Report Tecnico - Isolamento di Reti Virtuali con pfSense, Kali Linux se Metasploitable

Introduzione

In questo laboratorio abbiamo simulato una rete segmentata in tre zone distinte, gestite da **pfSense** come firewall centrale, utilizzando **Oracle VirtualBox**. Le macchine Kali Linux e Metasploitable sono state collegate rispettivamente alla rete **LAN** e **OPT1**.

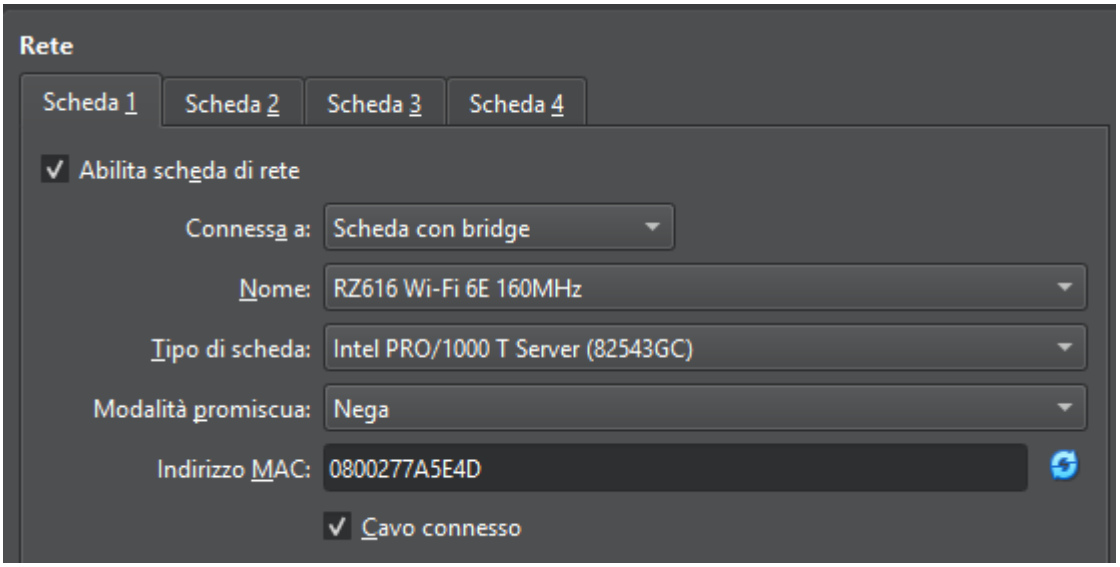
L'obiettivo è stato configurare correttamente le interfacce e gli indirizzi IP statici, testare la comunicazione tra le reti e infine applicare una **regola firewall** su pfSense per bloccare l'accesso a un servizio web, verificandone il funzionamento.

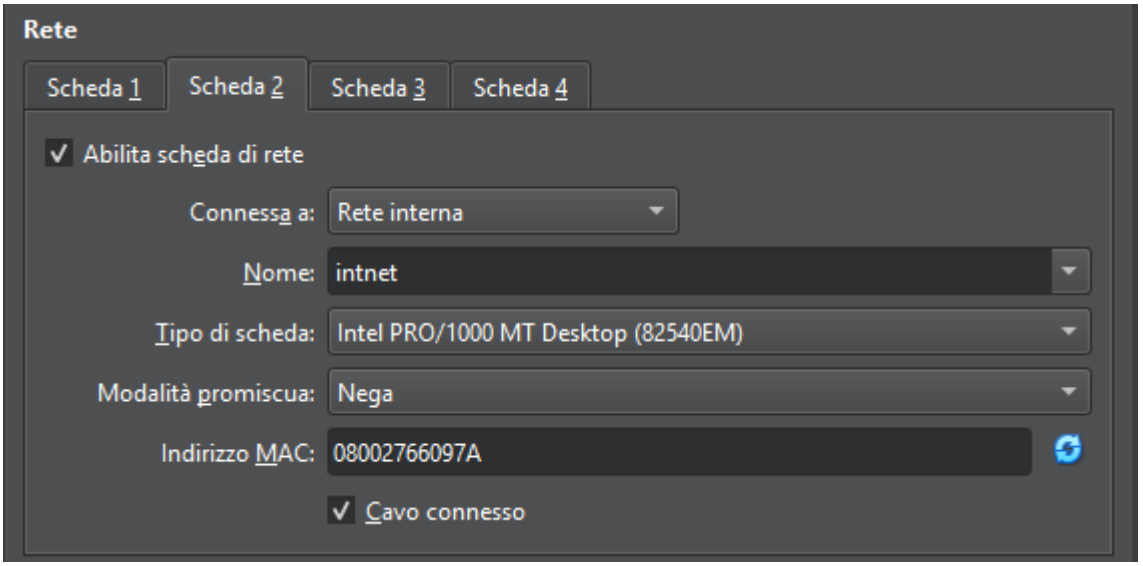
Configurazione delle Schede di Rete in Oracle VirtualBox

