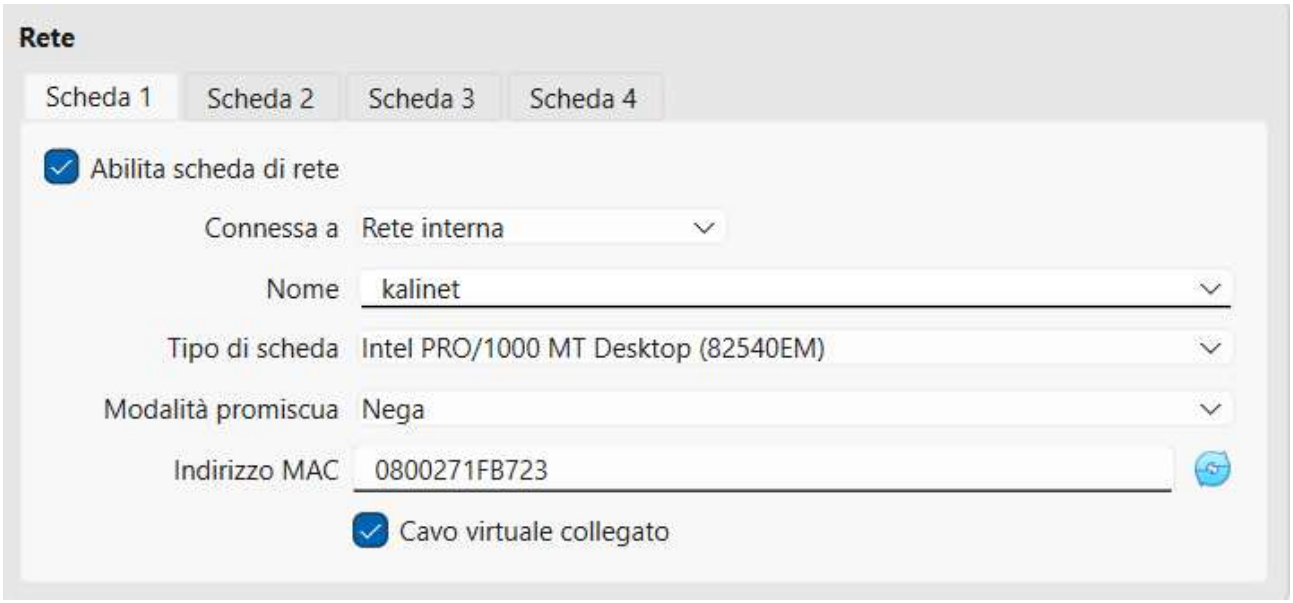
Impostazione della Scheda 3 nella sezione Rete della VM Pfsense

2.1.2 Configurazione della scheda di rete della VM Kali Linux

La macchina Kali Linux è stata configurata con una singola scheda di rete, collegata alla rete interna utilizzata per la LAN di pfSense:

- Connessa a: Rete interna
- Nome rete: kalinet

In questo modo Kali Linux risiede nella subnet della LAN di pfSense ed utilizza quest'ultima come gateway per raggiungere le altre reti.



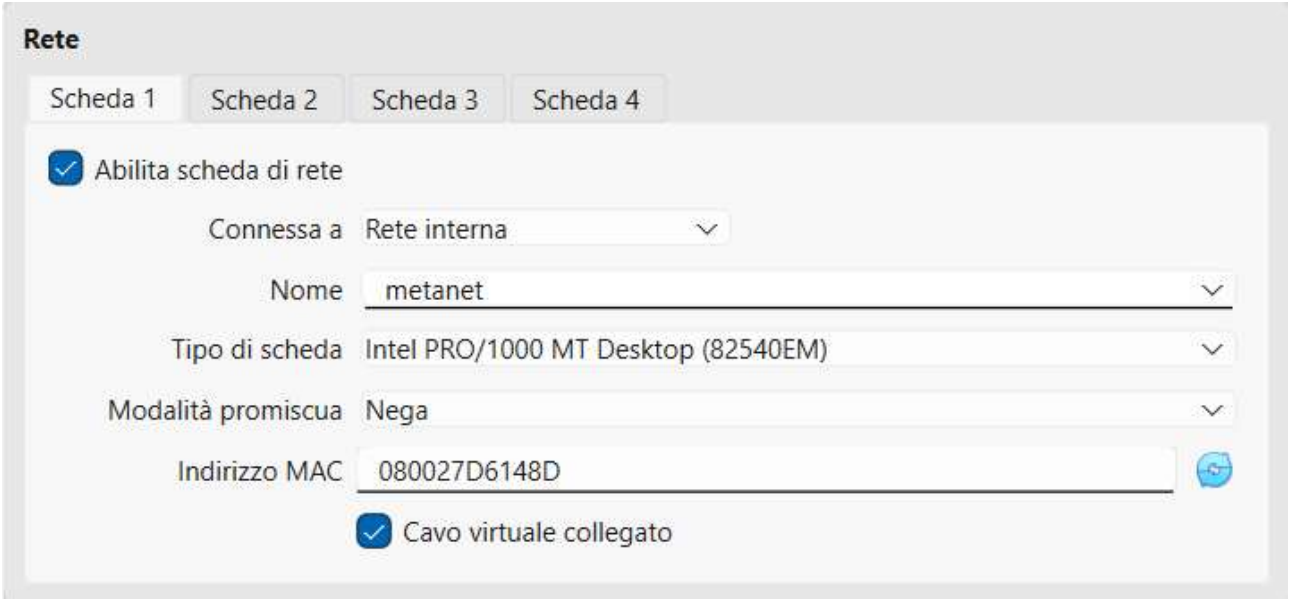
Impostazione della Scheda 1 nella sezione Rete della VM Kali

2.1.3 Configurazione della scheda di rete della VM Metasploitable2

La macchina Metasploitable2 è stata configurata con una singola scheda di rete, dedicata esclusivamente alla rete interna collegata all'interfaccia OPT1 di pfSense:

- Connessa a: Rete interna
- Nome rete: metanet

Questa configurazione consente di isolare Metasploitable2 dalla rete della Kali Linux, rendendo necessario il passaggio attraverso pfSense per qualsiasi comunicazione tra le due macchine.



