Relazione di Laboratorio: Implementazione Policy Firewall & Segmentazione di Rete

1. Sommario Esecutivo

L'obiettivo di questa esercitazione di laboratorio era implementare la segmentazione della rete e configurare una policy firewall per impedire a una specifica macchina non autorizzata (Kali Linux) di scansionare un bersaglio vulnerabile (Metasploitable/DVWA). L'obiettivo è stato raggiunto con successo isolando le macchine su sottoreti separate e creando una regola di blocco sull'interfaccia LAN.

---

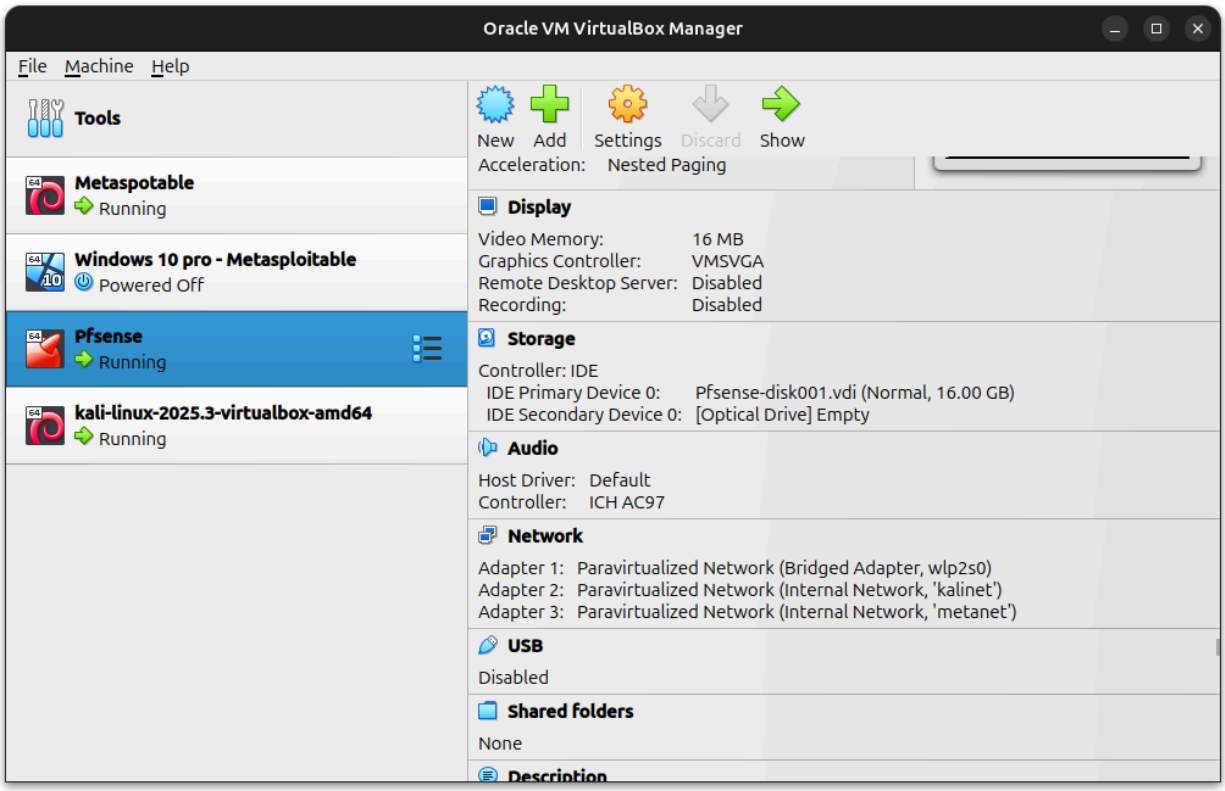
2. Topologia di Rete & Segmentazione

Per soddisfare il requisito dell'assegnazione riguardante la segmentazione della rete, l'ambiente è stato configurato con tre interfacce di rete distinte. Ciò garantisce che l'attaccante (Kali) e la vittima (Metasploitable) risiedano su domini di broadcast differenti, costringendo il traffico a passare attraverso il firewall Pfsense per l'ispezione.

Configurazione della Virtualizzazione:
La VM Pfsense è stata configurata con tre adattatori di rete in VirtualBox per supportare questa topologia:

- **Adattatore 1:** Scheda con Bridge (Connettività WAN).
- **Adattatore 2:** Rete Interna kalinet (LAN).
- **Adattatore 3:** Rete Interna metanet (OPT1/Rete Bersaglio).

