RELAZIONE TECNICA: Configurazione Firewall e Segmentazione di Rete con pfSense

Studente: Caccamo Rocco Paolo

Corso: Cyber Security & Ethical Hacking - Epicode **Data:** 12/12/2025

---

1. Obiettivo dell'Esercitazione

L'obiettivo di questa attività è stato configurare un firewall pfSense per gestire la segmentazione di rete tra una macchina attaccante (Kali Linux) e una macchina vulnerabile (Metasploitable 2). Nello specifico, è stato richiesto di:

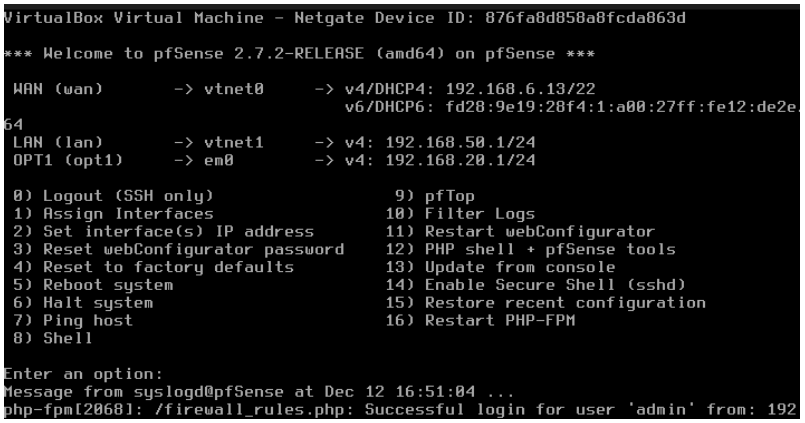
1. Isolare le due macchine su sottoreti diverse.
2. Configurare una regola firewall per bloccare il traffico HTTP (Porta 80) verso la macchina target.
3. Garantire che il traffico ICMP (Ping) rimanga consentito per la diagnostica.

2. Topologia di Rete

Utilizzando la console di pfSense, ho configurato le interfacce di rete assegnando indirizzi IP statici per fungere da gateway per le rispettive sottoreti.

La configurazione finale, verificata tramite console, è la seguente:

- **WAN (vtnet0):** Assegnata via DHCP (Rete esterna).
- **LAN (vtnet1):** Gateway **192.168.50.1/24** (Kali Linux).
- **OPT1 (em0):** Gateway **192.168.20.1/24** (Metasploitable).
- Come mostrato nello screenshot seguente, le interfacce sono attive e configurate correttamente.



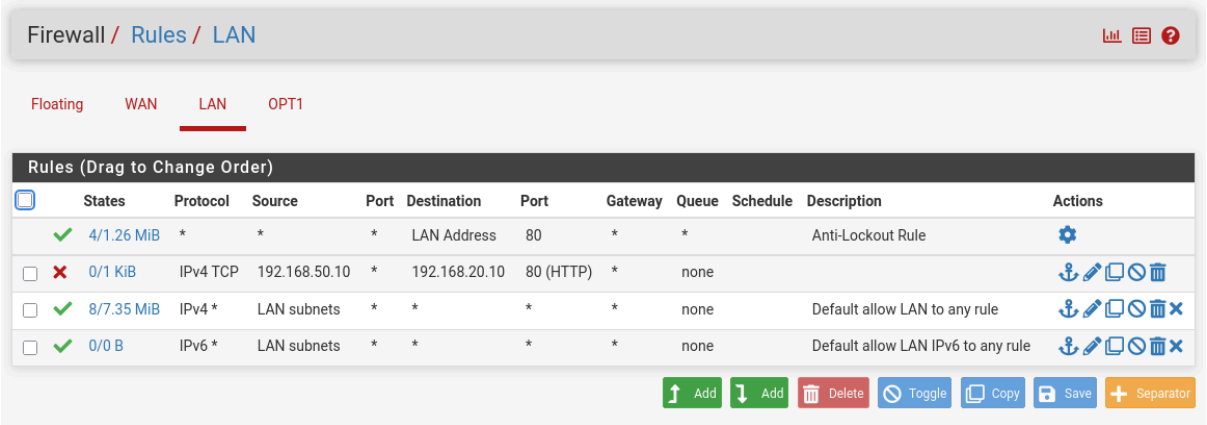
3. Configurazione della Policy di Sicurezza (Firewall Rules)

Per soddisfare i requisiti di sicurezza, ho creato una regola firewall specifica sull'interfaccia **LAN** (sorgente del traffico).

La regola è stata configurata per bloccare selettivamente il protocollo TCP destinato alla porta 80 della macchina Metasploitable.

- **Action:** Block
- **Interface:** LAN
- **Protocol:** IPv4 TCP
- **Source:** 192.168.50.10 (IP Kali)
- **Destination:** 192.168.20.10 (IP Metasploitable)
- **Destination Port:** 80 (HTTP)

La regola è stata posizionata in cima alla lista per garantirne la priorità rispetto alla regola predefinita "Default allow LAN to any".