Impostazione della Scheda 1 nella sezione Rete della VM Metasploitable2

2.2 Configurazione delle interfacce su Pfsense (CLI + GUI)

Dopo aver configurato le schede di rete delle macchine virtuali in VirtualBox, si è proceduto alla configurazione delle interfacce di rete direttamente su pfSense. Questa fase ha previsto inizialmente l'assegnazione delle interfacce dalla console testuale (CLI) e successivamente la configurazione dettagliata tramite l'interfaccia web (GUI).

2.2.1 Assegnazione delle interfacce tramite CLI su pfsense

Al primo avvio di pfSense, tramite la console testuale (CLI), è stata eseguita la procedura di Assign Interfaces per associare le prime due schede di rete virtuali alle

rispettive interfacce logiche del firewall.

In questa fase sono state configurate:

- **WAN (vtnet0)**
  Interfaccia collegata alla scheda configurata in modalità Scheda con bridge, utilizzata per l'accesso alla rete esterna.
  L'indirizzamento IP dell'interfaccia WAN (**192.168.1.88**) è stato ottenuto automaticamente tramite DHCP dal router domestico (**192.168.1.254**), consentendo a pfSense l'accesso alla rete esterna.

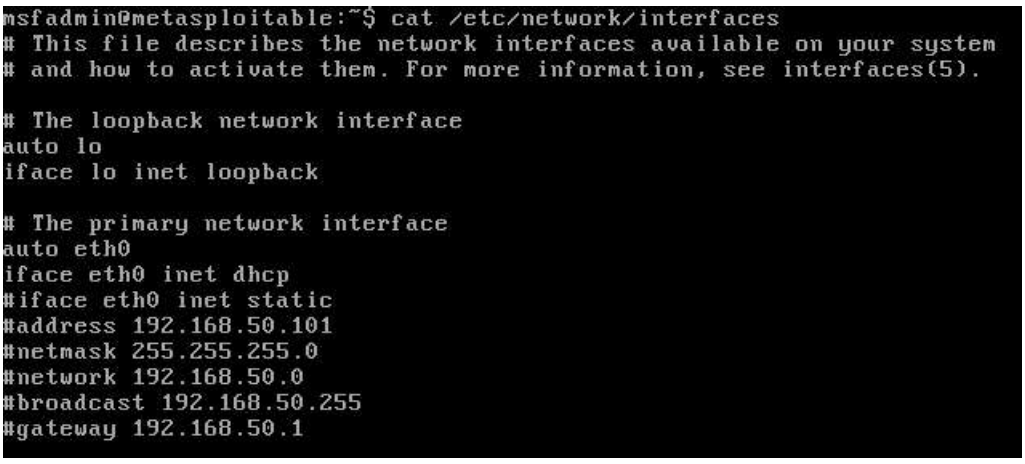
- **LAN (vtnet1)**
  Interfaccia collegata alla rete interna kalinet, dedicata alla comunicazione con la macchina Kali Linux.
  All'interfaccia LAN è stato assegnato l'indirizzo IP statico 192.168.50.1 /24 che rappresenta il gateway della subnet utilizzata dalla Kali Linux.

L'assegnazione di queste due interfacce è avvenuta direttamente dalla CLI di pfSense durante la configurazione iniziale.

2.2.2 Aggiunta e configurazione dell'interfaccia OPT1 tramite GUI pfSense

Successivamente, dopo aver configurato le prime due interfacce tramite CLI, è stata aggiunta una **terza interfaccia OPT1 (vtnet2)** direttamente dalla GUI di pfSense.

Per garantire una configurazione di rete stabile e coerente con l'infrastruttura definita su pfSense, sulla macchina Metasploitable2 si è optato per modificare la configurazione dell'interfaccia di rete tramite il file ***/etc/network/interfaces*** mettendolo in DHCP come segue:



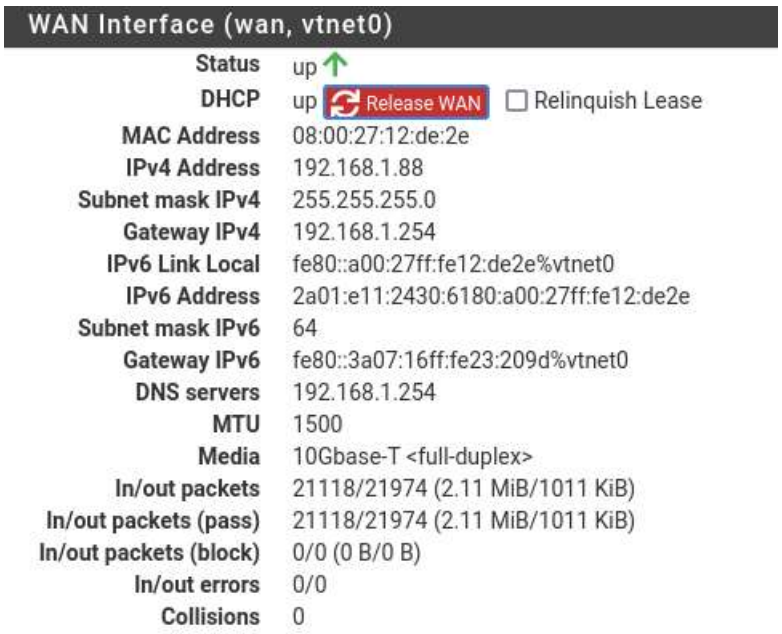
L’interfaccia OPT1 è stata abilitata tramite la GUI di pfSense, in quanto dalla CLI non risultava immediato portare l’interfaccia in stato UP.
Una volta abilitata, la configurazione dell’indirizzamento IPv4 e dei relativi parametri di rete è stata completata tramite CLI.