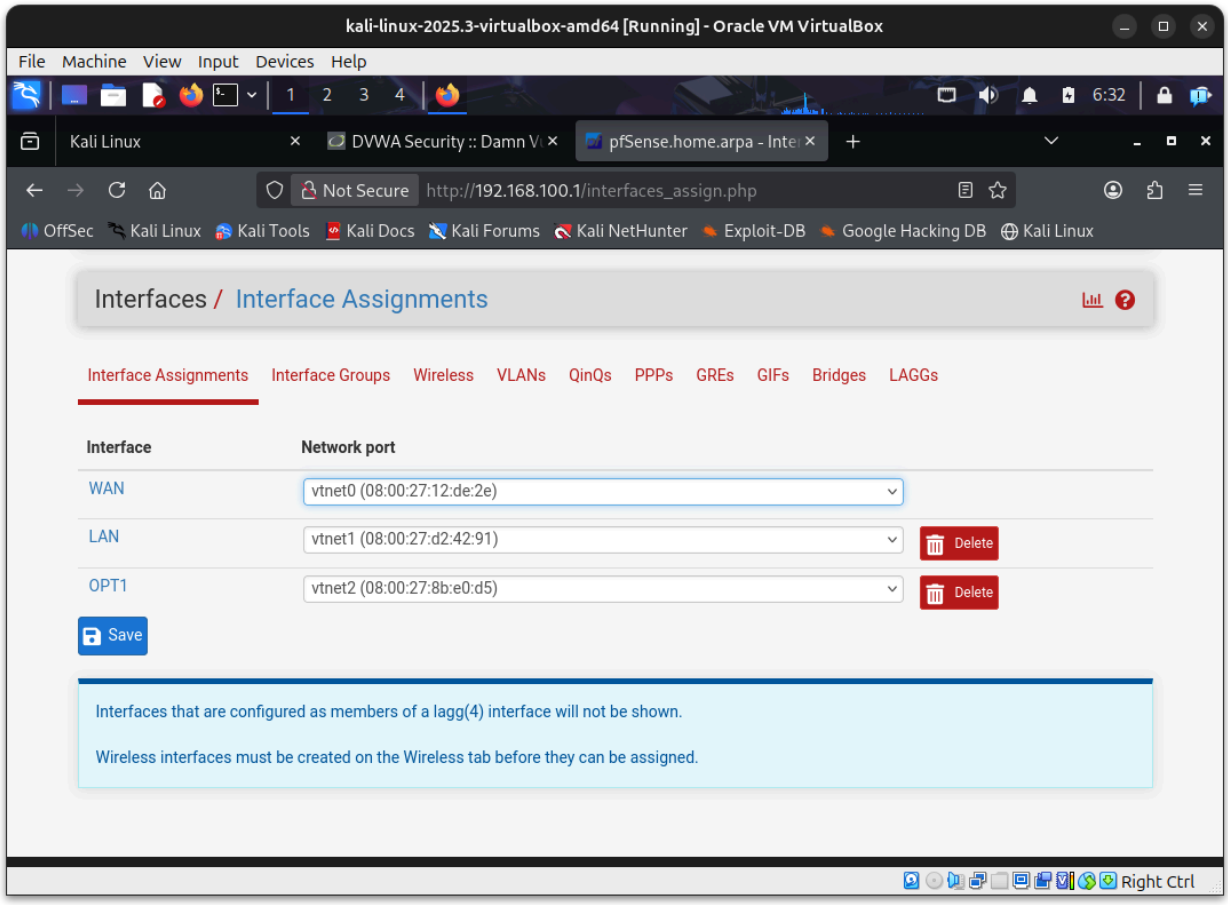
Le VM di Kali e Metasploitable sono state invece configurate con un adattatore per VM rispettivamente IN kalinet (LAN) e IN metanet (OPT1).



Evidenza Figura 1: Questo screenshot prova che la configurazione di virtualizzazione rispetta il requisito di "aggiungere una nuova interfaccia" per gestire le reti separate.

Assegnazione delle Interfacce:
All'interno dell'interfaccia Web (GUI) di Pfsense, la nuova porta di rete (vtnet2) è stata riconosciuta e assegnata con successo a una nuova interfaccia denominata OPT1.

