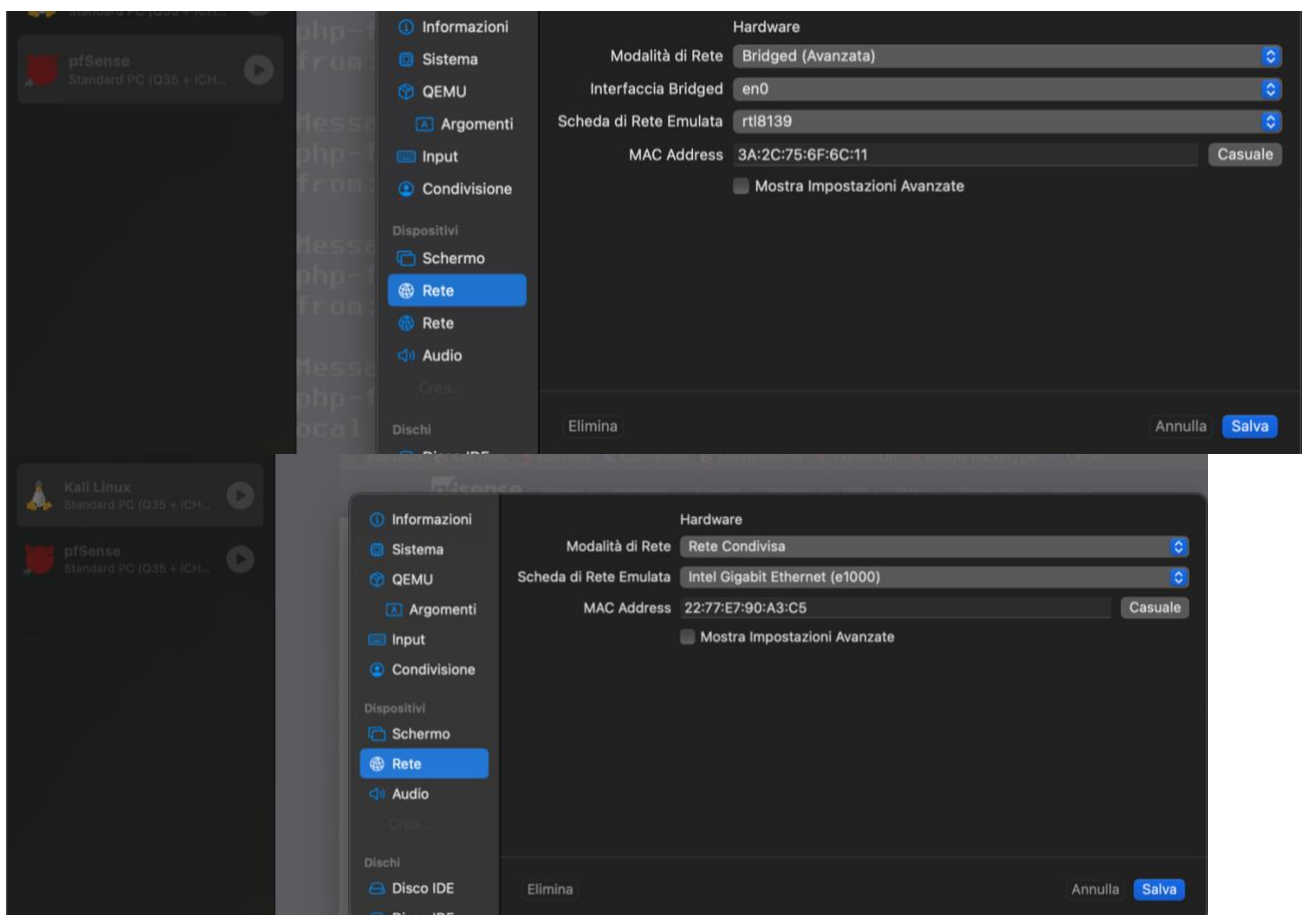