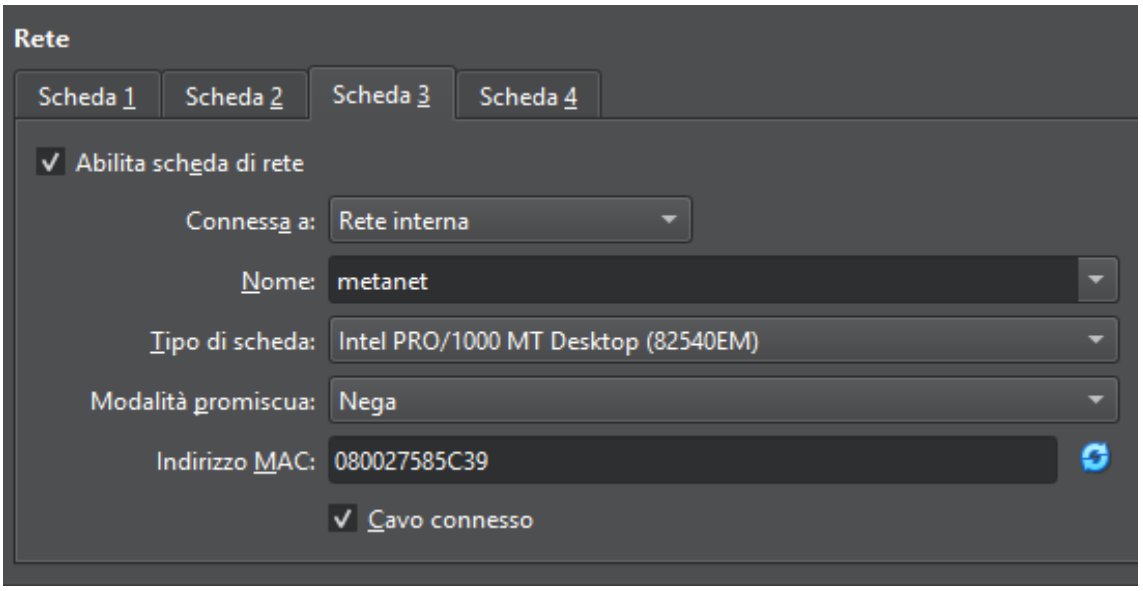
La macchina virtuale **pfSense** è stata configurata con **tre interfacce di rete**, ognuna collegata a un contesto diverso, per simulare una segmentazione realistica dell'infrastruttura:

- **Scheda 1** è impostata su **"Scheda con bridge"** per consentire a pfSense di collegarsi alla rete fisica dell'host, comportandosi come un vero e proprio gateway.
- **Scheda 2** è collegata a una **rete interna** chiamata `intnet`, che rappresenta la **LAN** e sarà utilizzata dalla macchina Kali Linux.
- **Scheda 3** è anch'essa configurata su **rete interna**, ma con nome `metanet`, pensata per ospitare la macchina Metasploitable all'interno di una rete separata (OPT1).

Questa struttura permette di isolare completamente le varie zone della rete: WAN (esterna), LAN (interna) e OPT1 (DMZ), lasciando a pfSense il compito di controllare il traffico tra di esse tramite firewall.