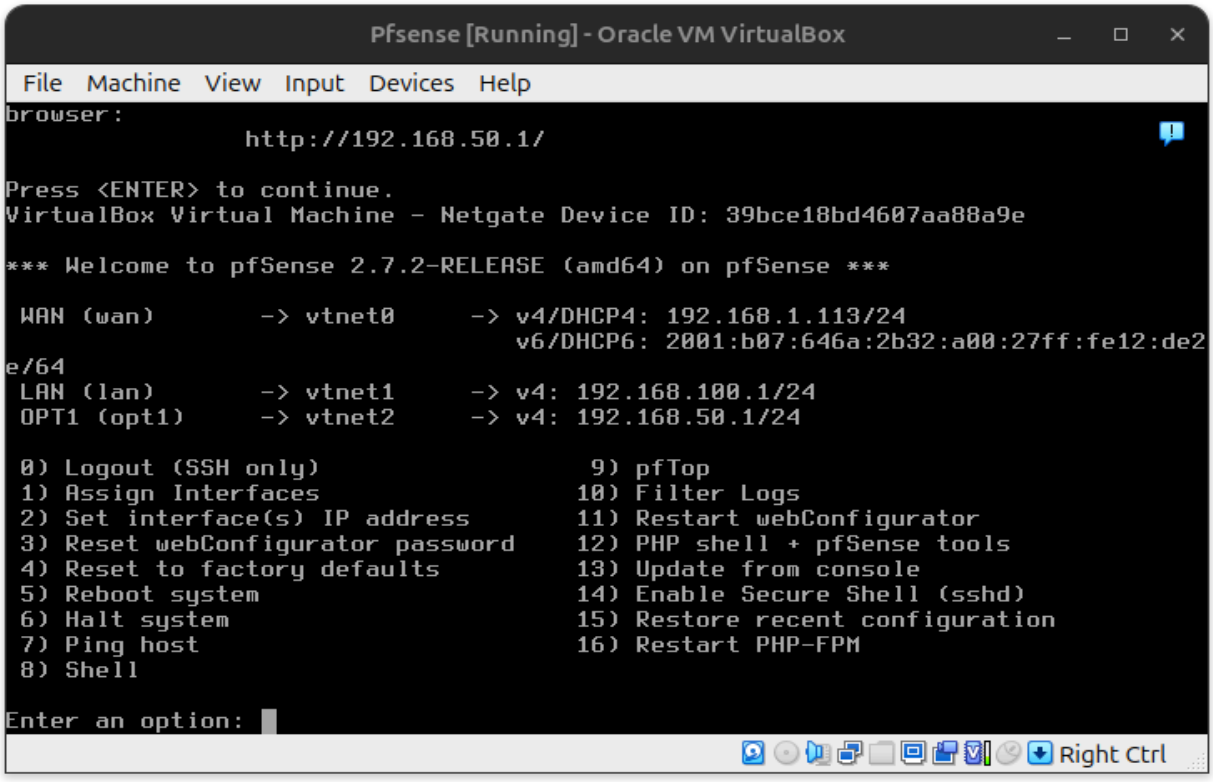
- **WAN (vtnet0):** Connessione a monte/Internet.
- **LAN (vtnet1):** La rete "Attaccante".
- **OPT1 (vtnet2):** La rete "Vittima".



Evidenza Figura 2: Questo conferma che il nuovo adattatore virtuale (vtnet2) è stato correttamente assegnato dal sistema operativo Pfsense.

Schema di Indirizzamento IP:
Le interfacce sono state configurate con i seguenti indirizzi IPv4 statici per stabilire le sottoreti:

- **Interfaccia LAN (Gateway Kali):** 192.168.100.1/24
- **Interfaccia OPT1 (Gateway Metasploitable):** 192.168.50.1/24



Evidenza Figura 3: L'output della console dimostra che la segmentazione logica della rete è attiva, con la rete Kali (100.x) separata dalla rete Target (50.x).

---

3. Fasi di Implementazione

3.1 Configurazione dell'Interfaccia

Dopo aver assegnato la porta vtnet2 all'interfaccia **OPT1**, è stata applicata la configurazione IPv4 statica (192.168.50.1). Ciò ha abilitato il router Pfsense a instradare il traffico tra le sottoreti 100.x (LAN) e 50.x (OPT1).

