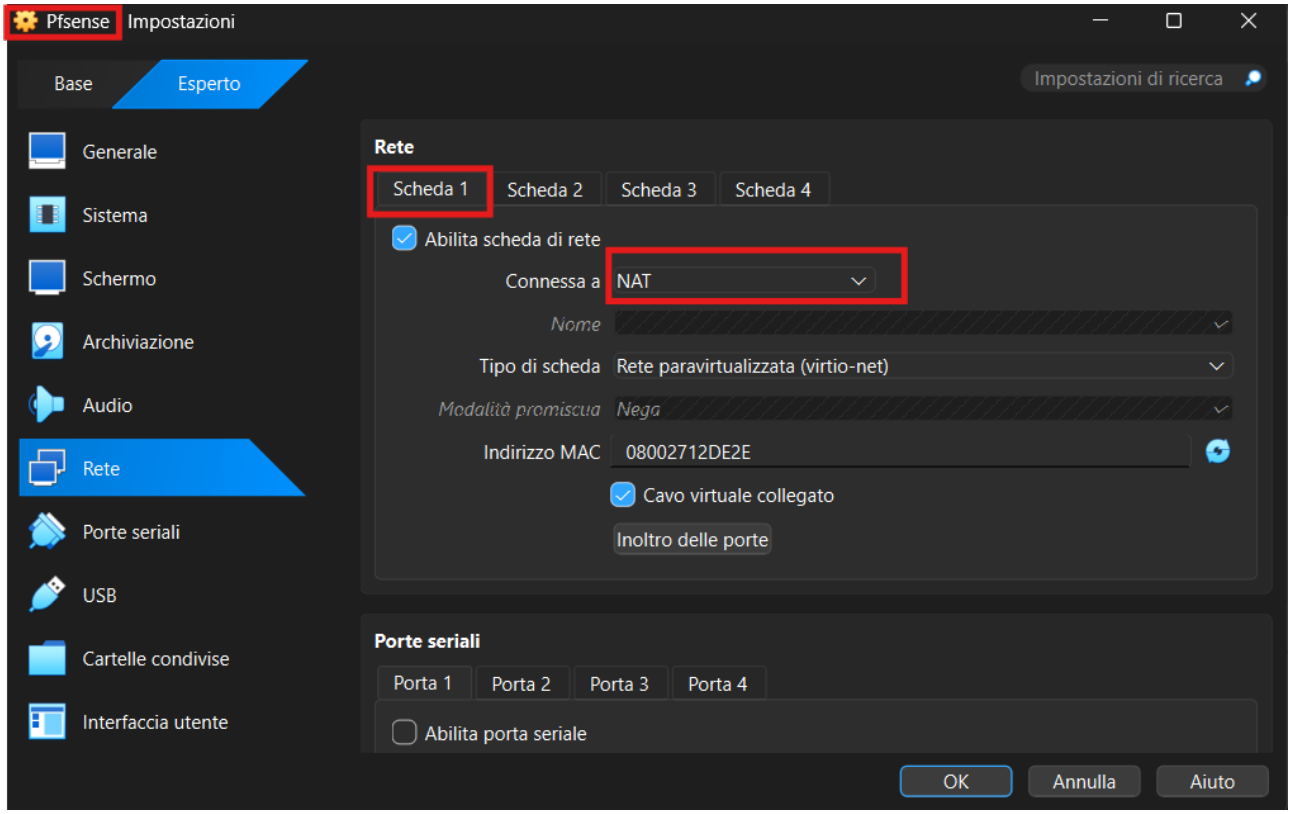
S3 – L5 – PROGETTO

In questo esercizio verrà configurato un ambiente di laboratorio con **pfSense come firewall**, collegando due reti interne (**Kali Linux** e **Metasploitable**), per **analizzare e dimostrare il filtraggio del traffico**, bloccando selettivamente il servizio **HTTP da Kali verso Metasploitable** e verificando il comportamento della rete **prima e dopo l'applicazione delle regole di firewall**.



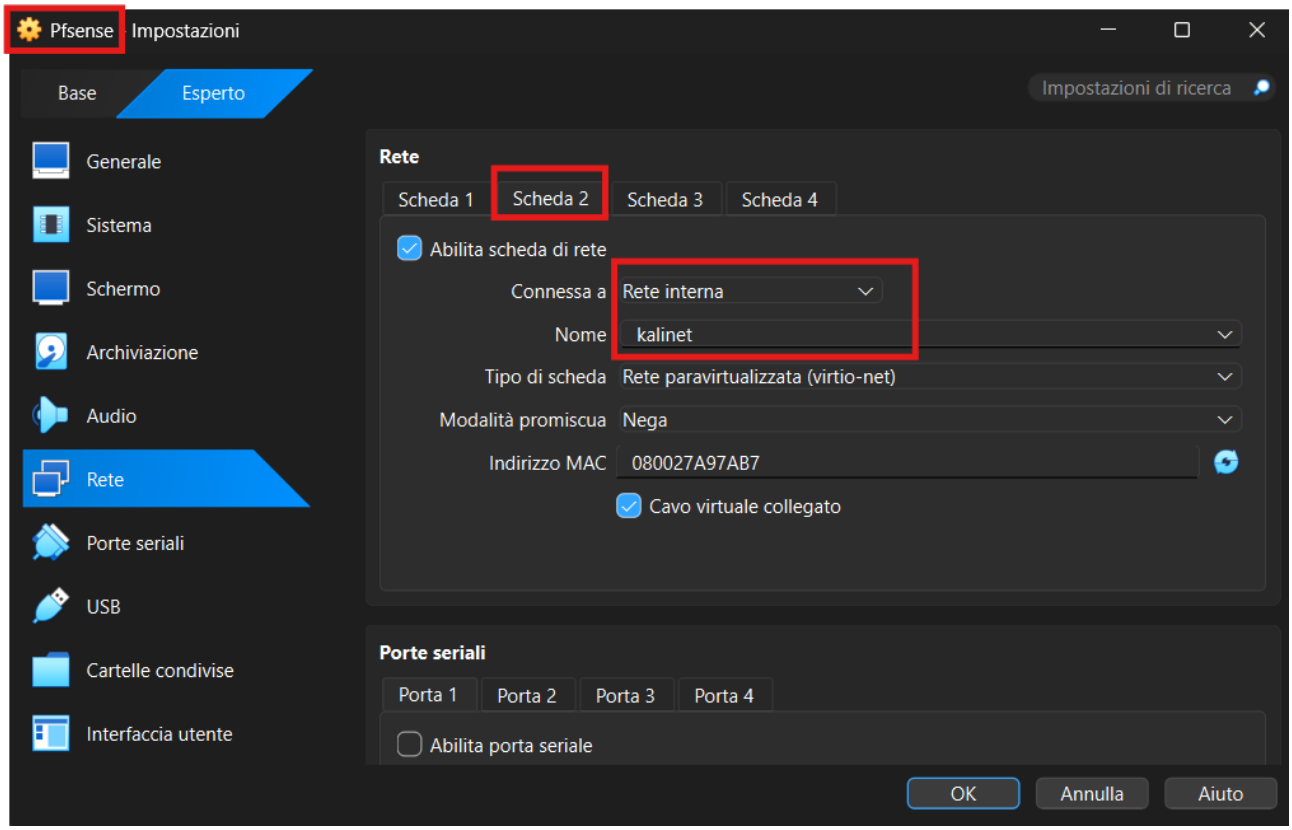
1) pfSense – VirtualBox Rete – Scheda 1 (NAT)