Configurazione degli indirizzi IP su pfSense

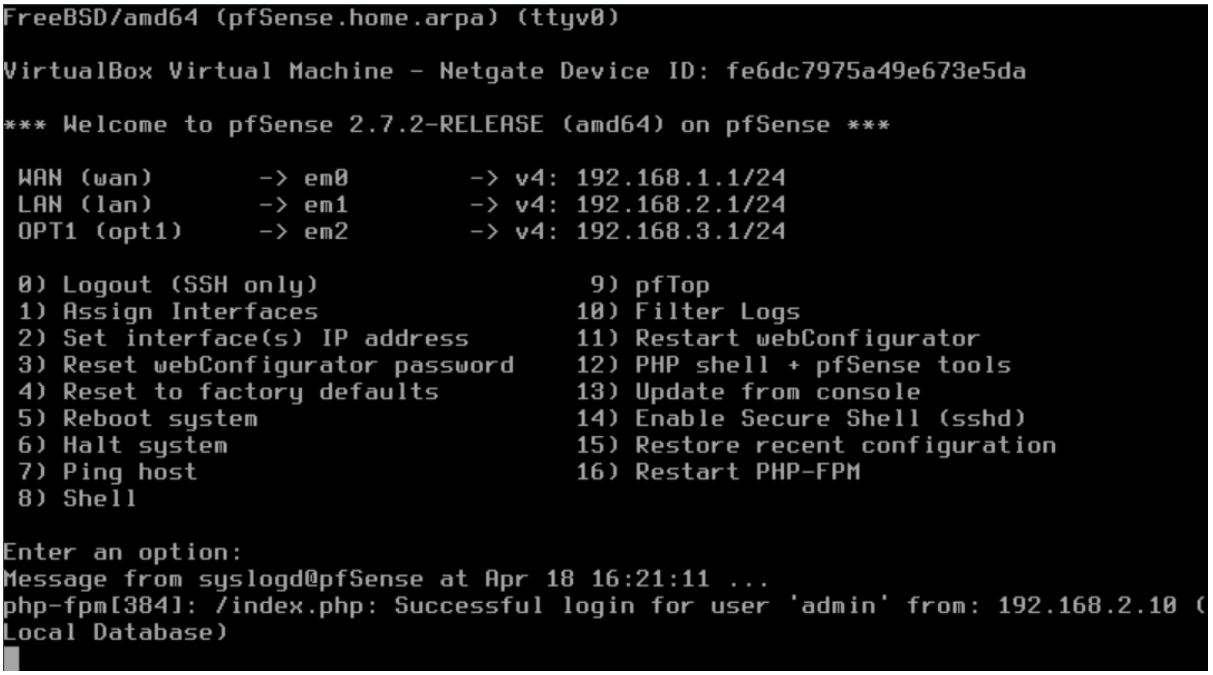
Dopo l'avvio e l'identificazione delle tre interfacce di rete da parte di pfSense (WAN, LAN e OPT1), si è proceduto con l'assegnazione **manuale** degli indirizzi IP. Tutte le interfacce sono state configurate con **indirizzi statici**, per garantire stabilità e controllo nella gestione del routing e delle regole firewall.

- **WAN** → `192.168.1.1/24`
- **LAN** → `192.168.2.1/24`

- **OPT1** → `192.168.3.1/24`

Questa configurazione consente a pfSense di operare come gateway e firewall tra tre reti distinte:

- La **rete WAN** rappresenta la connessione "esterna", simulata tramite l'interfaccia bridge.
- La **rete LAN** è utilizzata da **Kali Linux**, che simula un host interno.
- La **rete OPT1** è dedicata a **Metasploitable**, isolata in una subnet separata, come se fosse una DMZ.



Configurazione dell'IP su Kali Linux (rete LAN)

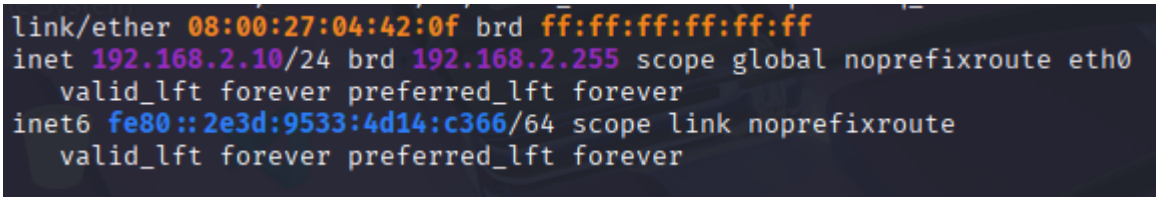
Una volta configurata l'interfaccia LAN su pfSense, abbiamo proceduto con l'assegnazione di un indirizzo IP **statico** alla macchina **Kali Linux**, che è collegata alla rete interna `intnet`, corrispondente proprio alla LAN.