In particolare, all’interfaccia **OPT1** è stato assegnato un indirizzo IPv4 statico (**192.168.51.1 /24**) che la identifica come gateway per la subnet dedicata alla macchina Metasploitable2 e fornisce a quest’ultima il **servizio DHCP** per l’assegnazione dell’indirizzo.

2.2.3 Verifica dello stato delle interfacce

Al termine della configurazione, dalla sezione Status → Interfaces della GUI di pfSense è stato verificato che tutte le interfacce risultassero attive (UP) e correttamente configurate:

- WAN: attiva e con indirizzo assegnato
- LAN: attiva e raggiungibile dalla Kali Linux
- OPT1: attiva e collegata alla rete della Metasploitable2



Interfaccia WAN (alla rete esterna tramite router domestico)

LAN Interface (lan, vtnet1)	
Status	up
MAC Address	08:00:27:73:98:4f
IPv4 Address	192.168.50.1
Subnet mask IPv4	255.255.255.0
IPv6 Link Local	fe80::a00:27ff:fe73:984f%vtnet1
MTU	1500
Media	10Gbase-T <full-duplex>
In/out packets	1029/1561 (129 KiB/1.29 MiB)
In/out packets (pass)	1029/1561 (129 KiB/1.29 MiB)
In/out packets (block)	0/0 (0 B/0 B)
In/out errors	0/0
Collisions	0

Interfaccia LAN verso Kali

OPT1 Interface (opt1, vtnet2)	
Status	up
MAC Address	08:00:27:a1:e3:52
IPv4 Address	192.168.51.1
Subnet mask IPv4	255.255.255.0
IPv6 Link Local	fe80::a00:27ff:fea1:e352%vtnet2
MTU	1500
Media	10Gbase-T <full-duplex>
In/out packets	7/2 (2 KiB/376 B)
In/out packets (pass)	7/2 (2 KiB/376 B)
In/out packets (block)	65/0 (10 KiB/0 B)
In/out errors	0/0
Collisions	0

Interfaccia OPT1 verso Metasploitable2

Le medesime informazioni si possono visualizzare tramite la CLI della Pfsense.

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

 WAN (wan)       -> vtnet0     -> v4/DHCP4: 192.168.1.88/24
                                  v6/DHCP6: 2a01:e11:2430:6180:a00:27ff:fe12:de2
e/64
 LAN (lan)       -> vtnet1     -> v4: 192.168.50.1/24
 OPT1 (opt1)     -> vtnet2     -> v4: 192.168.51.1/24
```

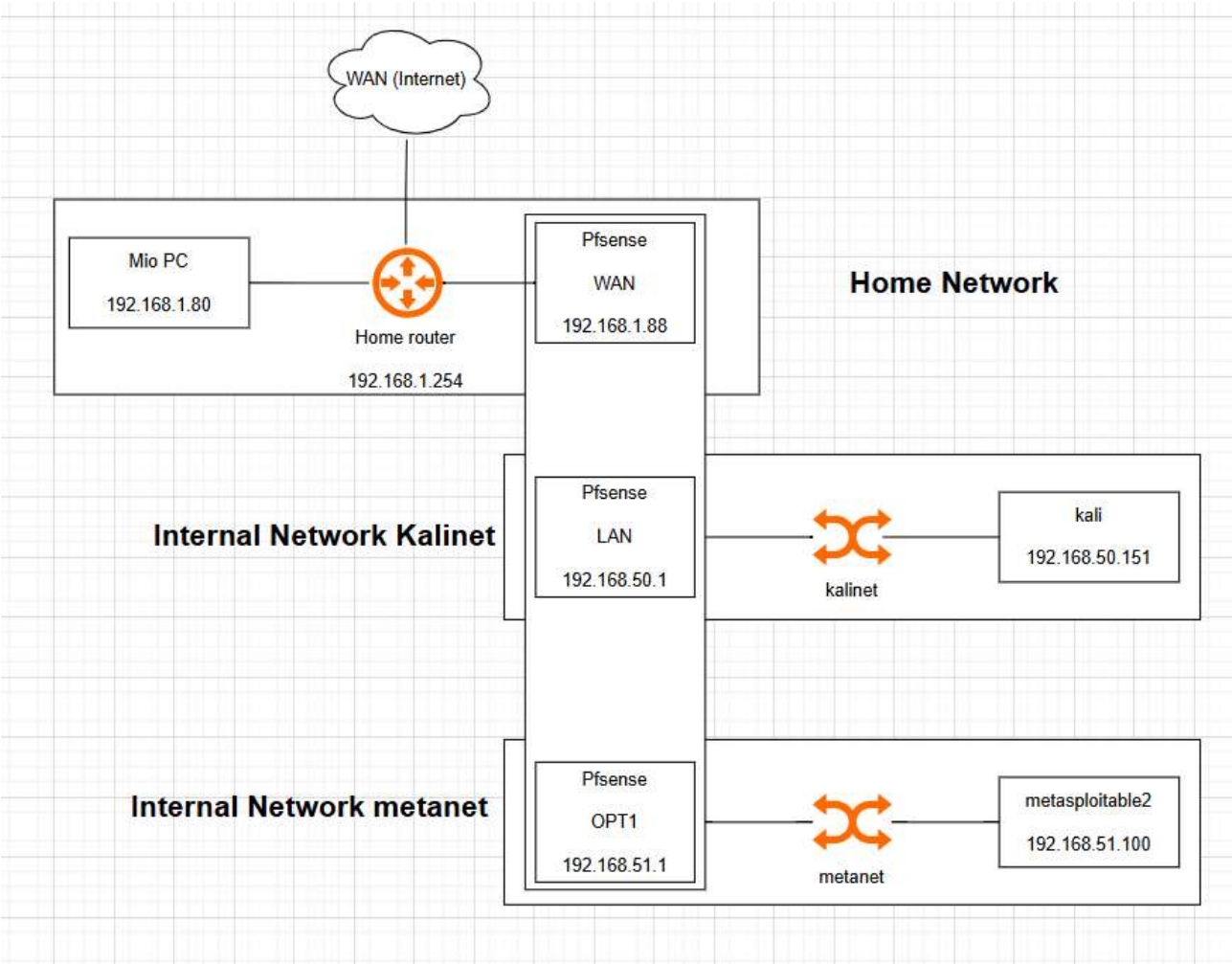
Interfacce presenti sulla Pfsense visibili da CLI