Cosa ho fatto

1. Ho aperto le **Impostazioni** della VM **pfSense** in VirtualBox.
2. In **Rete → Scheda 1** ho abilitato la scheda e selezionato **Connessa a: NAT**.

Perché

- La Scheda 1 funge da **WAN** e permette a pfSense di avere connettività "verso l'esterno" tramite NAT (necessario per simulare Internet/uscita).



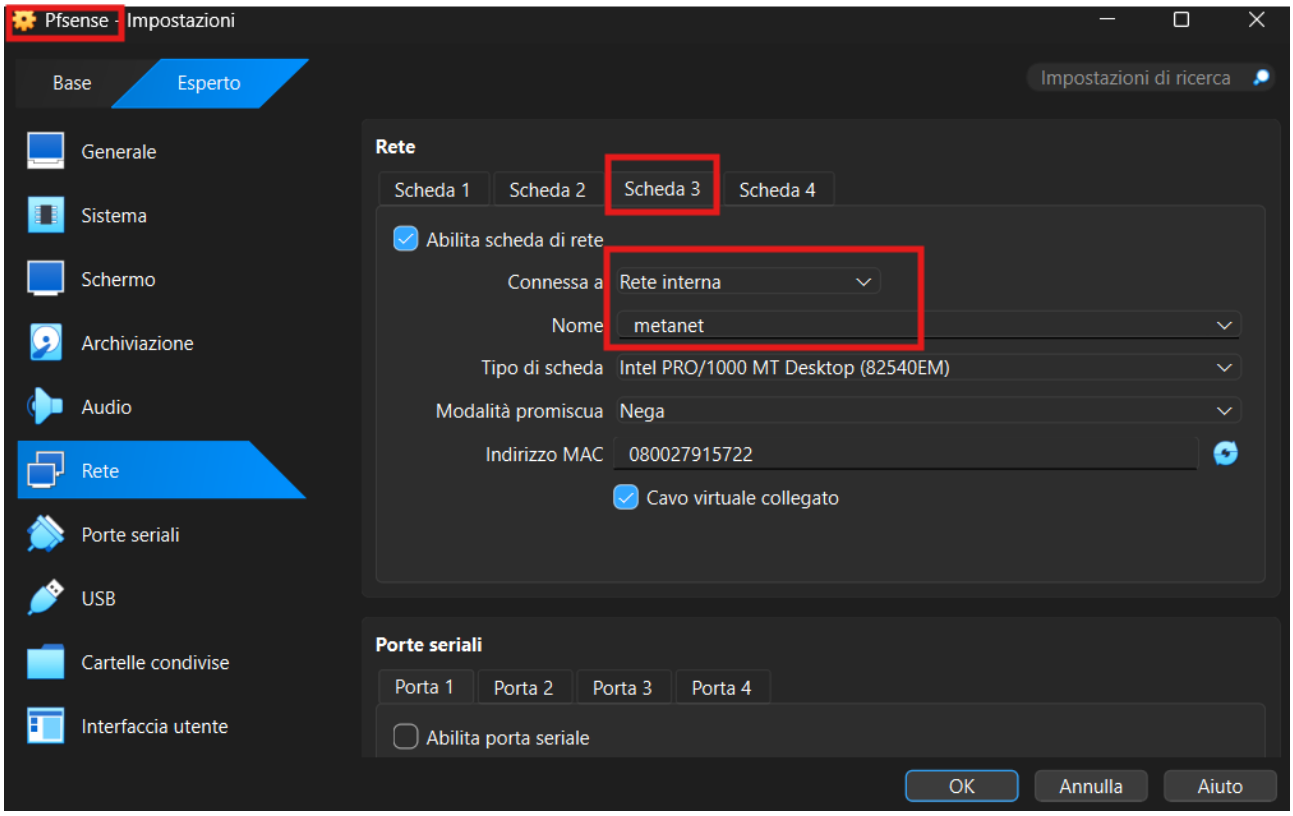
2) pfSense – VirtualBox Rete – Scheda 2 (Rete interna: kalinet)

Cosa ho fatto

1. Sempre in VirtualBox, in **Rete → Scheda 2** ho abilitato la scheda.
2. Ho impostato **Connessa a: Rete interna**.
3. Ho assegnato il nome rete interna **kalinet**.

Perché

- Questa scheda crea la LAN “di laboratorio” su cui si trova **Kali** (segmento dedicato ai client/attaccante).