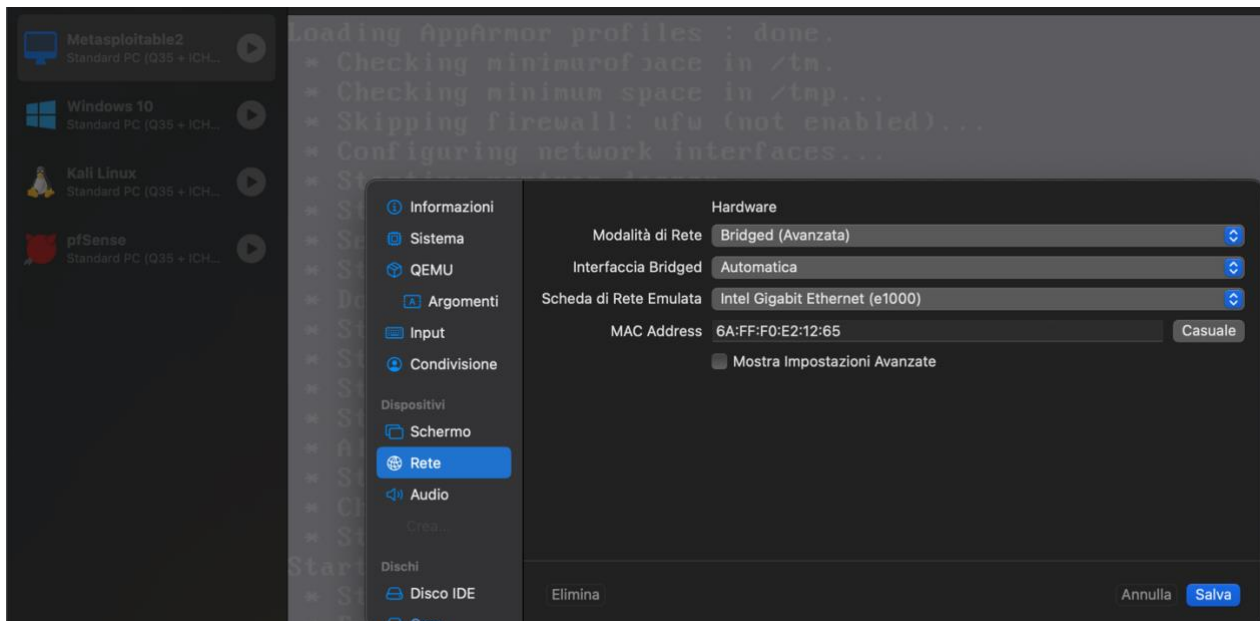