```
Valid interfaces are:

vtnet0  08:00:27:12:de:2e   (up) VirtIO Networking Adapter
vtnet1  08:00:27:73:98:4f   (up) VirtIO Networking Adapter
vtnet2  08:00:27:a1:e3:52   (up) VirtIO Networking Adapter
```

Status delle connessioni logiche

2.2.4 Topologia Rete



3. TEST DI RAGGIUNGIBILITÀ PRIMA DELL'APPLICAZIONE DELLA REGOLA DI FIREWALL

Una volta completata la configurazione delle macchine virtuali e delle interfacce di rete su pfSense, sono stati eseguiti i test di raggiungibilità preliminari per verificare il corretto funzionamento della topologia di rete prima dell'applicazione di qualsiasi regola di blocco.

L'obiettivo di questa fase era confermare che la **macchina Kali Linux fosse in grado di raggiungere la macchina Metasploitable2 attraverso pfSense**, sia a livello di connettività di rete (ICMP) sia a livello applicativo (HTTP).

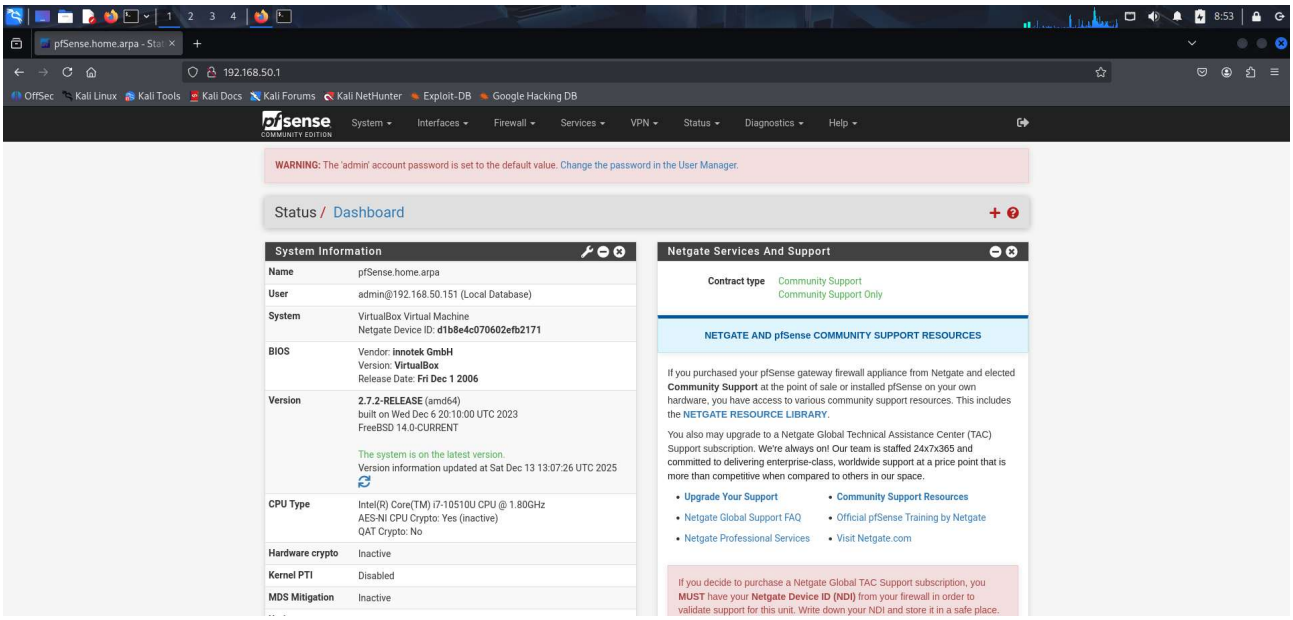
3.1 Verifica preliminare di connettività tramite accesso alla GUI di pfSense

Prima di eseguire i test di raggiungibilità verso la macchina Metasploitable2, è stata

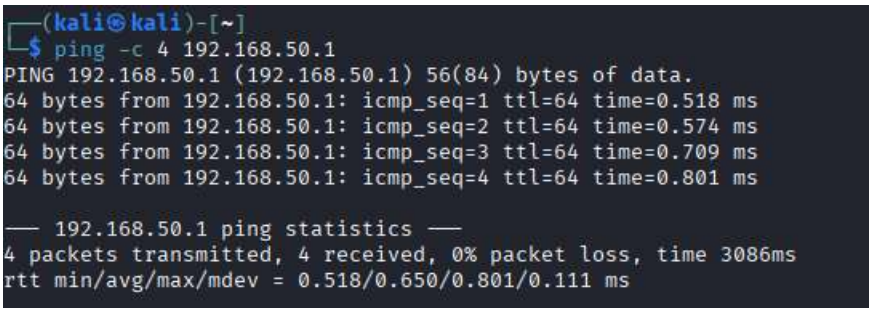
verificata la corretta comunicazione tra la macchina Kali Linux e il firewall pfSense tramite l'accesso all'interfaccia di gestione web.

L'accesso alla GUI di pfSense dal browser della Kali Linux, utilizzando l'indirizzo IP assegnato all'interfaccia LAN del firewall, ha rappresentato un primo test di raggiungibilità andato a buon fine.
Questo risultato ha confermato che la configurazione della rete interna kalinet, l'indirizzamento IP e il routing tra Kali Linux e pfSense erano corretti.

Il superamento di questa verifica preliminare ha consentito di procedere con i successivi test di connettività verso la macchina Metasploitable2, con la certezza che le configurazioni di base dell'ambiente di rete fossero funzionanti.



Dashboard della Pfsense



ping dalla Kali (192.168.50.151) verso la Pfsense (192.168.50.1)

3.2 Test di raggiungibilità tramite ICMP (ping)

Dalla macchina Kali Linux è stato eseguito un test di connettività verso la macchina Metasploitable2 utilizzando il comando **ping**, indirizzato all'IP assegnato alla Metasploitable2 (**192.168.51.100**) nella subnet collegata all'interfaccia OPT1 di

pfSense.

Il comando ha restituito risposte corrette, confermando che il traffico ICMP tra le due subnet veniva correttamente instradato da pfSense prima dell'applicazione della regola firewall.

