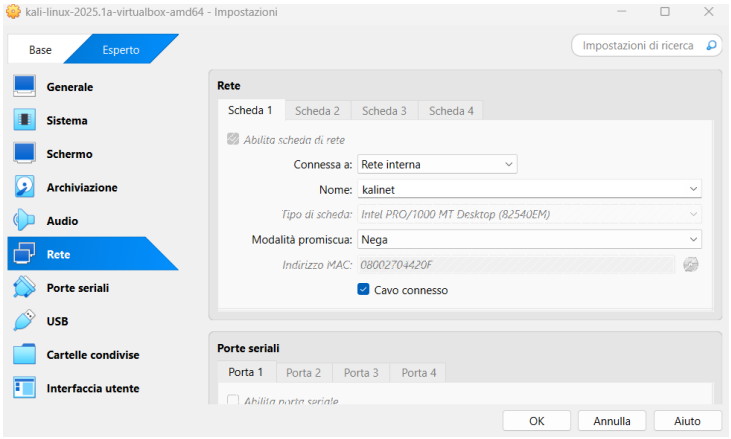
Report sulla Configurazione di un Ambiente di Test con pfSense come Switch Logico

Introduzione

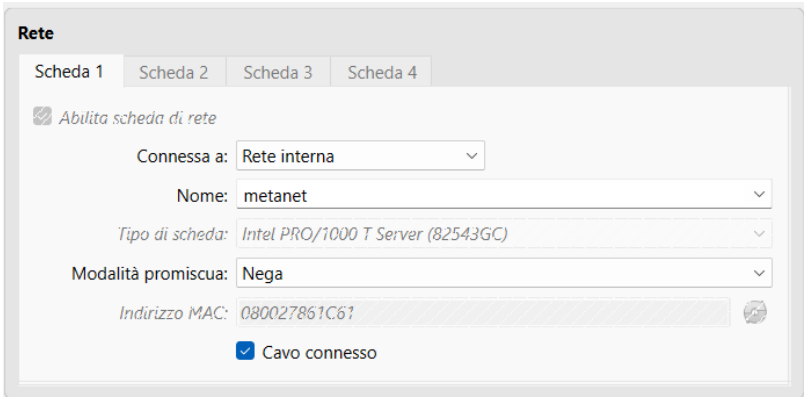
Il presente report descrive la configurazione di un ambiente di test di sicurezza informatica utilizzando VirtualBox e tre macchine virtuali: pfSense, Kali Linux e Metasploitable. L'obiettivo principale è configurare pfSense in modo da fungere da router/firewall interconnettendo due reti logiche distinte su cui risiedono Kali Linux e Metasploitable, e implementare una regola firewall per bloccare l'accesso a DVWA (Damn Vulnerable Web Application) ospitata su Metasploitable dalla macchina Kali Linux.

Architettura di Rete Virtuale



L'ambiente di test è stato realizzato utilizzando reti interne di VirtualBox per isolare le macchine virtuali e simulare scenari di rete reali. Sono state create le seguenti reti interne:

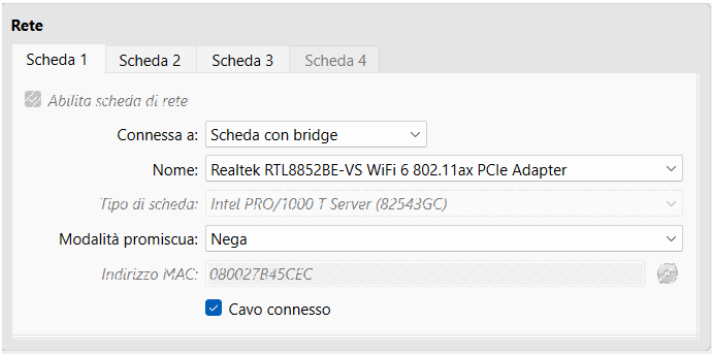
- **kalinet:** Rete interna dedicata alla macchina Kali Linux.
- **metanet:** Rete interna dedicata alla macchina Metasploitable.