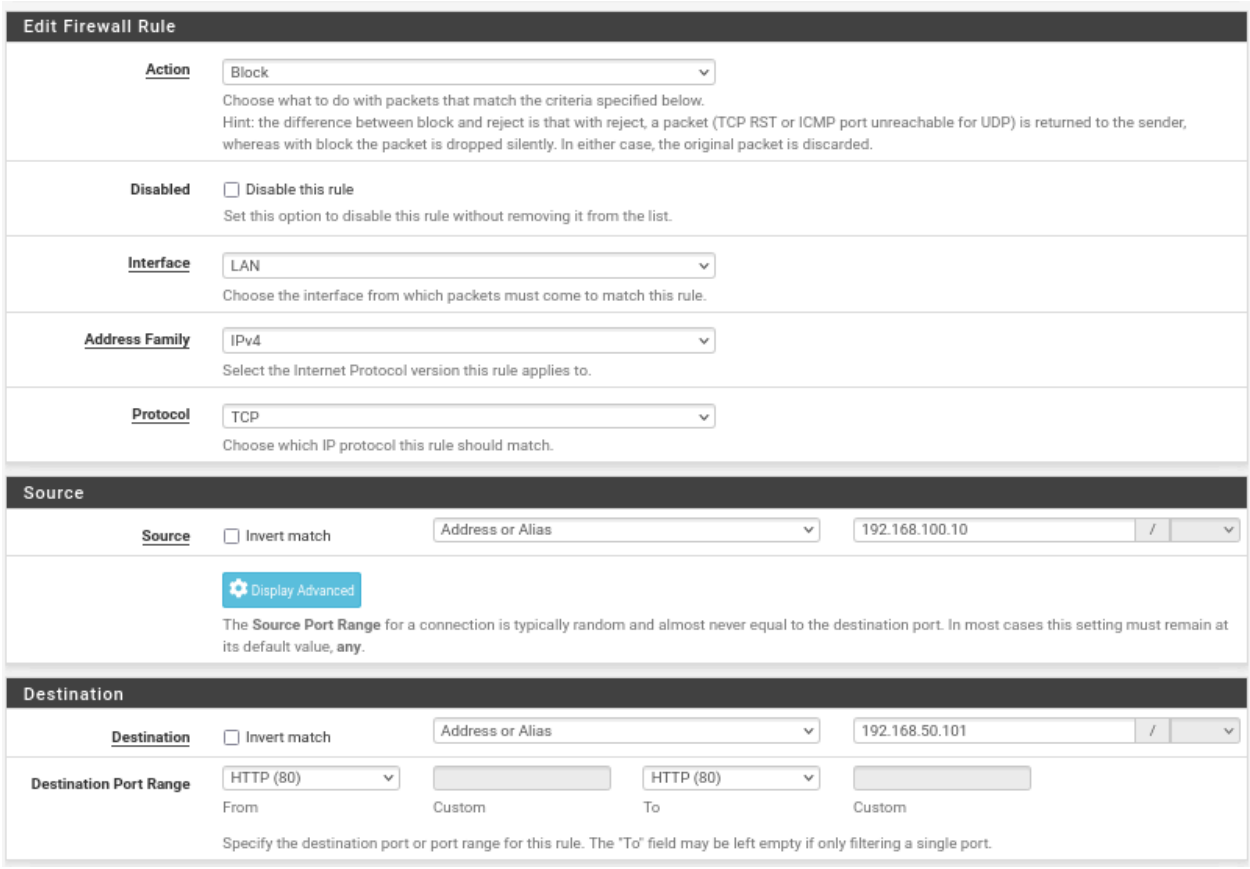
3.2 Logica della Regola Firewall

Per impedire alla macchina Kali di eseguire scansioni web o accedere all'applicazione web DVWA ospitata su Metasploitable, è stata creata una regola di filtraggio pacchetti sull'**interfaccia LAN**. La regola è stata posizionata sull'interfaccia LAN perché le regole del firewall vengono elaborate sull'*interfaccia da cui il traffico ha origine* (ingress).

Dettagli Configurazione Regola:

- **Azione (Action):** Block (Scarta il pacchetto silenziosamente).