```
┌──(kali㉿kali)-[~]
└─$ ping -c 4 192.168.51.100
PING 192.168.51.100 (192.168.51.100) 56(84) bytes of data.
64 bytes from 192.168.51.100: icmp_seq=1 ttl=63 time=1.14 ms
64 bytes from 192.168.51.100: icmp_seq=2 ttl=63 time=1.96 ms
64 bytes from 192.168.51.100: icmp_seq=3 ttl=63 time=0.861 ms
64 bytes from 192.168.51.100: icmp_seq=4 ttl=63 time=0.814 ms

── 192.168.51.100 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3014ms
rtt min/avg/max/mdev = 0.814/1.194/1.959/0.459 ms
```

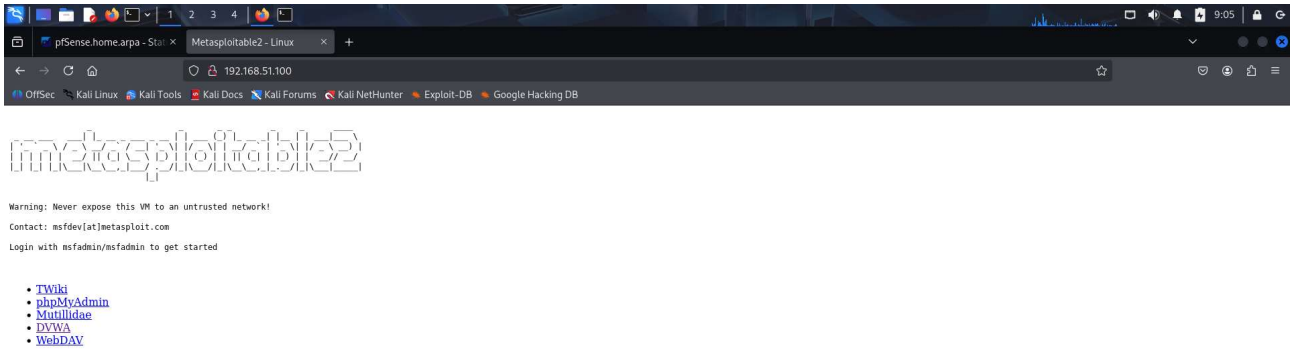
Ping dalla Kali verso Metasploitable2 prima della regola di firewall

3.3 Test di raggiungibilità del servizio web

Successivamente, dalla macchina Kali Linux è stato aperto il browser web per verificare l'accesso al **servizio HTTP** esposto dalla Metasploitable2.

Digitando l'indirizzo IP della macchina Metasploitable2 nel browser, è stato possibile visualizzare correttamente la pagina principale del sistema, che elenca i servizi vulnerabili disponibili, tra cui la DVWA (Damn Vulnerable Web Application).

Questo test conferma che, prima dell'applicazione della regola firewall, la comunicazione HTTP tra Kali Linux e Metasploitable2 è pienamente funzionante.



Homepage di Metasploitable2 prima della regola di firewall

4. APPLICAZIONE DELLA REGOLA FIREWALL E VERIFICA DEL BLOCCO

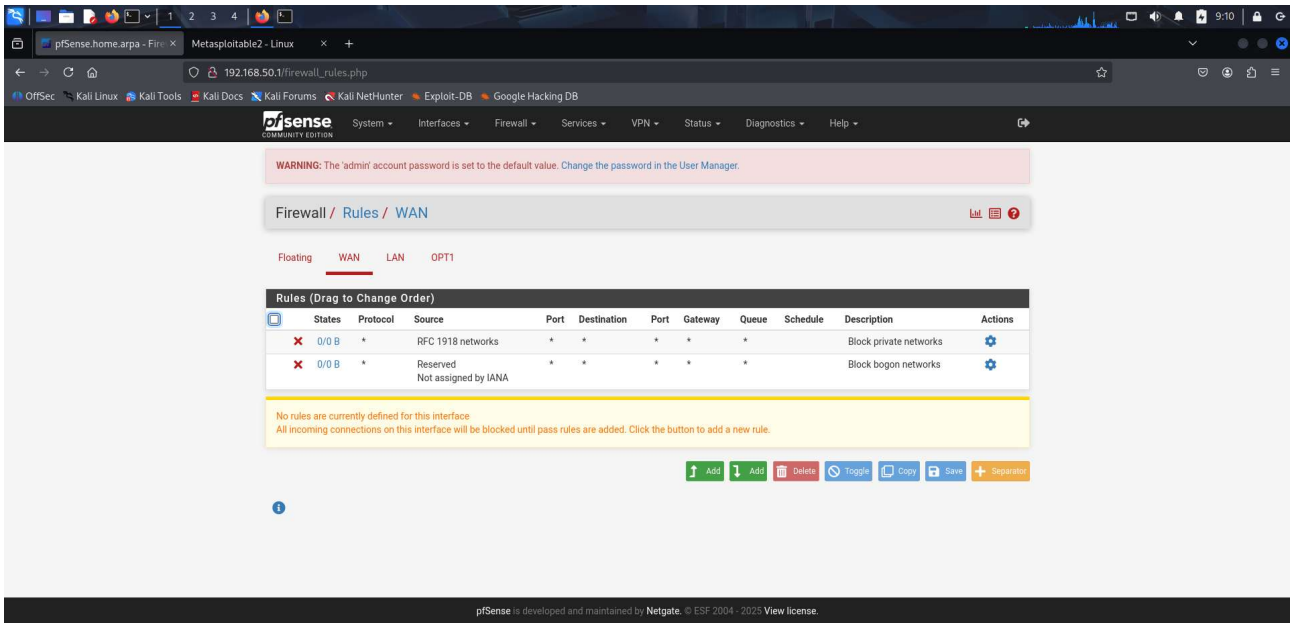
Una volta completata la configurazione dell'ambiente virtuale e verificata la piena raggiungibilità tra la macchina Kali Linux e la macchina Metasploitable2, si è proceduto all'implementazione della regola firewall richiesta dall'esercitazione.