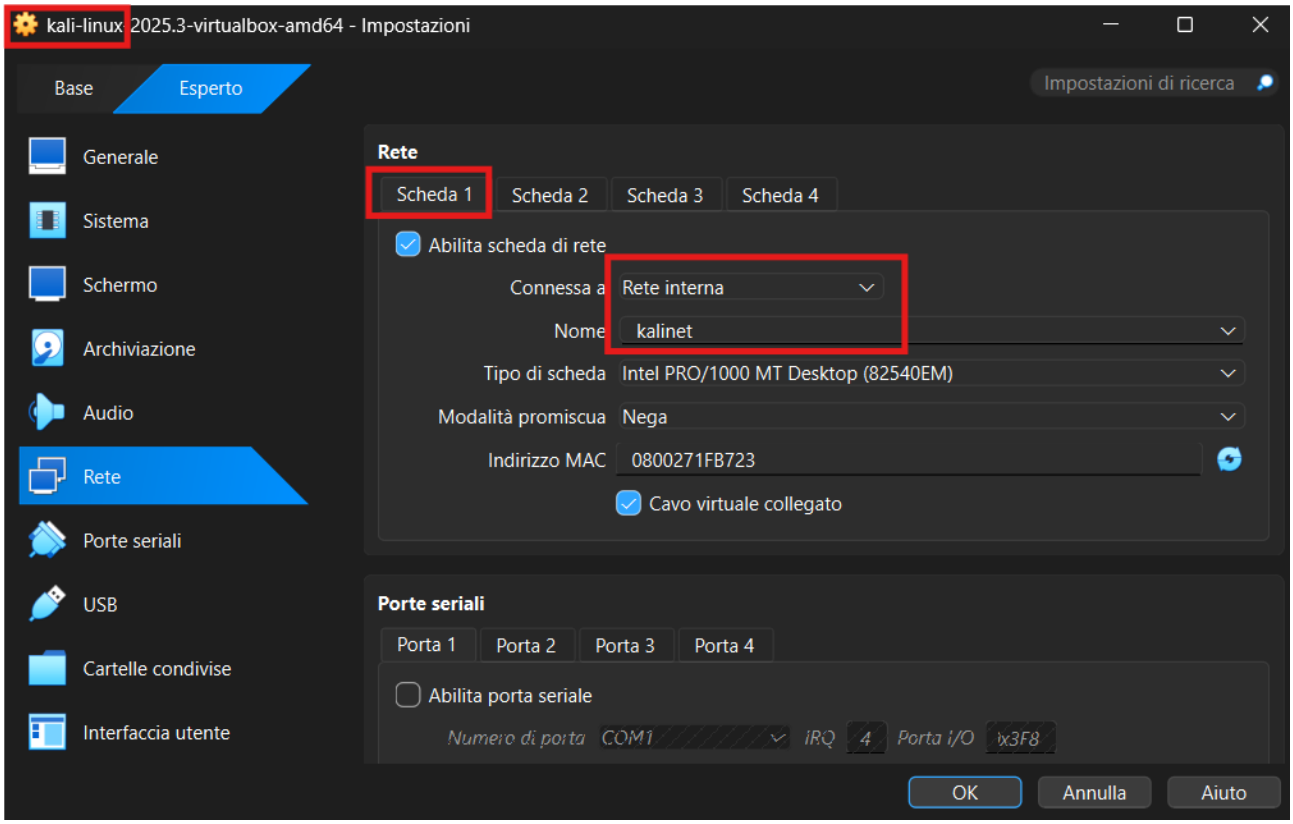
3) pfSense – VirtualBox Rete – Scheda 3 (Rete interna: metanet)

Cosa ho fatto

1. In **Rete → Scheda 3** ho abilitato la scheda.
2. Ho impostato **Connessa a: Rete interna**.
3. Ho assegnato il nome rete interna **metanet**.

Perché

- Questa scheda crea la rete interna dedicata alla **macchina target** (Metasploitable), separata dalla rete “Kali”.



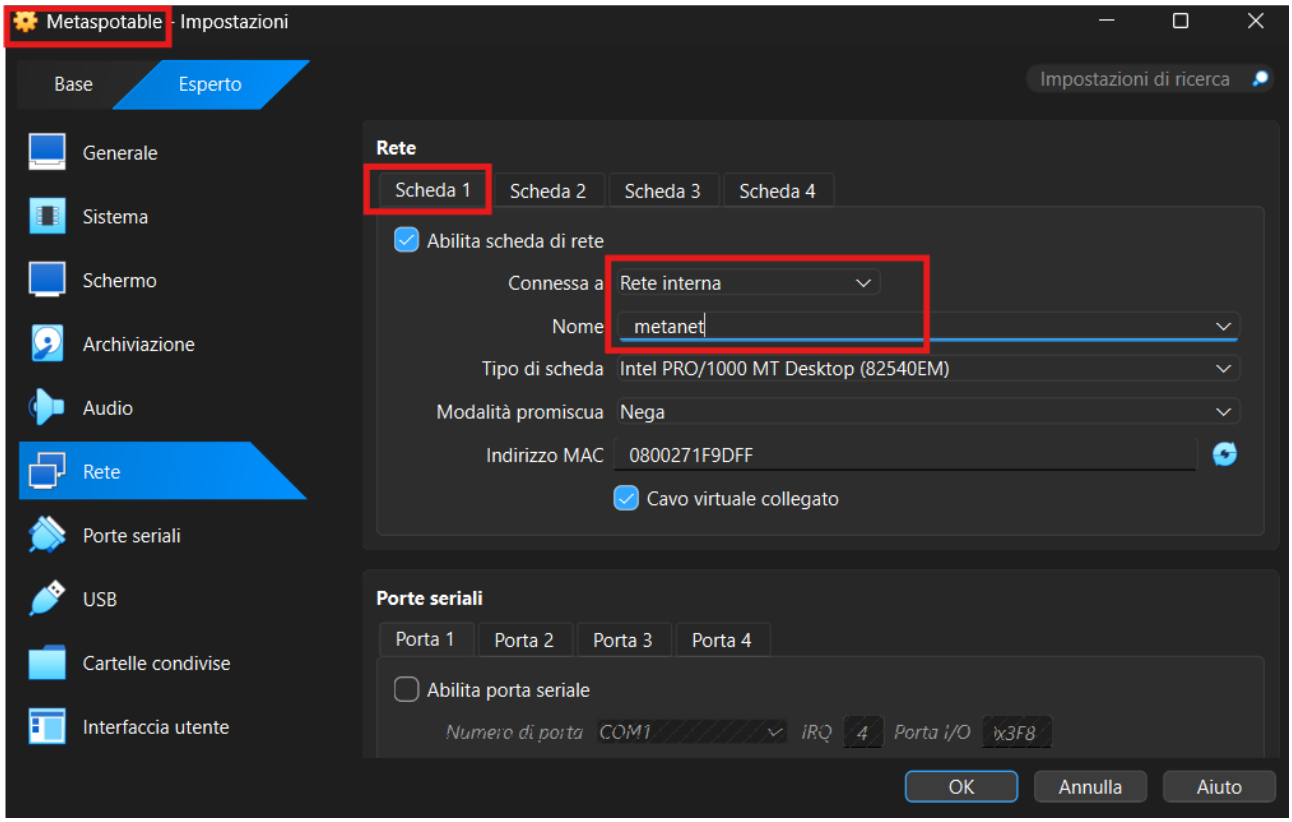
4) Kali Linux – VirtualBox Rete – Scheda 1 (Rete interna: kalinet)