## ESERCIZIO S3L5

**TRACCIA: Creare una regola firewall che blocchi l'accesso alla DVWA (su metasploitable) dalla macchina Kali Linux e ne impedisca di conseguenza lo scan. Un requisito fondamentale dell'esercizio è che le macchine Kali e Metasploitable siano su reti diverse, potete aggiungere una nuova interfaccia di rete a Pfsense in modo tale da gestire una ulteriore rete. Connettetevi poi in Web Gui per attivare la nuova interfaccia e configurarla.**

Per prima cosa ci dobbiamo assicurare che le macchine kali e Metasploitable siano su reti diverse e che Pfsense abbia una nuova interfaccia di rete in modo tale da gestire un ulteriore rete:



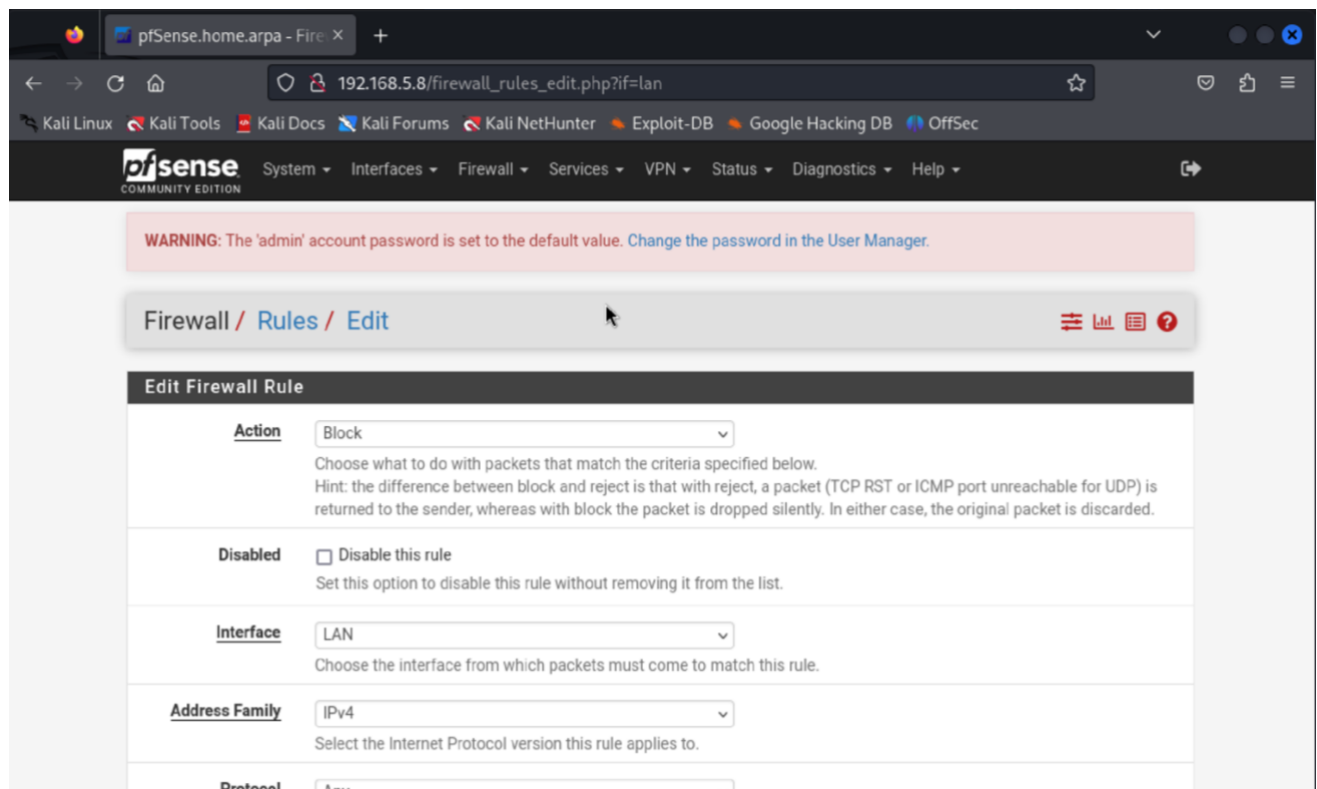


Per eseguire questo esercizio dobbiamo utilizzare la nostra macchina virtuale kali linux, e tramite firefox, connetterci alla pagina di pfsense tramite l'indirizzo di rete.

Una volta che siamo entrati su pfsense, dobbiamo impostare una regola che ci permetta di bloccare il traffico tra kali e Metasploitable.

**Di seguito i passaggi per creare una regola per bloccare il traffico tra Kali e Metasploitable:**

- Vai su **Firewall > Rules**.
- Seleziona l'interfaccia di rete che rappresenta la **rete Kali**
- Clicca su **Add** per aggiungere una nuova regola.



Successivamente dobbiamo modificare i campi in basso, l'action sarà "block", come interfaccia selezioniamo la rete di kali, protocollo "any" ovvero tutti i protocolli, come source inseriamo la rete di Kali.

- L'IP di destinazione invece sarà l'IP di Metasploitable.
- Inseriamo una descrizione che in futuro ci faccia capire a cosa serve quella regola senza il bisogno di andare ad aprirla: Block Kali to DVWA.

pfSense.home.arpa - Fire x +

192.168.5.8/firewall\_rules\_edit.php?if=lan

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Choose the interface from which packets must come to match this rule.