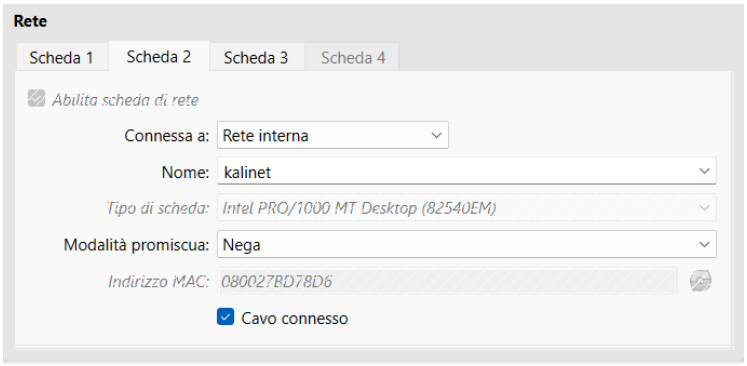


La macchina virtuale pfSense è stata configurata con tre interfacce di rete virtuali:

- **WAN (Scheda Bridge):** Connessa alla rete fisica dell'host per l'accesso iniziale all'interfaccia web di pfSense e per eventuali aggiornamenti.
- **LAN (Rete Interna: kalinet):** Interfaccia connessa alla rete interna su cui risiede Kali Linux.
- **OPT1 (Rete Interna: metanet):** Interfaccia connessa alla rete interna su cui risiede Metasploitable, per semplicità verrà mostrata solamente la scheda interna di kali.

In questa configurazione, pfSense agisce come un router che interconnette le due reti interne (kalinet e metanet), gestendo il traffico tra di esse e applicando le regole firewall definite. Dal punto di vista logico, pfSense svolge il ruolo di uno switch di livello 3 (router) che segmenta le due reti.

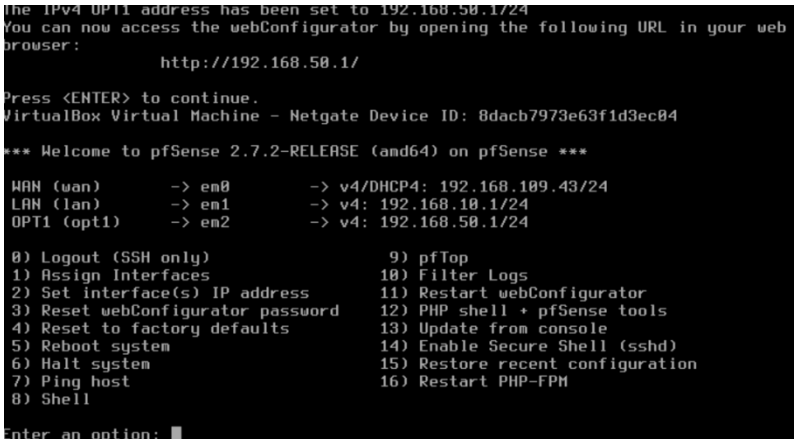




Configurazione degli Indirizzi IP Tramite pfSense

pfSense è stato configurato per gestire l'assegnazione degli indirizzi IP alle macchine virtuali Kali Linux e Metasploitable attraverso il servizio DHCP su ciascuna delle reti interne.

1. **Configurazione dell'Interfaccia per kalinet:**
    - L'interfaccia di pfSense connessa a kalinet (denominata "LAN" durante la configurazione iniziale o successivamente rinominata) è stata configurata con un indirizzo IP statico all'interno della sottorete desiderata 192.168.10.1/24.



Configurazione dell'Interfaccia per metanet:

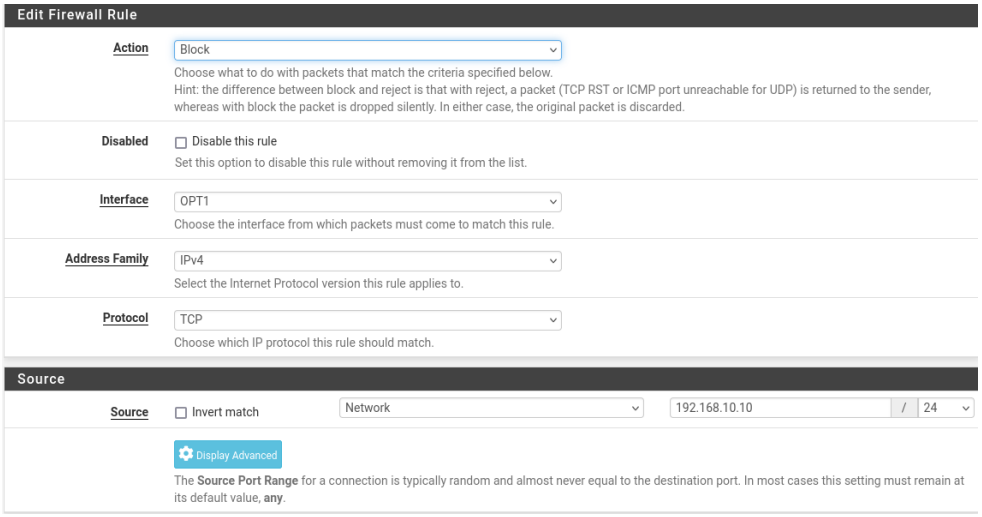
- La terza interfaccia di pfSense connessa a metanet (denominata "OPT1" o rinominata in modo appropriato, ad esempio "METANET_INT") è stata configurata con un indirizzo IP statico in una sottorete diversa 192.168.50.1/24.

Creazione della Regola Firewall per Bloccare l'Accesso a DVWA

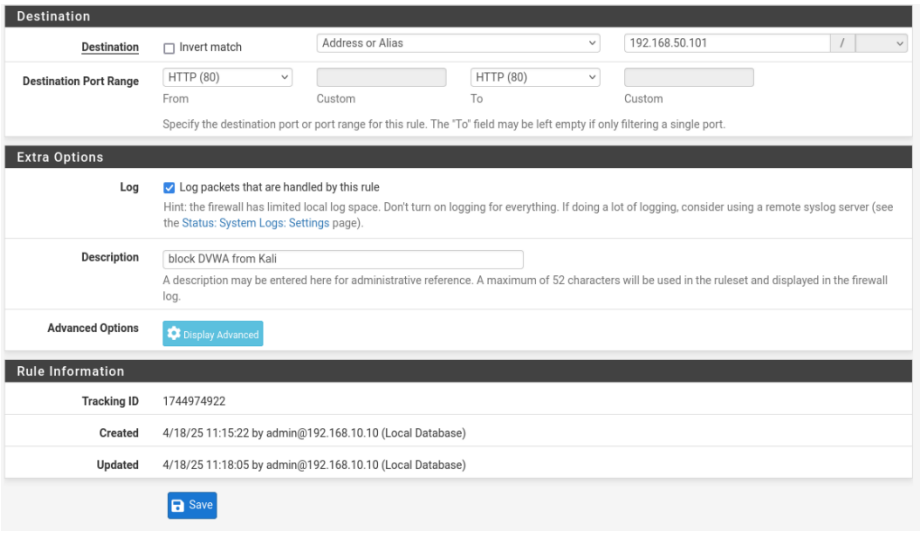
L'obiettivo è impedire alla macchina Kali Linux (IP: 192.168.10.10), situata sulla rete kalinet, di accedere all'applicazione DVWA ospitata su Metasploitable (IP: 192.168.50.101), situata sulla rete metanet. Per fare ciò, è stata creata una regola firewall su pfSense.

1. **Navigazione alla Sezione Firewall Rules:**
    - Nell'interfaccia web di pfSense, è stato navigato su "Firewall" -> "Rules".
    - È stata selezionata la scheda corrispondente all'interfaccia da cui proviene il traffico che si desidera bloccare, ovvero l'interfaccia connessa alla rete di Kali Linux ("LAN").

2. **Creazione della Regola di Blocco:**
    - È stata aggiunta una nuova regola con le seguenti specifiche:
        - **Action:** Block (Blocca il traffico corrispondente alla regola).
        - **Interface:** LAN (Applica la regola al traffico in entrata sull'interfaccia LAN di pfSense, ovvero il traffico proveniente dalla rete kalinet).
        - **Protocol:** TCP (DVWA comunica tipicamente tramite il protocollo TCP sulla porta 80 (HTTP) o 443 (HTTPS)).
        - **Source:**
            - **Type:** Single host or alias
            - **Address:** Indirizzo IP della macchina Kali Linux (192.168.10.10).