L'indirizzo scelto è **192.168.2.10**, perfettamente compatibile con la subnet configurata su pfSense (`192.168.2.1/24`). In questo modo, Kali può comunicare correttamente con il gateway (pfSense) e con tutte le altre macchine presenti sulla stessa rete LAN.

La configurazione è la seguente:

- **Indirizzo IP:** `192.168.2.10`
- **Subnet mask:** `255.255.255.0` (/24)
- **Gateway:** `192.168.2.1`

Questa impostazione ci assicura che Kali Linux sia pienamente operativa nella rete LAN e pronta per testare la connettività verso l'esterno e verso le altre reti gestite da pfSense, come l'OPT1 dove risiede.



Configurazione dell'IP su Metasploitable (rete OPT1)

Dopo aver configurato correttamente l'interfaccia OPT1 su pfSense, abbiamo collegato la macchina **Metasploitable** alla rete interna `metanet`, che rappresenta la rete **OPT1**. Anche in questo caso, come per Kali, abbiamo deciso di impostare un **indirizzo IP statico**, così da avere pieno controllo sulla topologia della rete e assicurare coerenza con l'infrastruttura.

L'indirizzo assegnato a Metasploitable è **192.168.3.10**, perfettamente compatibile con la rete `192.168.3.0/24`, gestita da pfSense tramite il gateway **192.168.3.1**.

La configurazione finale è la seguente:

- **Indirizzo IP:** `192.168.3.10`
- **Subnet mask:** `255.255.255.0` (/24)
- **Gateway:** `192.168.3.1`

Questa configurazione permette a Metasploitable di comunicare con pfSense e con eventuali host presenti nella stessa rete OPT1, ma non direttamente con Kali, a meno che le regole del firewall lo consentano. Abbiamo quindi una **segmentazione efficace**, che simula perfettamente una DMZ o una rete vulnerabile isolata.

```
# This file describes the network interfaces available on your syste
# 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 192.168.3.10
netmask 255.255.255.0
network 192.168.3.0
broadcast 192.168.3.255
gateway 192.168.3.1
```

Accesso alla DVWA da Kali Linux

Con entrambe le macchine configurate, si può testare l'accesso alla DVWA (Damn Vulnerable Web Application) ospitata su Metasploitable:

1. Aprire un browser su Kali Linux.

2. Navigare all'indirizzo `http://192.168.2.10/dvwa`.

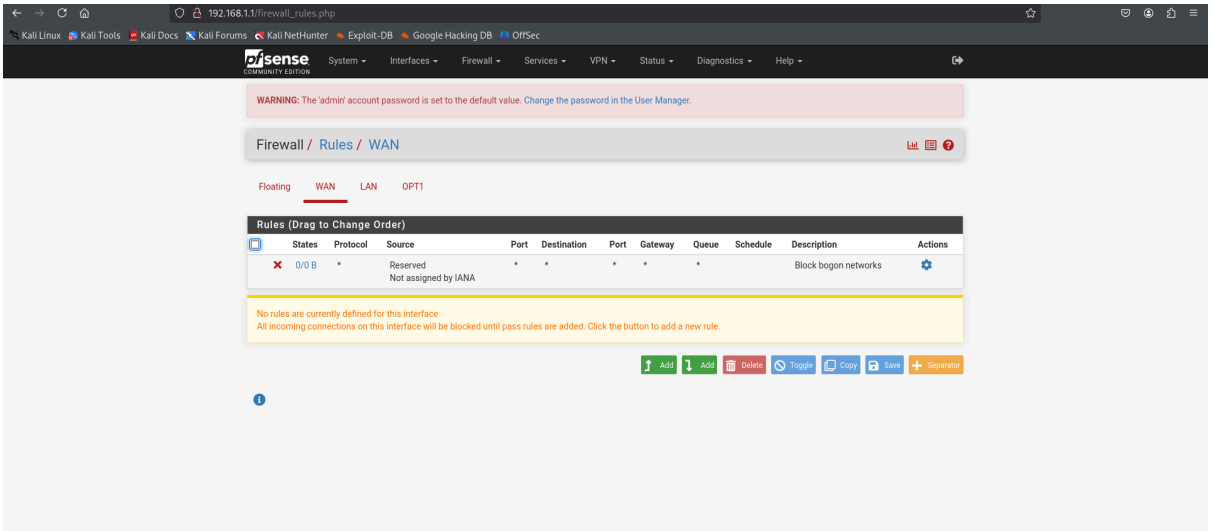
Se tutto è configurato correttamente, la pagina di login della DVWA dovrebbe essere accessibile.

