Relazione progetto individuale U1-S3-L5

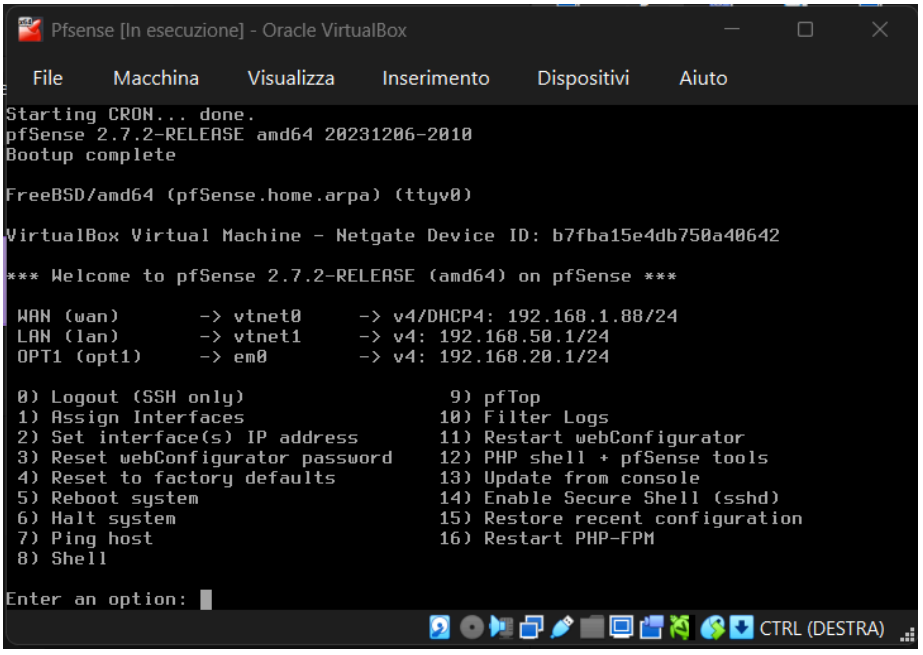
Configurazione del Firewall pfSense

Questo esercizio ha avuto come obiettivo la creazione e l'applicazione di una regola firewall su pfSense per bloccare l'accesso al servizio **DVWA** (su Metasploitable) dalla macchina **Kali Linux**. Un requisito fondamentale dell'esercizio è che le macchine Kali e Metasploitable fossero su reti diverse, gestite da interfacce separate del firewall pfSense.

1. Configurazione Dettagliata delle Interfacce di pfSense

Per soddisfare il requisito di reti separate, sono state aggiunte due nuove interfacce di rete (LAN, OPT1) oltre all'interfaccia WAN già presente e la configurazione degli indirizzi IP è stata eseguita da terminale di pfSense.

Di seguito il dettaglio della configurazione applicata:



Le due macchine connesse alle interfacce sono state settate in DHCP di modo che venisse loro assegnato in automatico un indirizzo IP

Kali Linux è stata collegata all'interfaccia **LAN** e ha ricevuto l'indirizzo IP 192.168.50.151 con subnet mask /24.

Metasploitable è stata collegata all'altra interfaccia **OPT1** e ha ricevuto l'indirizzo IP 192.168.20.11 con subnet mask /24.

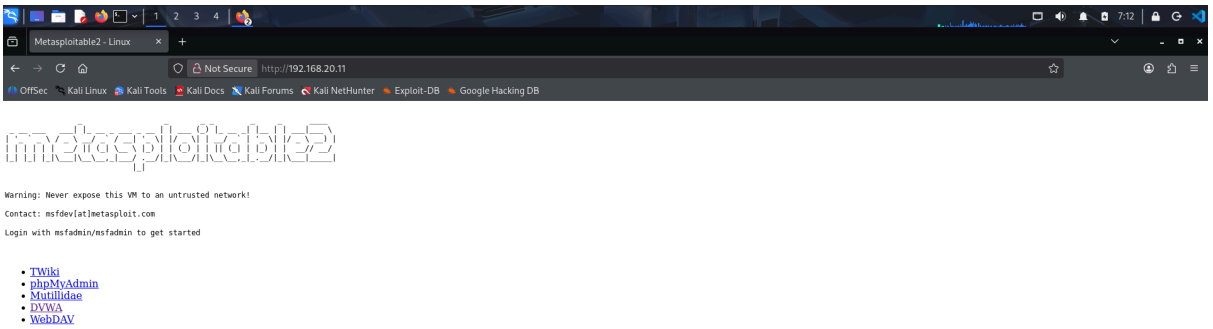
2. Test di Accessibilità Pre-Regola

Prima di implementare la regola di blocco, sono stati eseguiti dei test dalla macchina Kali Linux per confermare la connettività e l'accessibilità al servizio web sulla macchina Metasploitable (IP 192.168.20.11).