Cosa ho fatto

1. Ho aperto le **Impostazioni** della VM **Kali Linux**.
2. In **Rete → Scheda 1** ho scelto **Connessa a: Rete interna**.
3. Ho selezionato la rete **kalinet**.

Perché

- Kali deve stare nella stessa rete interna della **LAN di pfSense** (kalinet) per poter raggiungere pfSense e la rete target attraverso il firewall.



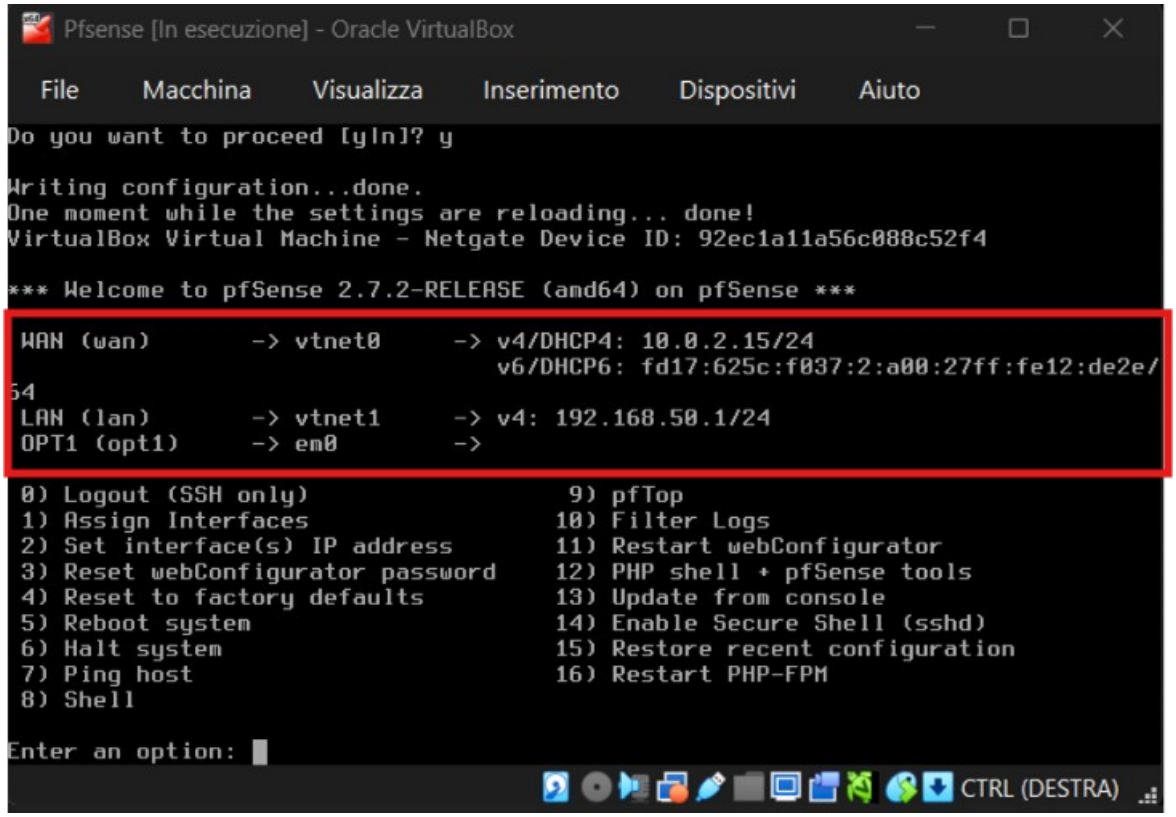
5) Metasploitable – VirtualBox Rete – Scheda 1 (Rete interna: metanet)

Cosa ho fatto

1. Ho aperto le **Impostazioni** della VM **Metasploitable**.
2. In **Rete → Scheda 1** ho selezionato **Connessa a: Rete interna**.
3. Ho scelto la rete **metanet**.

Perché

- Metasploitable deve stare nella rete interna “target” (metanet) che viene gestita da pfSense tramite l’interfaccia OPT1.