**Address Family** IPv4  
Select the Internet Protocol version this rule applies to.

**Protocol** Any  
Choose which IP protocol this rule should match.

**Source**

**Source** ☐ Invert match Address or Alias 192.168.1.16 /

**Destination**

**Destination** ☐ Invert match Address or Alias 192.168.5.5 /

**Extra Options**

**Log** ☐ Log packets that are handled by this rule  
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

**Description**  
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

**Advanced Options**

pfSense.home.arpa - Fire x +

192.168.5.8/firewall\_rules\_edit.php?id=2

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

**Protocol** Any  
Choose which IP protocol this rule should match.

**Source**

**Source** ☐ Invert match Address or Alias 192.168.1.16 /

**Destination**

**Destination** ☐ Invert match Address or Alias 192.168.5.5 /

**Extra Options**

**Log** ☐ Log packets that are handled by this rule  
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

**Description** Block Kali to DVWA  
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

**Advanced Options** ☒ Display Advanced

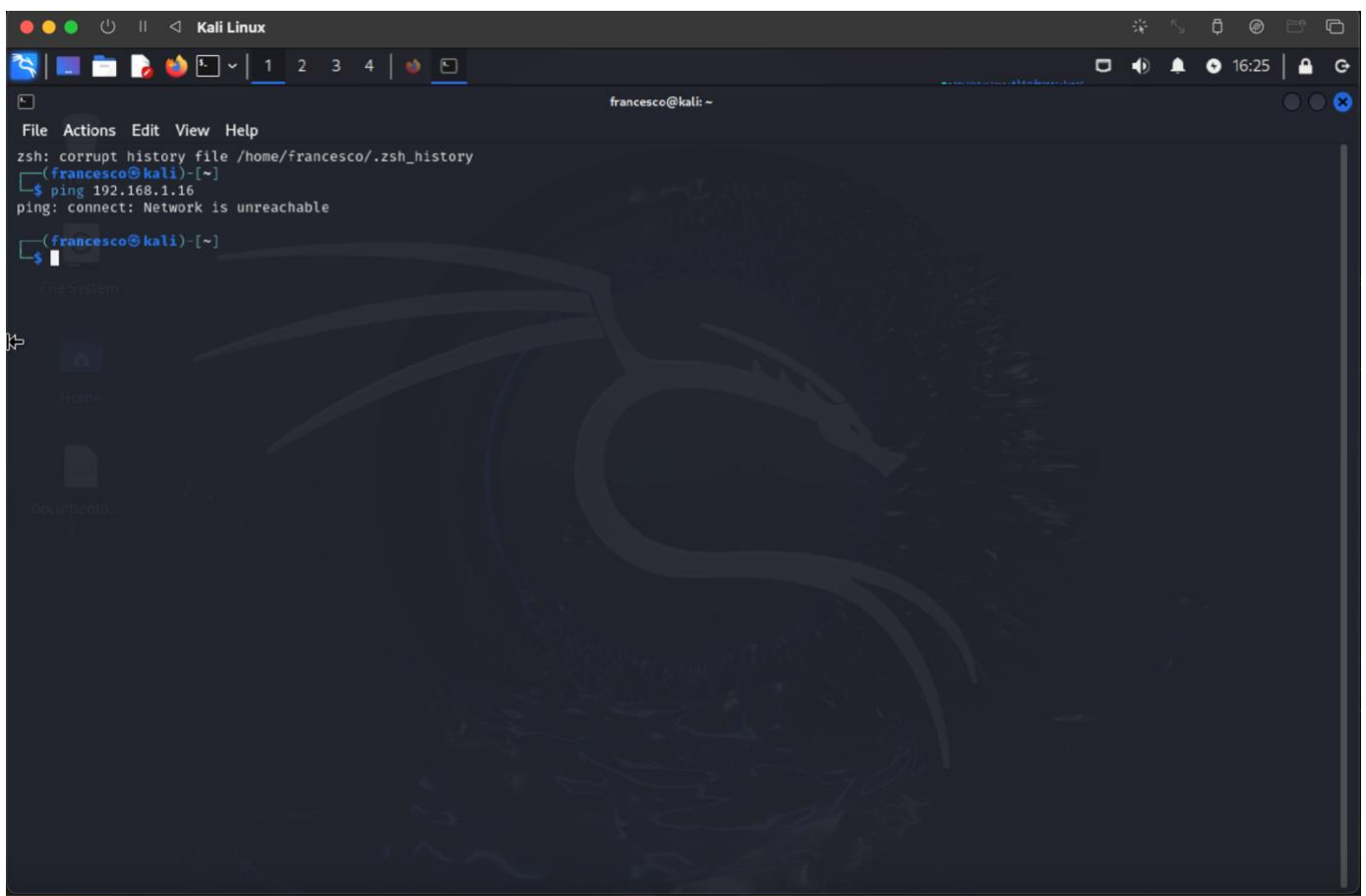
**Rule Information**

**Tracking ID** 1734103450

Dopo aver effettuato le varie modifiche, salviamo e dopo aver salvato non dobbiamo dimenticare di cliccare su apply changes, altrimenti le nostre modifiche non saranno salvate.

Adesso dobbiamo controllare se abbiamo creato la regola nel modo corretto.

Per farlo ci rechiamo nuovamente sulla nostra VM Kali linux e facciamo una prova ping per vedere se riusciamo a raggiungere la DVWA.

A screenshot of a Kali Linux terminal window. The window title is "Kali Linux". The terminal shows a message "zsh: corrupt history file /home/francesco/.zsh\_history". Below that, the prompt is "(francesco@kali)~". The user enters the command "ping 192.168.1.16". The output is "ping: connect: Network is unreachable". The prompt returns to "(francesco@kali)~". The terminal background has a dark theme with a large, faint dragon logo. The window's top bar shows various system icons and the time "16:25".

```
zsh: corrupt history file /home/francesco/.zsh_history
(francesco@kali)~
$ ping 192.168.1.16
ping: connect: Network is unreachable
(francesco@kali)~
$
```

Come possiamo vedere, alla prova del ping riceviamo il messaggio “Network is unreachable”.

Quindi la regola sembra funzionare in modo corretto.