A. Accesso al Server Web

È stato tentato l'accesso all'indirizzo IP di Metasploitable dalla macchina Kali Linux.

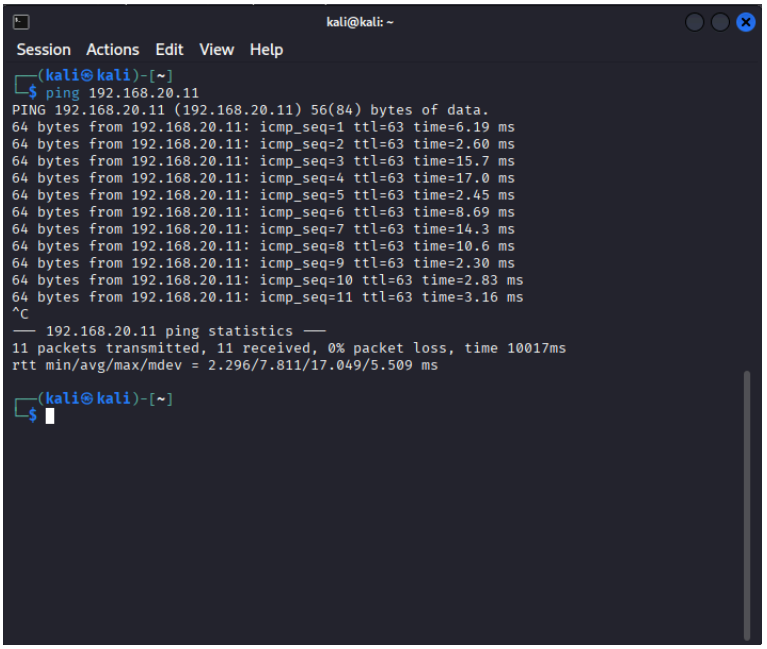
- **Risultato:** L'accesso alla pagina web all'indirizzo *http://192.168.20.11* ha avuto successo, mostrando la pagina di benvenuto di Metasploitable .



B. Test di Connettività (Ping)

È stato eseguito un comando `ping` dalla macchina Kali Linux verso l'IP di Metasploitable per verificare la connettività ICMP.

- **Comando:** `ping 192.168.20.11`.
- **Risultato:** Il ping ha avuto successo, con 11 pacchetti trasmessi e 11 ricevuti .



3. Applicazione della Regola Firewall (LAN Interface)

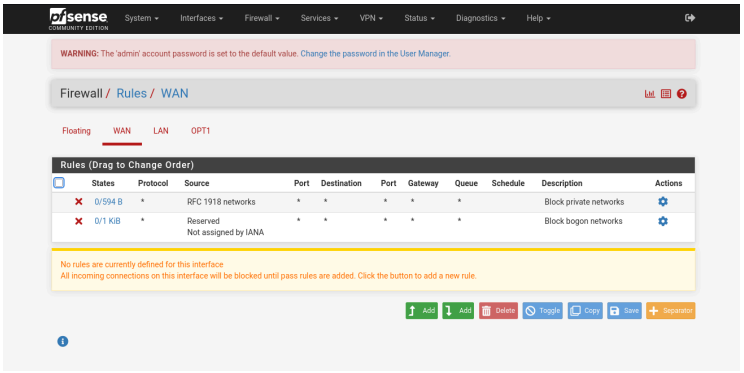
L'obiettivo era bloccare l'accesso al servizio web (porta 80) di Metasploitable (192.168.20.11) dalla macchina Kali (192.168.50.151). Poiché il traffico ha origine dalla rete **LAN** (Kali), la regola è stata applicata sull'interfaccia **LAN** del firewall.

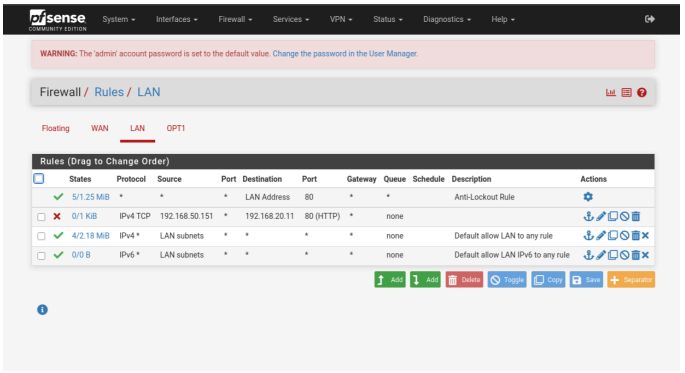
La regola creata è la seguente :