6) pfSense – Console (schermo nero) con WAN / LAN / OPT1

Cosa ho fatto

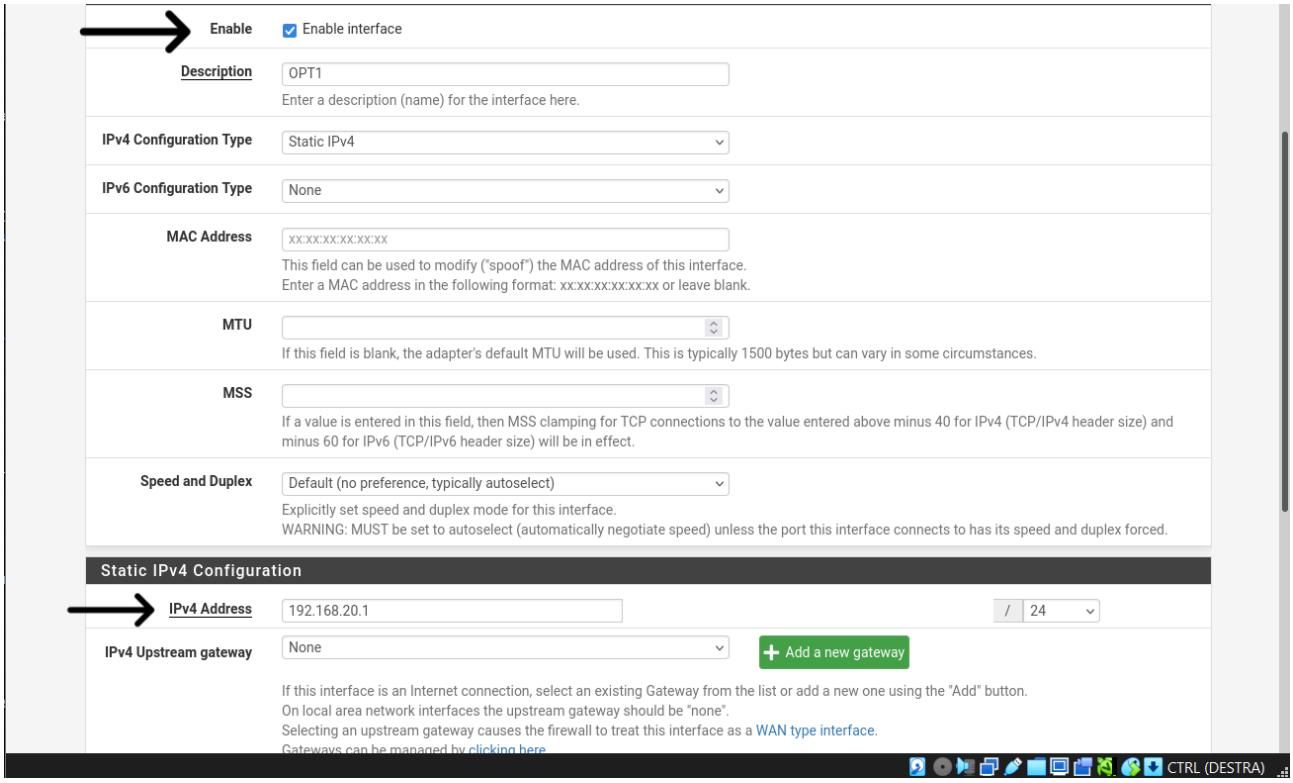
1. Ho avviato la VM **pfSense**.
2. Dalla console ho verificato che pfSense riconosca le **3 interfacce** e i relativi indirizzi.

Cosa si vede

- **WAN (vtnet0)** con IP in DHCP (rete NAT, es. 10.0.2.x).
- **LAN (vtnet1)** con IP **192.168.50.1/24** (rete kalinet).
- **OPT1 (em0)** associata alla terza scheda (rete metanet) e configurata lato pfSense.

Perché è importante

- Dimostra la corretta **mappatura delle schede di rete** e la separazione dei segmenti.



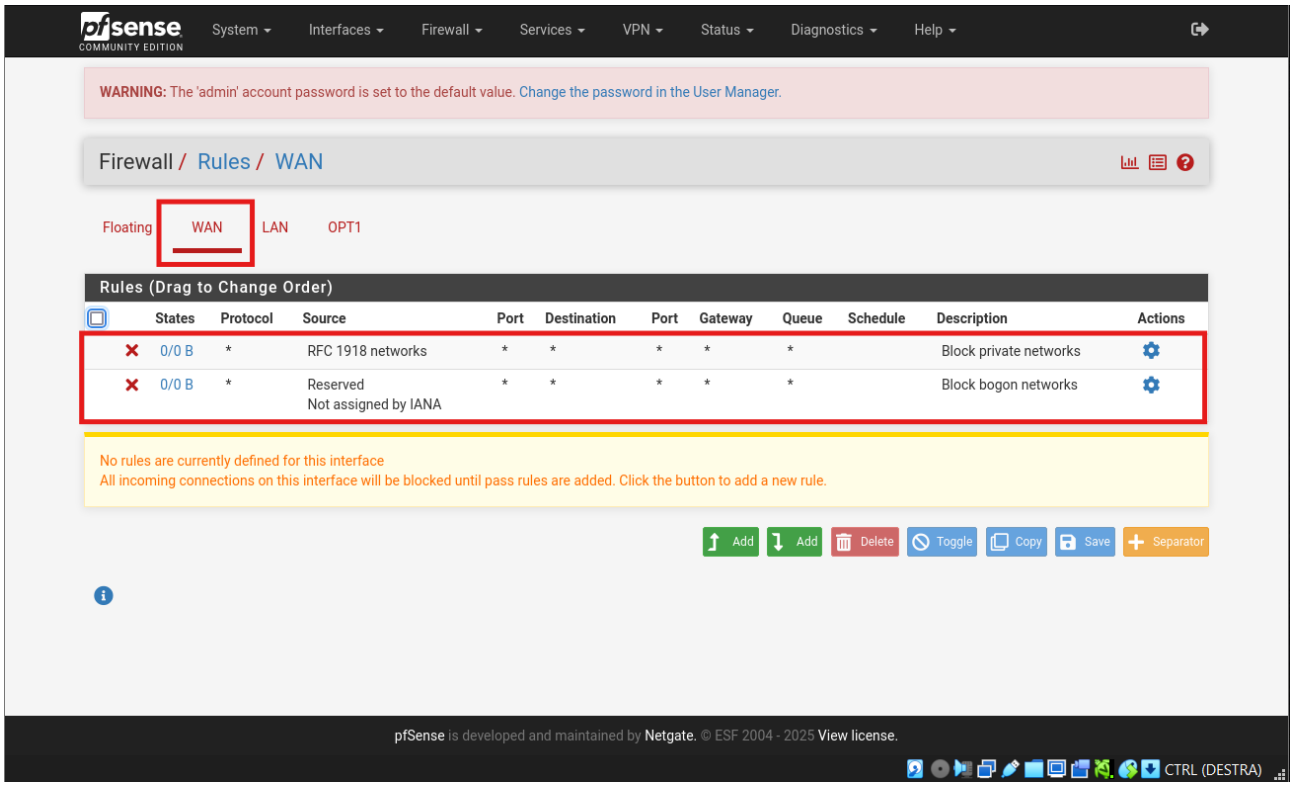
7) pfSense GUI – Interfaccia OPT1 configurata (192.168.20.1/24)

Cosa ho fatto

1. Dal browser di Kali ho aperto il pannello di pfSense.
2. Sono andato in **Interfaces → OPT1**.
3. Ho abilitato l'interfaccia e impostato:
    - **IPv4 Configuration Type: Static IPv4**
    - **IPv4 Address: 192.168.20.1 /24**
    - **Gateway: None** (corretto per rete locale)

Perché

- OPT1 è la rete dove risiede la macchina target: pfSense fa da **gateway** per la subnet **192.168.20.0/24**.