- **Interfaccia (Interface):** LAN (Traffico proveniente *da* Kali).
- **Protocollo (Protocol):** TCP (Il protocollo usato per la navigazione HTTP).
- **Sorgente (Source):** 192.168.100.10 (L'IP specifico della macchina Kali).
- **Destinazione (Destination):** 192.168.50.101 (L'IP specifico della macchina Metasploitable).
- **Porta di Destinazione (Destination Port):** 80 (HTTP) (La porta del server web).



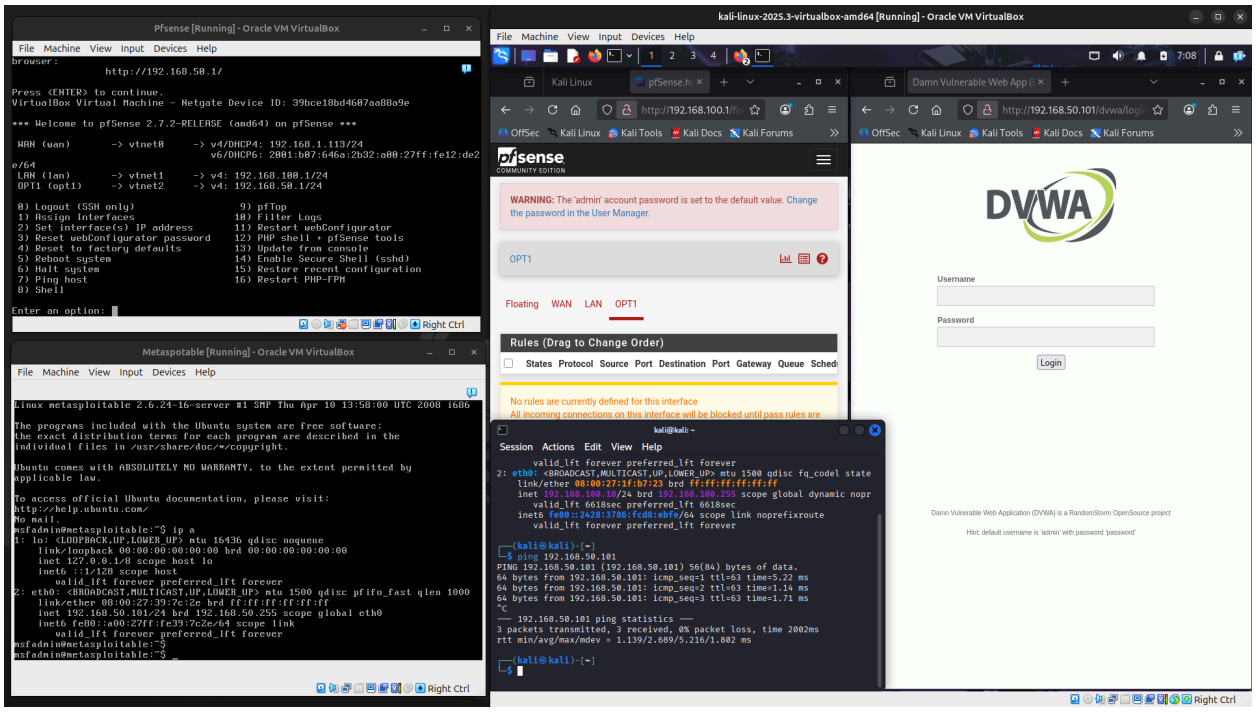
Evidenza Figura 4: Questo dettaglio mostra i parametri specifici utilizzati per applicare la policy. Dimostra che viene colpito solo il traffico HTTP (Porta 80) proveniente dall'IP sorgente specifico, soddisfacendo l'obiettivo di "bloccare l'accesso alla DVWA".

Spiegazione Tecnica:
Prendendo di mira la Porta TCP 80, questa regola interrompe specificamente l'handshake a 3 vie (3-way handshake) necessario per stabilire una connessione HTTP. Quando la macchina Kali tenta di inviare un pacchetto SYN per avviare una scansione web o navigare nel sito, il firewall scarta il pacchetto, causando il blocco del tentativo di connessione e il conseguente timeout.

4. Test e Verifica

4.1 Pre-Configurazione (Baseline)

Prima di applicare la regola di blocco, è stata verificata la connettività. La macchina Kali (192.168.100.10) è stata in grado di pingare con successo il bersaglio e caricare la pagina di login DVWA ospitata su 192.168.50.101.