L'obiettivo della regola era impedire l'accesso al servizio web esposto dalla Metasploitable2, mantenendo al contempo attiva la connettività di rete a livello ICMP, così da dimostrare un filtraggio selettivo del traffico basato sul servizio.

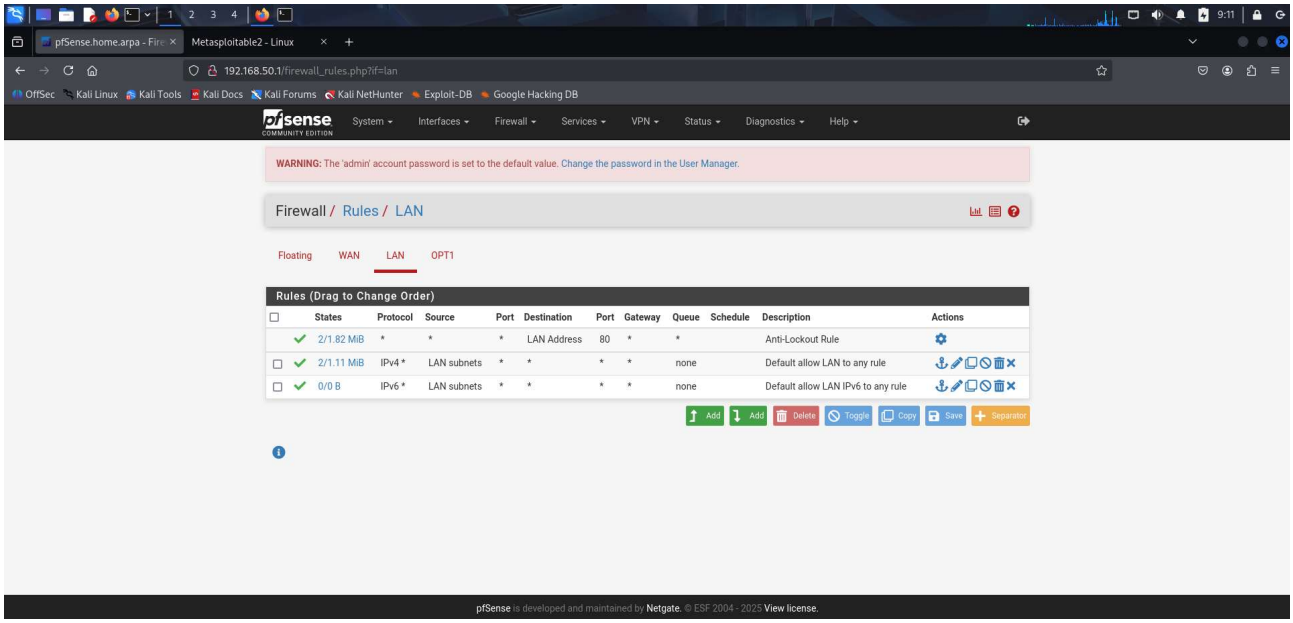
4.1 Stato delle regole firewall prima dell'applicazione della regola

Prima dell'introduzione della regola di blocco, l'interfaccia LAN di pfSense presentava esclusivamente le regole di default, tra cui la regola che consente il traffico IPv4 dalla LAN verso qualsiasi destinazione.
Questa configurazione permetteva alla macchina Kali Linux di raggiungere la Metasploitable2 sia tramite traffico ICMP sia tramite traffico HTTP.

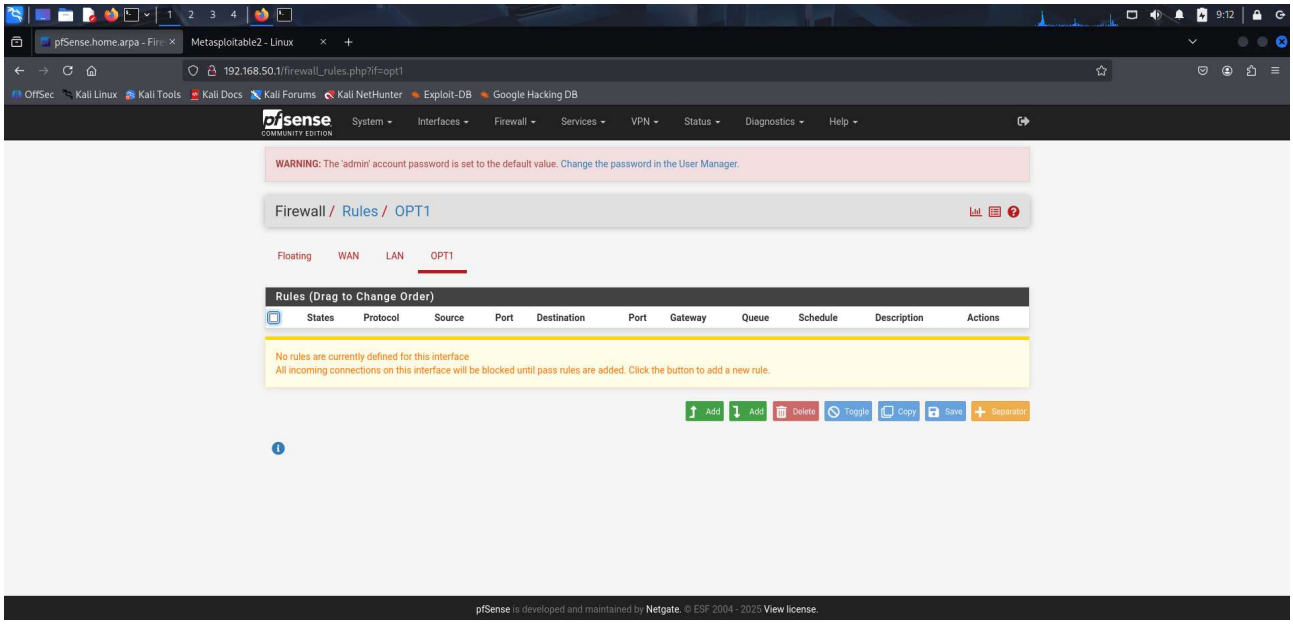
Le interfacce WAN e OPT1 risultavano configurate esclusivamente con le regole di default, senza restrizioni aggiuntive applicate manualmente.



Regole firewall sull'interfaccia WAN prima dell'applicazione della regola



Regole firewall sull'interfaccia LAN prima dell'applicazione della regola



Regole firewall sull'interfaccia OPT1 prima dell'applicazione della regola

4.2 Creazione della regola firewall sull'interfaccia LAN

La regola firewall è stata creata sull'interfaccia LAN di pfSense, in quanto pfSense applica le regole sul traffico in ingresso all'interfaccia stessa.
Essendo la macchina Kali Linux connessa alla LAN, la regola è stata correttamente

posizionata su tale interfaccia.

La regola è stata configurata con le seguenti caratteristiche:

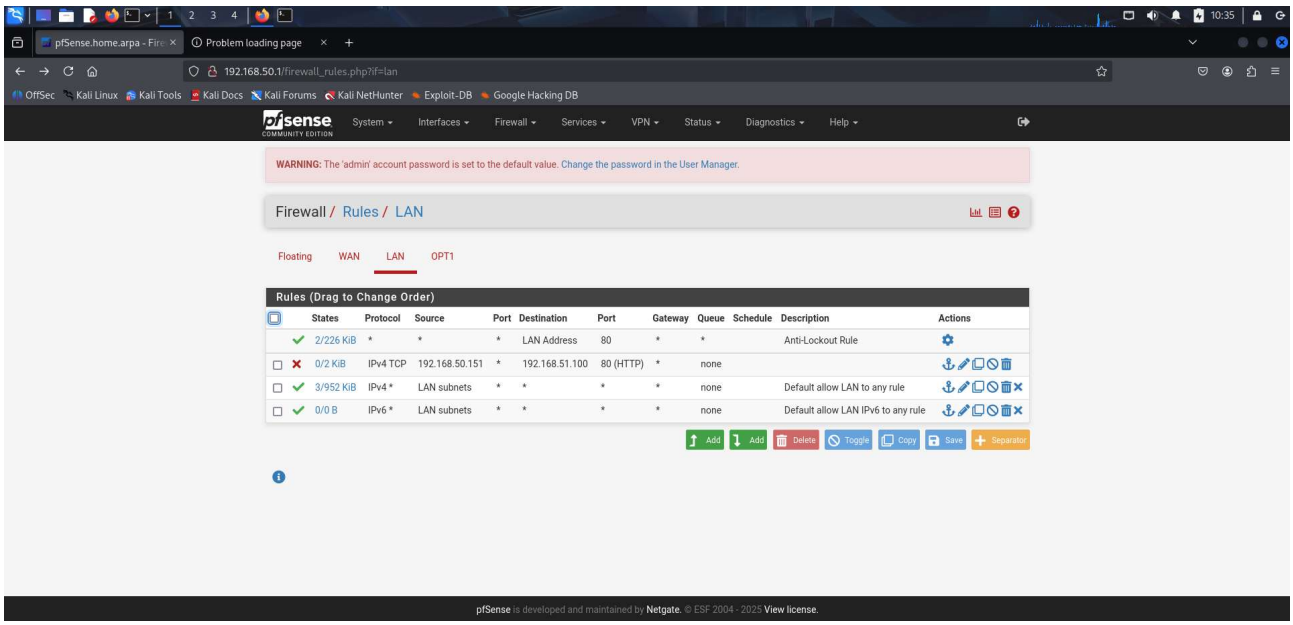