8) pfSense – Firewall → Rules → WAN

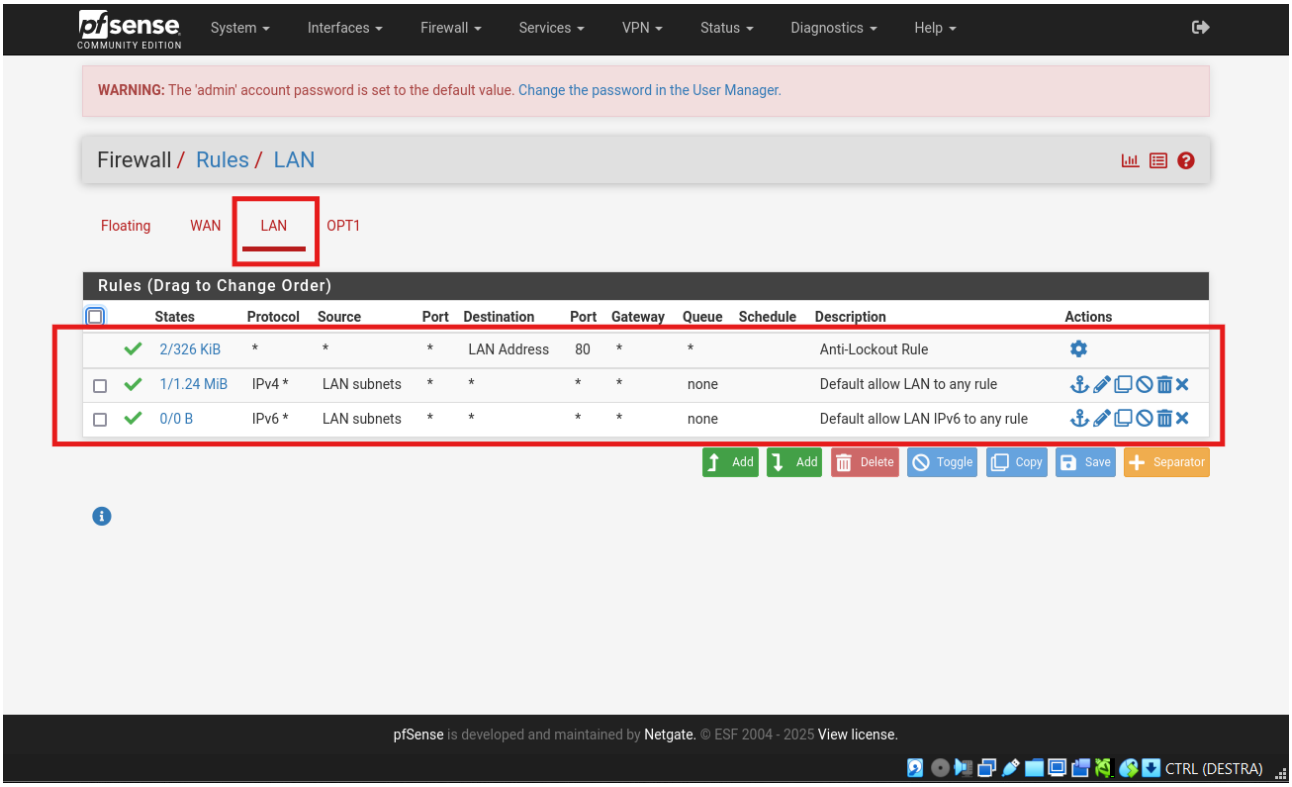
Cosa ho fatto

1. In pfSense ho aperto **Firewall → Rules → WAN**.

Cosa si vede / perché va bene

- Sono presenti le regole di default tipiche della WAN:
  - **Block private networks**
  - **Block bogon networks**

- Non ho aggiunto regole custom sulla WAN perché l’esercizio richiede un controllo mirato tra le reti interne (Kali ↔ Metasploitable).