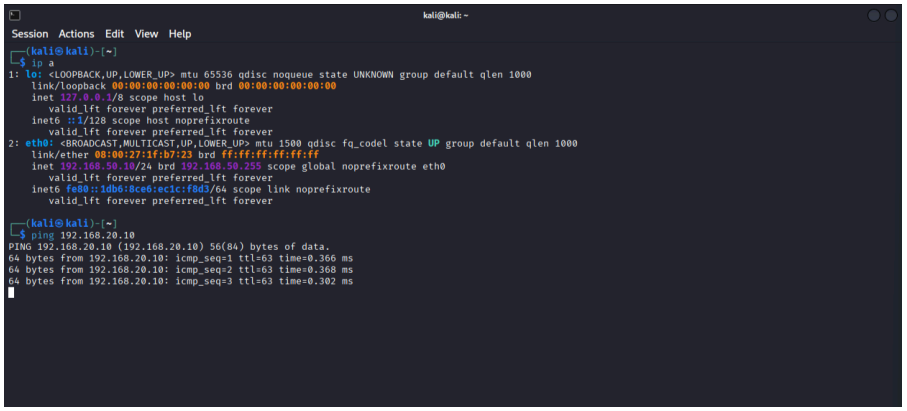
---

4. Test di Verifica

Al termine della configurazione, ho eseguito dei test di connettività dalla macchina Kali Linux verso la macchina Metasploitable per verificare l'efficacia delle regole.

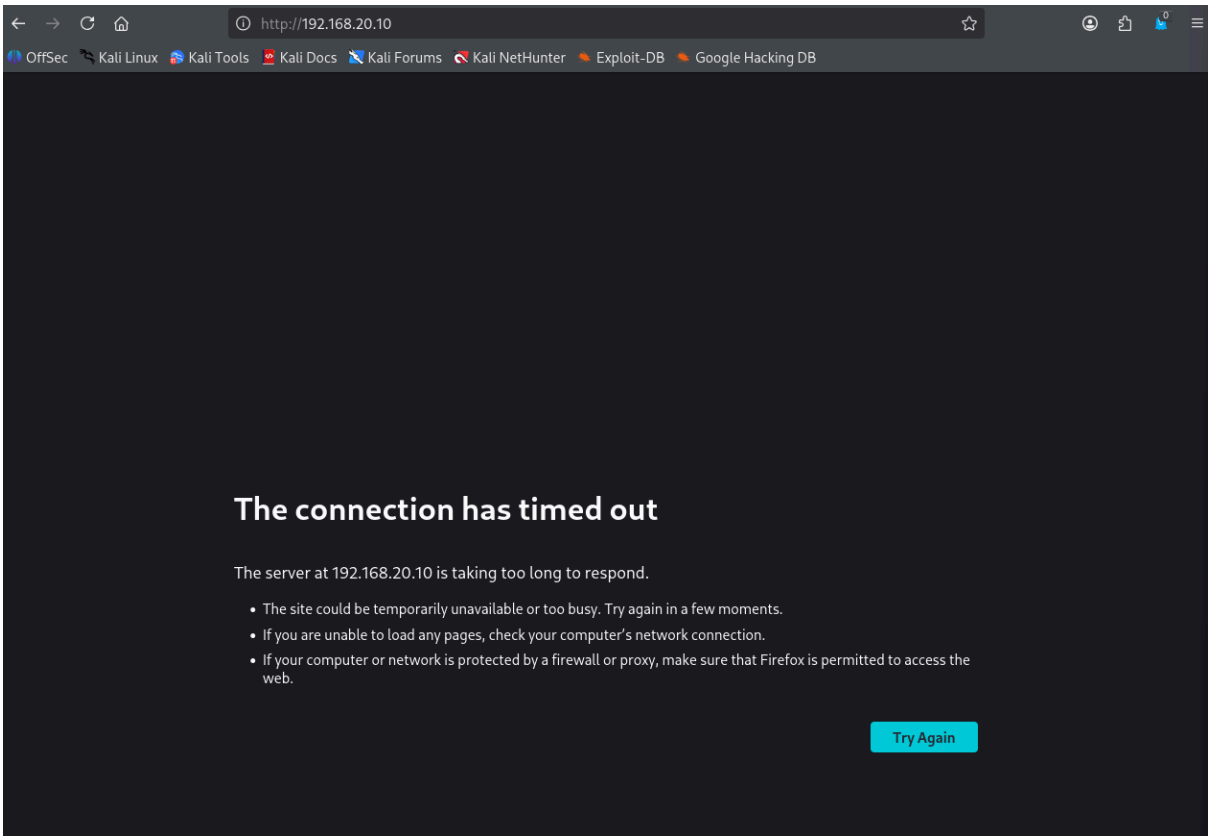
4.1 Test Connettività ICMP (Ping)

Ho eseguito un comando `ping` verso l'indirizzo 192.168.20.10. **Esito:** Positivo. Il firewall permette il passaggio dei pacchetti ICMP poiché la regola di blocco è specifica solo per il protocollo TCP. Ciò dimostra che il routing tra le due reti funziona correttamente.



4.2 Test Accesso Web (HTTP)

Ho tentato di accedere al servizio web DVWA tramite browser all'indirizzo `http://192.168.20.10`. **Esito:** Negativo (Timeout). Il browser non riesce a stabilire una connessione, andando in timeout. Questo conferma che il firewall sta scartando silenziosamente i pacchetti diretti alla porta 80, impedendo l'accesso al sito web vulnerabile.



---

5. Conclusioni

L'esercitazione è stata completata con successo. La separazione delle reti è stata implementata correttamente e le regole firewall

agiscono con la granularità richiesta, bloccando servizi specifici senza isolare completamente l'host a livello di rete.