- **Action**: Block
- **Interface**: LAN
- **Address Family**: IPv4
- **Protocol**: TCP
- **Source**:
  - Address or Alias
  - 192.168.50.151 (IP address della Kali)
- **Destination**:
  - Address or Alias
  - 192.168.51.100 (IP address della Metasploitable2)
- **Destination port range**:
  - From: HTTP (80)
  - To: HTTP (80)

La regola è stata inserita in posizione prioritaria rispetto alla regola di default “allow LAN to any”, in modo da garantirne l’applicazione prima di qualsiasi permesso generale.

4.3 Stato delle regole firewall dopo l’applicazione della regola

Dopo l’applicazione della regola, l’interfaccia LAN di pfSense presenta una regola di blocco specifica per il traffico HTTP diretto verso la Metasploitable2, seguita dalle regole di default.

Le interfacce WAN e OPT1 non sono state modificate e continuano a utilizzare le regole di default, in quanto il filtraggio richiesto è limitato al traffico originato dalla LAN.



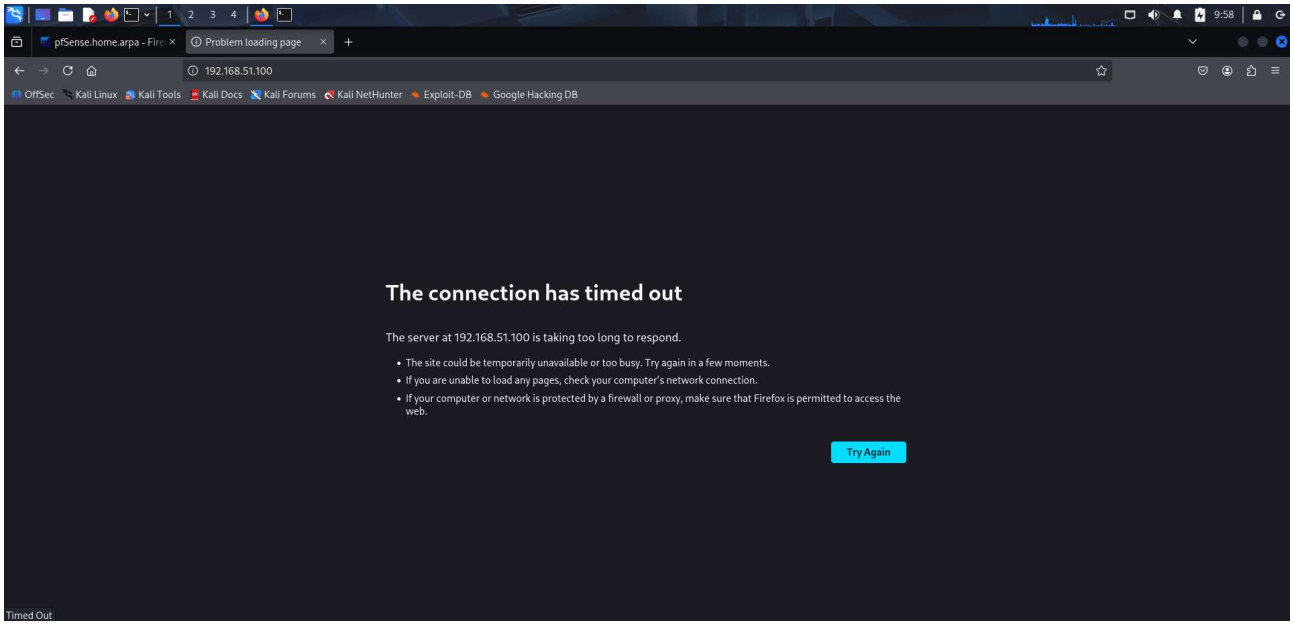
Regole di firewall LAN post applicazione blocco

4.4 Verifica del comportamento del servizio web (HTTP)

A seguito dell'applicazione della regola firewall, è stato effettuato un nuovo test di accesso al servizio web della Metasploitable2 dalla macchina Kali Linux.

Digitando l'indirizzo IP della Metasploitable2 nel browser della Kali, la pagina non risulta più raggiungibile, confermando che il traffico HTTP è correttamente bloccato dalla regola firewall configurata su pfSense.

Questo risultato dimostra l'efficacia della regola nel filtrare selettivamente il traffico applicativo.