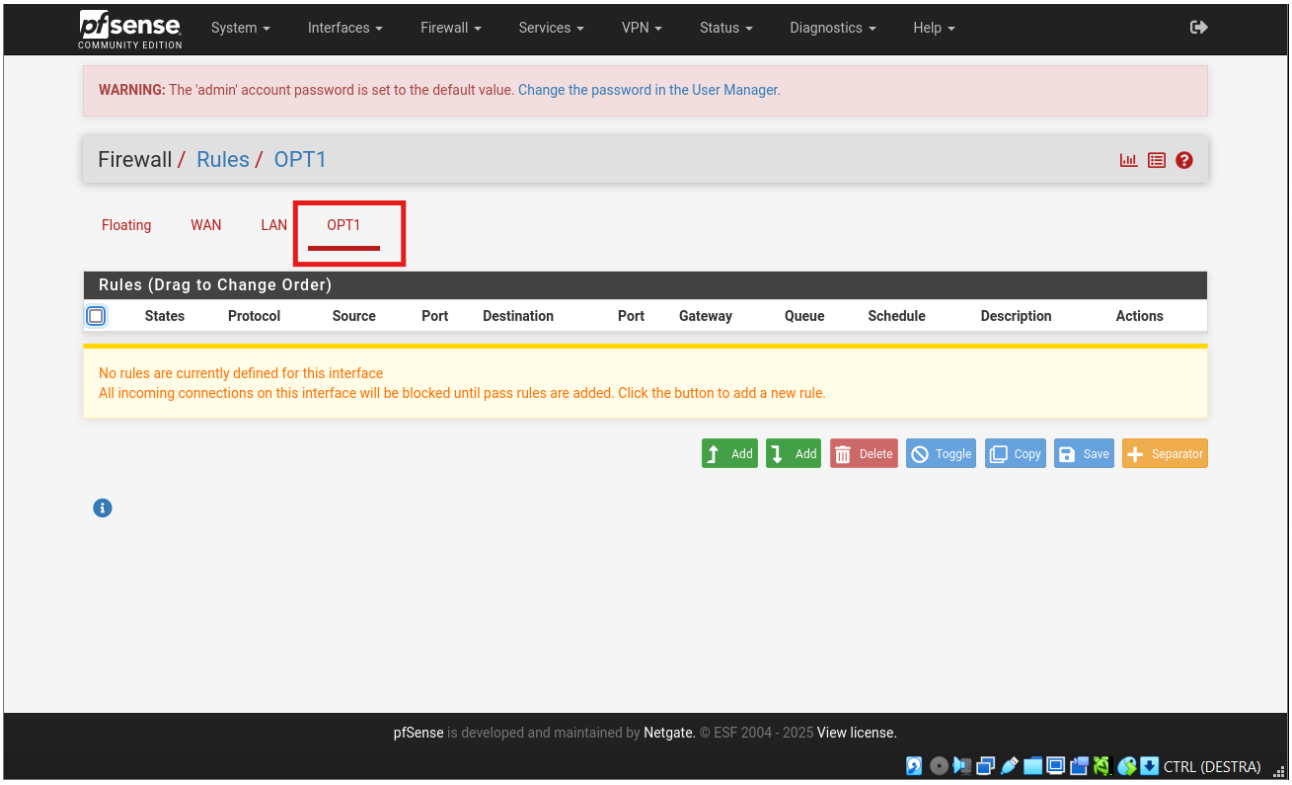
9) pfSense – Firewall → Rules → LAN

Cosa ho fatto

1. In pfSense ho aperto **Firewall → Rules → LAN**.

Cosa si vede / perché va bene

- Regole di default (allow LAN to any) + regole/struttura necessarie all’esercizio.
- Questa sezione è quella dove si inserisce la regola che **blocca HTTP solo da Kali verso Metasploitable** (regola mirata lato LAN perché Kali si trova in questo segmento).



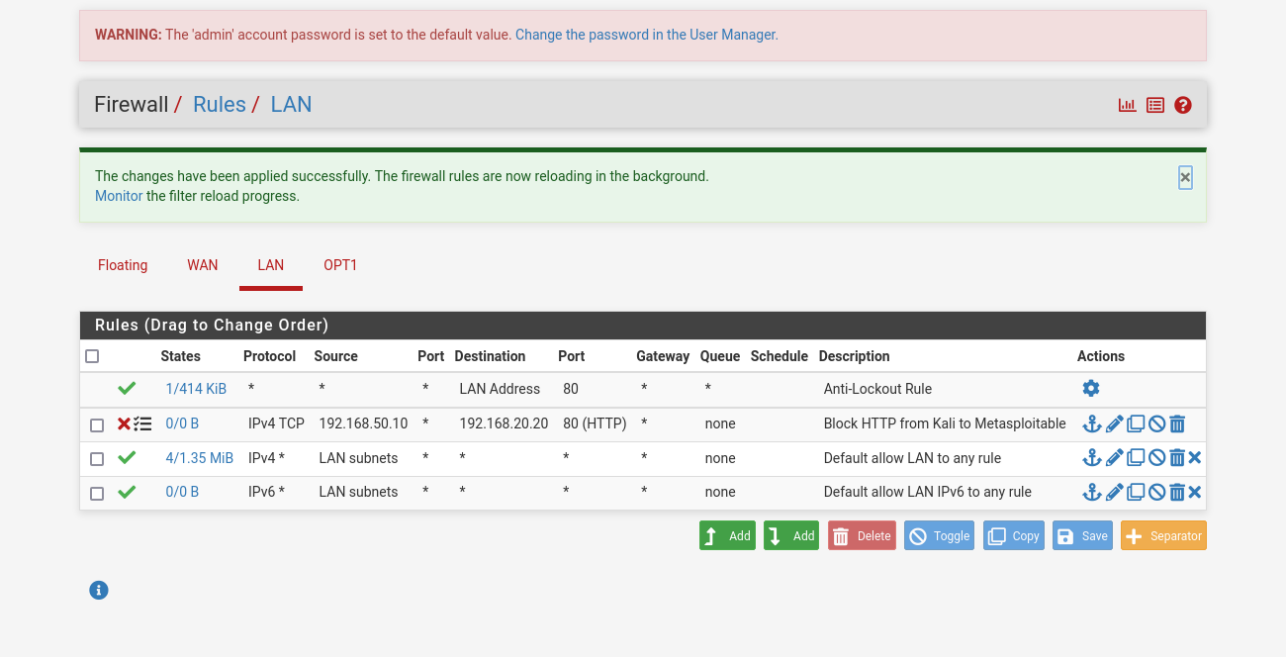
10) pfSense – Firewall → Rules → OPT1

Cosa ho fatto

1. In pfSense ho aperto **Firewall → Rules → OPT1**.

Cosa si vede / perché va bene

- Nessuna regola specifica su OPT1 (stato “No rules…”).
- È coerente con l’impostazione dell’esercizio: la regola richiesta è costruita in modo mirato rispetto alla sorgente **Kali (LAN)** e al servizio da bloccare (HTTP verso la macchina target).