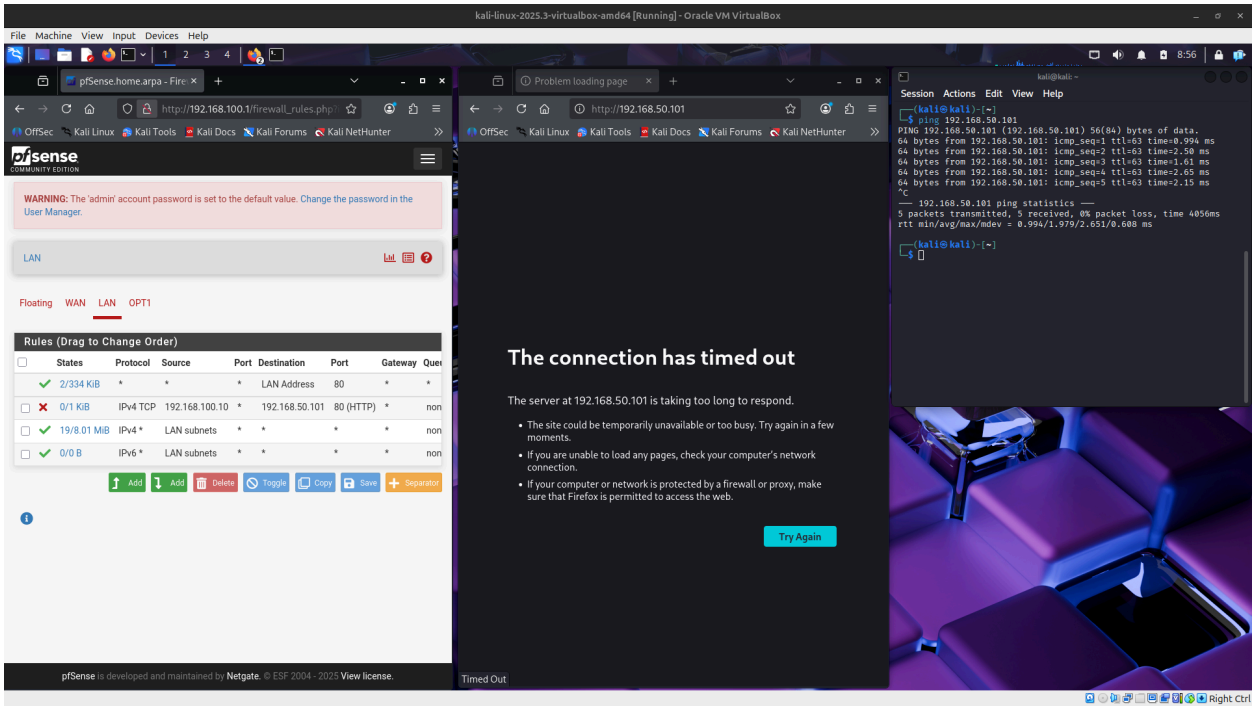


Evidenza Figura 5: Questo screenshot "Prima" è fondamentale per provare che il routing e il server web funzionavano correttamente *prima* della regola di sicurezza. Conferma che qualsiasi fallimento successivo è dovuto al firewall e non a un errore di rete.

4.2 Post-Configurazione (Verifica)

Dopo aver applicato la regola firewall, il test è stato ripetuto per verificare il blocco.
Osservazioni:

1. **Accesso Web:** Il browser su Kali ha tentato di connettersi a http://192.168.50.101 ma non è riuscito a caricare la risorsa. Il browser ha mostrato un errore "The connection has timed out", indicando che i pacchetti TCP venivano scartati dal firewall.
2. **Statistiche Firewall:** La lista delle regole di Pfsense mostra che la regola di blocco specifica è attiva.



Evidenza Figura 6: Questo screenshot "Dopo" convalida il successo del laboratorio. Mostra un timeout della connessione (HTTP) e la perdita dei pacchetti (Ping) esclusivamente verso la macchina bersaglio, confermando che la scansione è stata impedita.

---

5. Conclusione

I requisiti del laboratorio sono stati soddisfatti. È stata aggiunta con successo una nuova interfaccia (OPT1) per segmentare la rete, separando la macchina attaccante da quella vittima. La regola firewall ha bloccato efficacemente l'accesso della macchina Kali ai servizi web sul target Metasploitable, come evidenziato dai timeout di connessione nella fase di verifica.