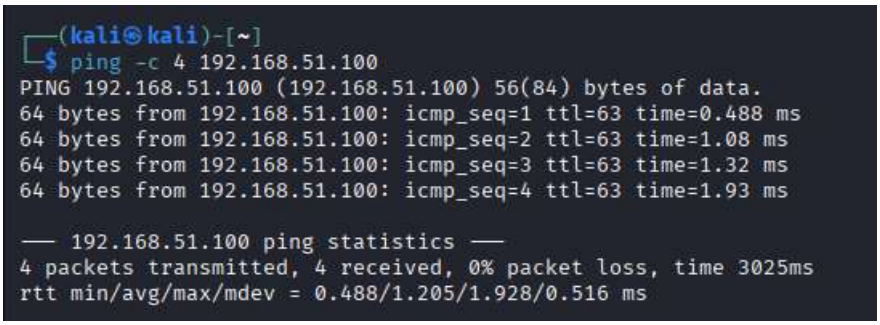
Homepage di Metasploiable2 post blocco

4.5 Verifica della connettività ICMP post-regola

Successivamente è stato verificato il comportamento del traffico ICMP tra Kali Linux e Metasploitable2.

Il test di ping continua a restituire risposte corrette, confermando che la regola firewall applicata non interferisce con il traffico ICMP e che il blocco è limitato esclusivamente al servizio HTTP.

Questo comportamento evidenzia come pfSense consenta un controllo granulare del traffico di rete, permettendo di bloccare specifici servizi senza compromettere la connettività generale tra le subnet.



ICMP della Kali verso Metasploitable2 dopo il blocco firewall

5. CONCLUSIONI

L'esercitazione ha permesso di configurare e testare un ambiente virtuale multi-subnet utilizzando pfSense come firewall e router centrale tra Kali Linux e Metasploitable2.

Attraverso la corretta configurazione delle reti in VirtualBox, delle interfacce di pfSense e dell'indirizzamento IP delle macchine virtuali, è stato possibile verificare inizialmente la piena raggiungibilità tra le subnet.
Successivamente, l'applicazione di una regola firewall mirata ha consentito di bloccare l'accesso al servizio web della Metasploitable2 dalla macchina Kali Linux, mantenendo attiva la connettività ICMP.

I test effettuati prima e dopo l'applicazione della regola dimostrano il corretto funzionamento del firewall pfSense nel filtraggio del traffico in base al servizio e alla subnet di origine, raggiungendo pienamente gli obiettivi richiesti dall'esercitazione.