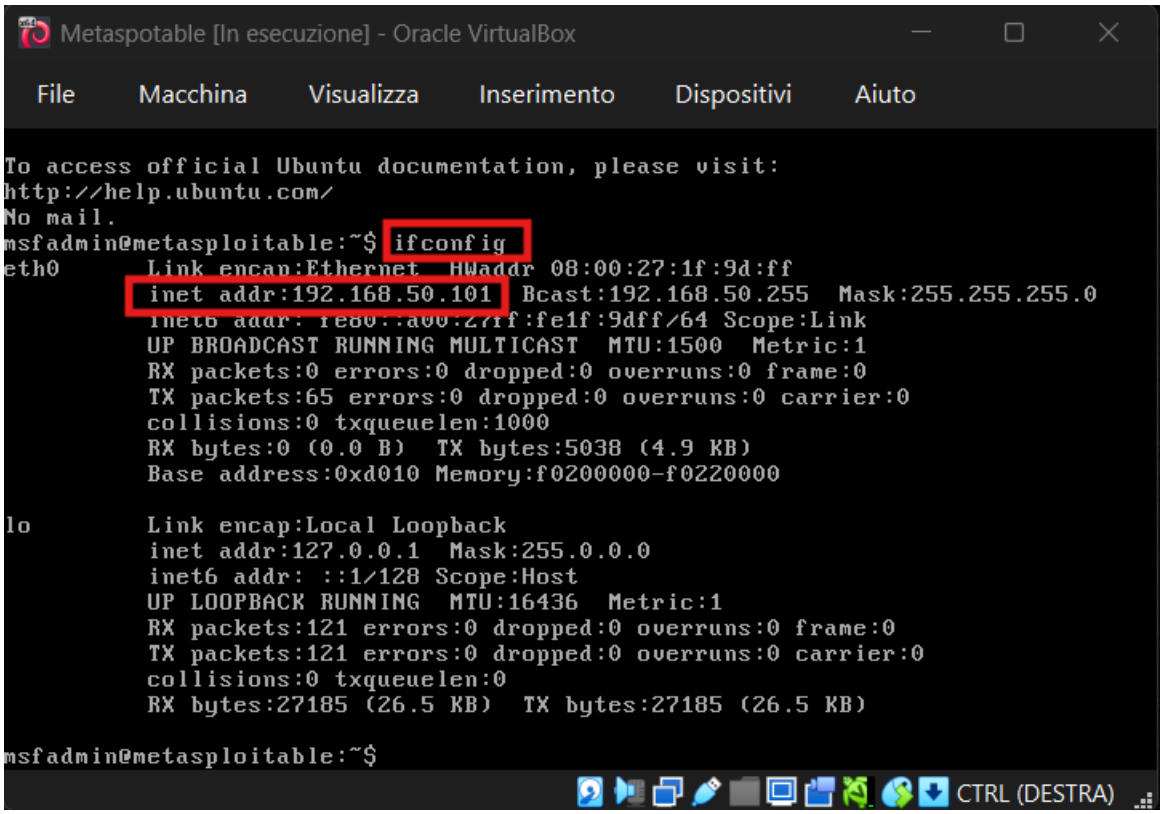
11) pfSense – Firewall → Rules → LAN – Regola di blocco HTTP

Cosa ho fatto

1. Dal pannello di pfSense ho aperto **Firewall → Rules → LAN**.
2. Ho creato una regola di tipo **Block** che blocca il traffico **HTTP (porta 80)**.
3. Ho impostato:
    - **Source**: `192.168.50.10` (Kali Linux)
    - **Destination**: `192.168.20.20` (Metasploitable)
    - **Protocol**: TCP
    - **Destination Port**: HTTP (80)

Perché

- Questa regola serve a **impedire esclusivamente l’accesso HTTP da Kali verso Metasploitable**, lasciando inalterati gli altri tipi di traffico.
- La posizione della regola sopra la “Default allow LAN to any” è fondamentale, perché pfSense applica le regole **dall’alto verso il basso**.



12) Metasploitable – Verifica indirizzo IP (ifconfig)

Cosa ho fatto

1. Ho effettuato l'accesso alla macchina **Metasploitable** tramite console (`msfadmin / msfadmin`).
2. Ho eseguito il comando:

   `ifconfig`

3. Ho verificato l'indirizzo IP assegnato all'interfaccia **eth0**.

Cosa si vede

- La macchina Metasploitable utilizza l'indirizzo IP **192.168.50.101**, appartenente alla rete interna configurata tramite pfSense.

Perché

- Questa verifica conferma che Metasploitable è **correttamente configurata a livello di rete** ed è raggiungibile (prima dell'applicazione della regola) dai segmenti gestiti dal firewall.

Spiegazione della regola di firewall

Nel corso dell'esercizio è stata configurata una regola di firewall su pfSense con lo scopo di **bloccare il traffico HTTP dalla macchina Kali Linux verso la macchina Metasploitable**, mantenendo attivi gli altri tipi di comunicazione di rete.

La regola è stata applicata sull'interfaccia **LAN**, in quanto Kali Linux si trova all'interno di questa rete. In pfSense le regole vengono valutate sull'interfaccia di ingresso del traffico, rendendo questa scelta coerente con l'architettura della rete configurata.

È stata scelta un'azione di tipo **Block** per impedire l'accesso al servizio web senza interrompere completamente la comunicazione tra i due host. Il protocollo selezionato è **TCP**, poiché utilizzato dal servizio HTTP, mentre la porta di destinazione è la **80**, specifica per questo servizio.

La sorgente della regola è stata limitata all'indirizzo IP di Kali Linux, mentre la destinazione è stata impostata sull'indirizzo IP di Metasploitable, così da rendere il blocco mirato e non esteso a tutta la rete. La posizione della regola sopra la regola di default consente di intercettare il traffico prima che venga autorizzato.

Conclusioni

L'attività svolta ha permesso di comprendere in modo pratico il funzionamento di un firewall e l'importanza della segmentazione e del controllo del traffico di rete. Attraverso pfSense è stato possibile configurare le interfacce di rete, definire regole di filtraggio mirate e verificarne l'efficacia tramite test reali da Kali Linux.

I test effettuati hanno dimostrato che, dopo l'applicazione della regola, il servizio HTTP sulla macchina Metasploitable non è più raggiungibile dal browser di Kali, mentre il traffico ICMP continua a funzionare correttamente. Questo conferma che la regola agisce in modo selettivo, bloccando solo il servizio specificato senza compromettere la comunicazione di rete generale.

L'esercizio evidenzia come un firewall correttamente configurato sia uno strumento fondamentale per aumentare la sicurezza di una rete, riducendo la superficie di attacco e limitando l'accesso ai servizi non autorizzati.