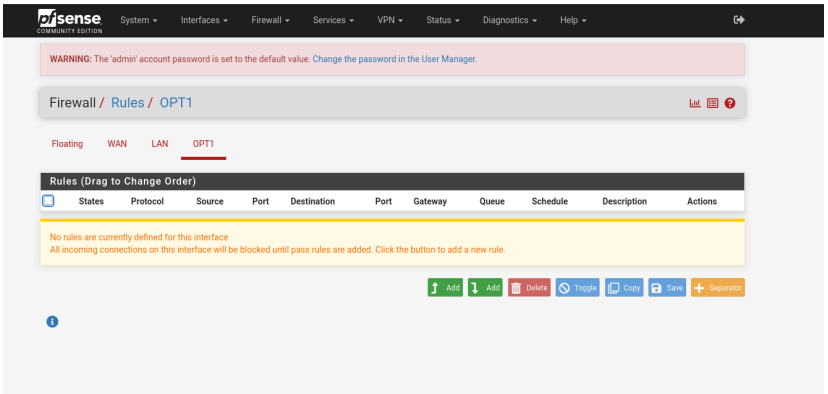
Azione	Protocollo	Sorgente	Porta Sorgente	Destinazione	Porta Destinazione	Descrizione
Blocca	IPv4 TCP	192.168.50.151 (Kali IP)	*	192.168.20.11 (Meta IP)	**80 (HTTP)**	Blocco mirato del traffico

- **Azione (Action): Blocca (Block)**.
- **Interfaccia (Interface): LAN**.
- **Protocollo (Protocol): IPv4 TCP**.
- **Sorgente (Source):** È stato specificato l'indirizzo IP esatto della macchina Kali Linux: **192.168.50.151**.
- **Destinazione (Destination):** È stato specificato l'indirizzo IP di Metasploitable: **192.168.20.11**.
- **Porta Destinazione (Destination Port Range): 80 (HTTP)**, la porta del servizio web DVWA.

Questa regola è stata posizionata in modo da precedere la regola di default **Default allow LAN to any rule** per assicurarne l'efficacia.







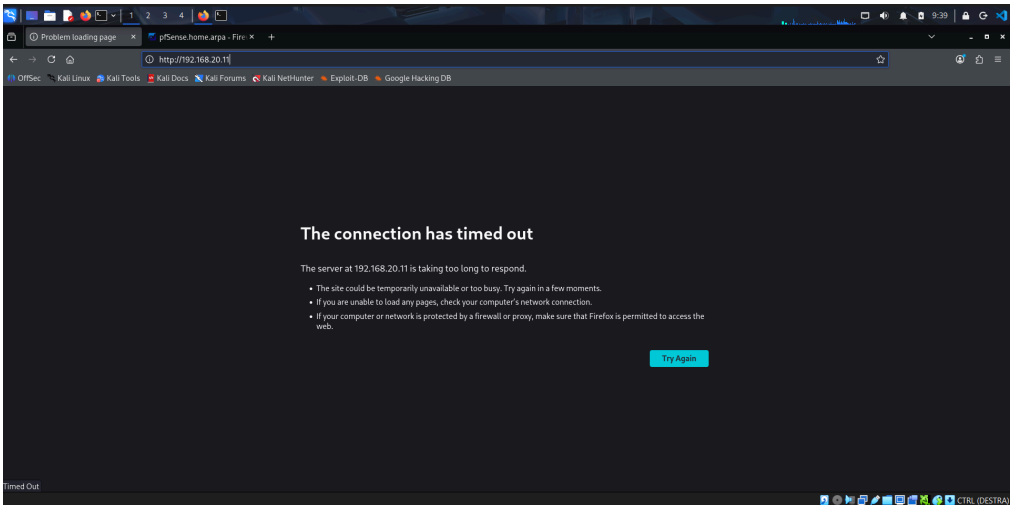
4. Test Post-Regola (Verifica del Blocco)

Dopo aver applicato e salvato la regola sul firewall, sono stati eseguiti nuovamente i test per confermare che l'accesso fosse bloccato, ma la connettività di base fosse mantenuta.

A. Accesso al Server Web (DVWA)

È stato ritentato l'accesso alla pagina web DVWA (porta 80) dalla macchina Kali.

- **Risultato:** L'accesso al sito *http://192.168.20.11* è fallito. Il browser ha restituito un errore di **"The connection has timed out"** (Timeout della connessione) . Ciò conferma che il traffico TCP verso la porta 80 è stato interrotto dalla regola.



B. Test di Connettività (Ping)

È stato eseguito nuovamente il comando `ping` dalla macchina Kali Linux verso l'IP di Metasploitable.

- **Risultato:** Il ping ha continuato a funzionare normalmente. Questo conferma che il blocco è stato applicato in modo preciso solo al protocollo **TCP** (porta 80), lasciando inalterato il protocollo **ICMP** (Ping).