        - **Destination:**
            - **Type:** Single host or alias
            - **Address:** Indirizzo IP della macchina Metasploitable (192.168.50.101).
            - **Port:** web (Alias predefinito che include le porte 80 e 443). In alternativa, si sarebbe potuta specificare la porta 80.
        - **Description:** Blocca accesso DVWA da Kali a Metasploitable (o una descrizione simile).



- **Log:** (Opzionale) Abilitato per registrare i pacchetti bloccati da questa regola per scopi di verifica.

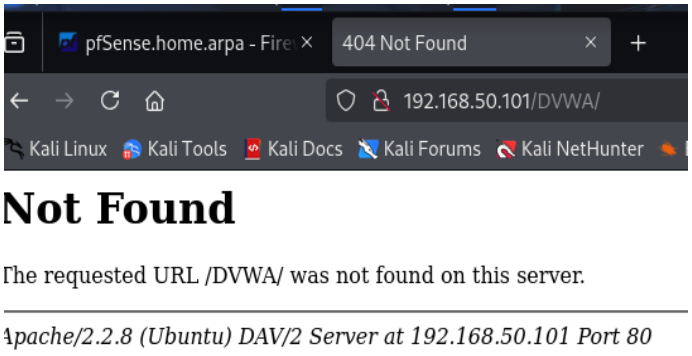
3. **Applicazione delle Modifiche:**

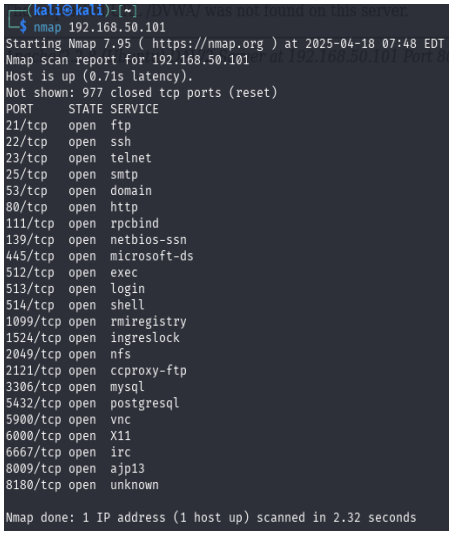
   - Dopo aver configurato la regola, è stato fondamentale fare clic sul pulsante "Save" e successivamente su "Apply Changes" per rendere effettiva la regola sul firewall di pfSense.

Verifica della Regola Firewall

Per verificare l'efficacia della regola firewall, sono stati eseguiti i seguenti test dalla macchina Kali Linux (IP: 192.168.10.10):

1. **Tentativo di Accesso Web a DVWA:**
   - È stato aperto un browser web su Kali Linux e si è tentato di accedere all'indirizzo IP di Metasploitable seguito dal percorso di DVWA (http://192.168.50.101/dvwa/). Il tentativo di connessione è fallito, indicando che il firewall di pfSense ha bloccato la richiesta.





2. **Scansione delle Porte con Nmap:**

   - È stato utilizzato lo strumento nmap da Kali Linux per scansionare le porte TCP della macchina Metasploitable, in particolare la porta 80. Il risultato della scansione ha mostrato che la porta 80 era "closed", indicando che il firewall stava bloccando le connessioni a quella porta.

Conclusioni

La configurazione descritta ha permesso di isolare le macchine Kali Linux e Metasploitable su due reti logiche distinte (kalinet e metanet), interconnesse e protette dal firewall pfSense. La regola firewall implementata sull'interfaccia LAN di pfSense ha bloccato con successo il traffico proveniente da Kali Linux (IP: 192.168.10.10) e diretto verso l'applicazione DVWA ospitata su Metasploitable (IP: 192.168.50.101) sulla porta web, dimostrando la capacità di pfSense di segmentare la rete e applicare politiche di sicurezza specifiche basate sugli indirizzi IP delle macchine.