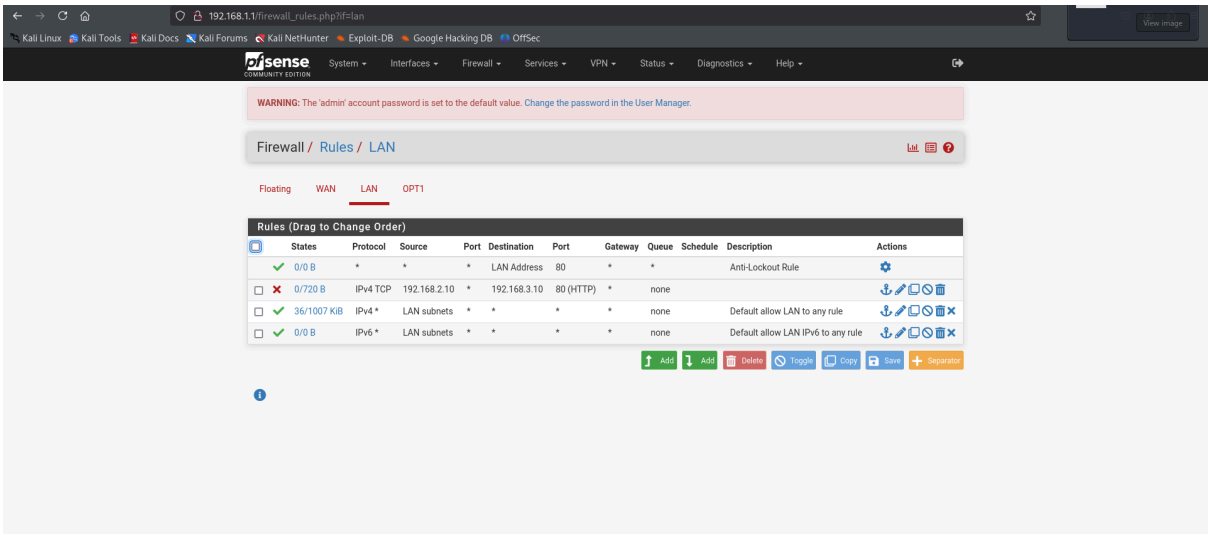
Creazione di una regola firewall per bloccare l’accesso da Kali a DVWA

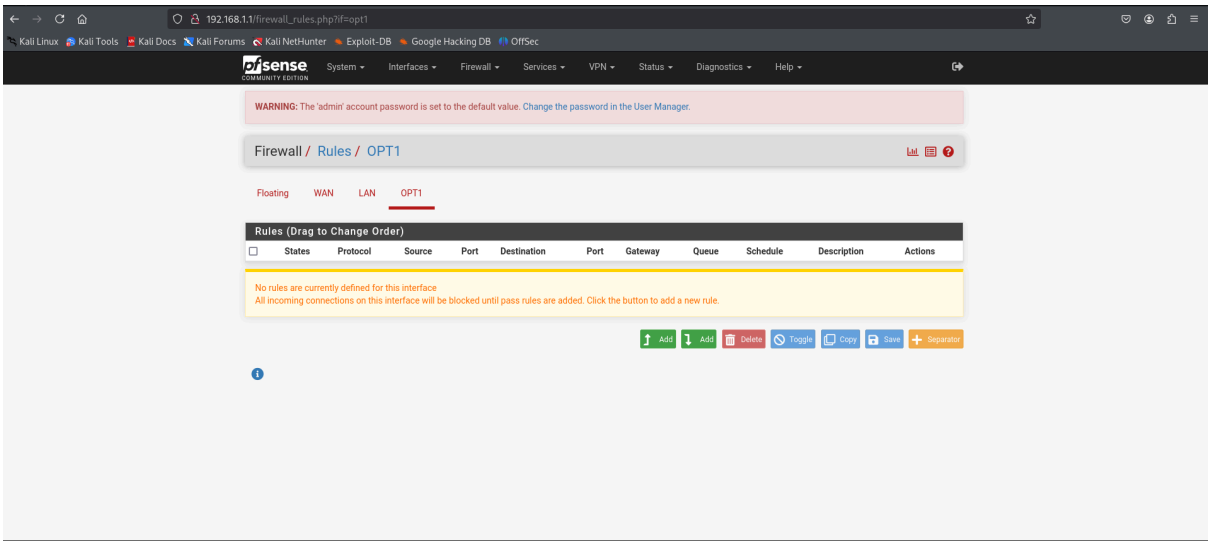
Per impedire l'accesso da Kali Linux alla DVWA su Metasploitable, si può creare una regola firewall su pfSense:

1. Accedere all'interfaccia web di pfSense.
2. Navigare su **Firewall > Rules > LAN**.
3. Aggiungere una nuova regola con i seguenti parametri:
    - **Action**: Block
    - **Interface**: LAN
    - **Protocol**: TCP
    - **Source**: 192.168.1.10
    - **Destination**: 192.168.2.10
    - **Destination Port Range**: 80 (HTTP)
4. Salvare la regola e applicare le modifiche.

Questa regola bloccherà le connessioni HTTP dalla macchina Kali Linux alla DVWA su Metasploitable.







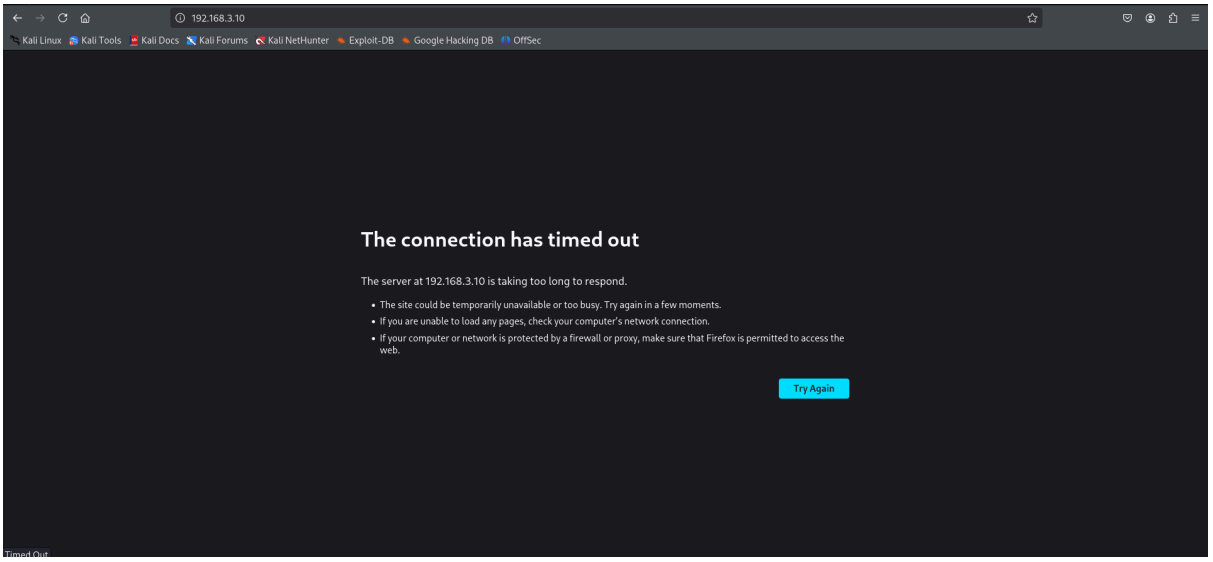
Verifica del blocco dell’accesso da Kali a DVWA

Per testare l'efficacia della regola firewall appena creata:

1. Su Kali Linux, aprire il browser.

2. Tentare di accedere nuovamente a `http://192.168.2.10/dvwa`.

Se la regola è attiva e correttamente configurata, l'accesso dovrebbe essere negato, indicando che il traffico HTTP da Kali a Metasploitable è stato bloccato con successo.



Questo conclude la configurazione e il test del laboratorio di segmentazione e controllo dell'accesso utilizzando pfSense, Kali Linux e Metasploitable su Oracle VirtualBox.