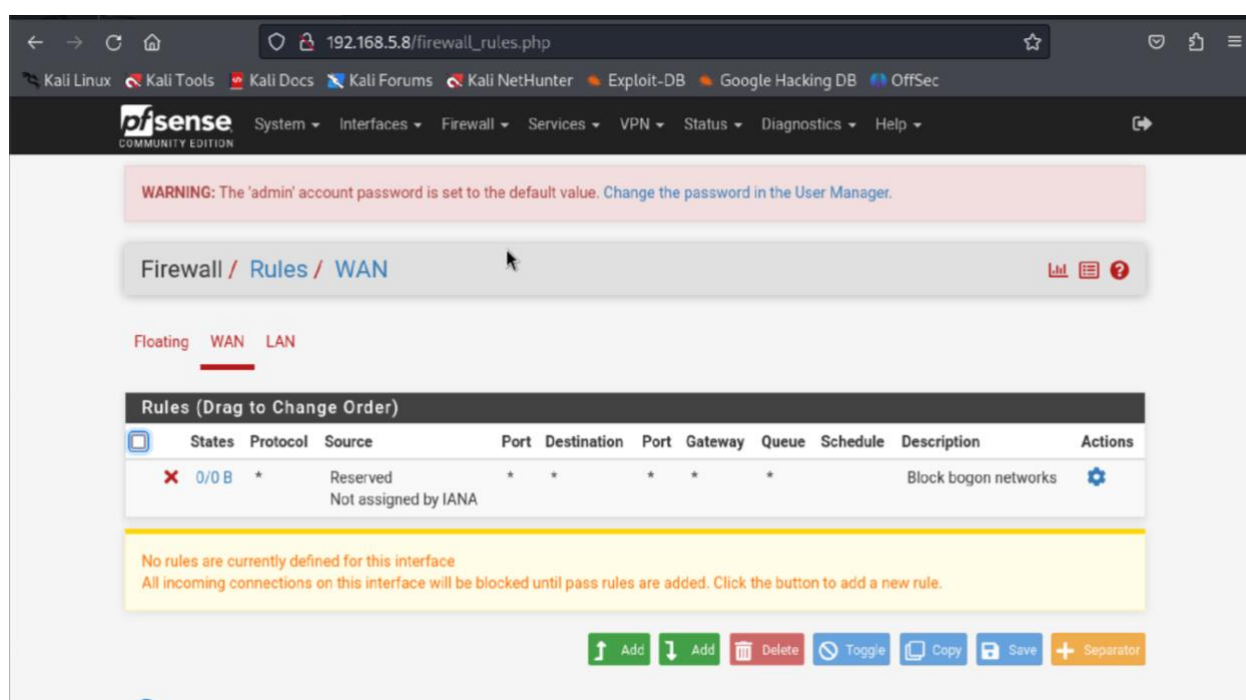


ESERCIZIO BONUS S3L5

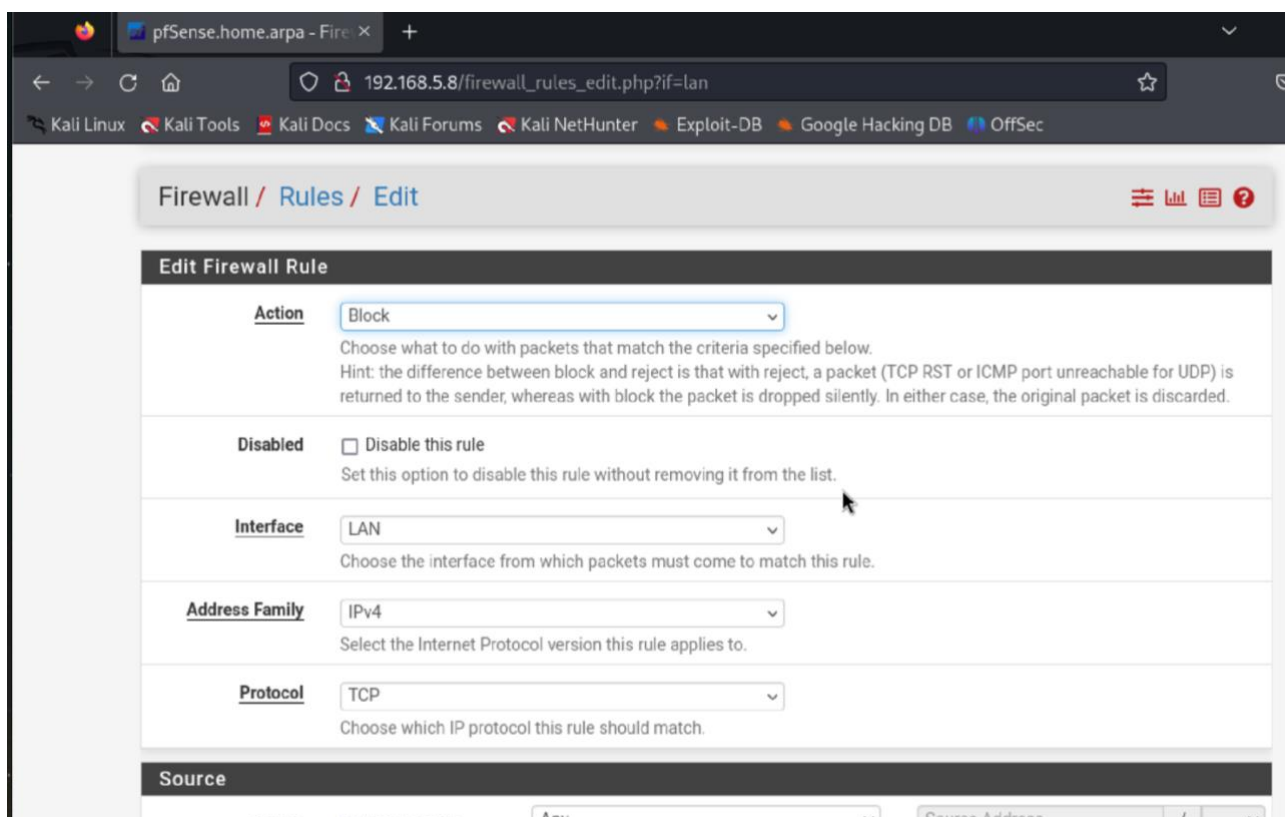
TRACCIA: impostare una regola su pfsense per bloccare da kali il telnet verso metasploitable.

Per bloccare il traffico Telnet da Kali verso Metasploitable usando pfSense, devi creare una regola di firewall che neghi esplicitamente il traffico sulla porta Telnet (porta 23).

Ci connettiamo nuovamente su pfsense, e da lì ci spostiamo su firewall rules, come nell'esercizio precedente andiamo su add per aggiungere una nuova regola.



Dopo aver cliccato su add iniziamo ad inserire i parametri per far funzionare correttamente la nostra regola:

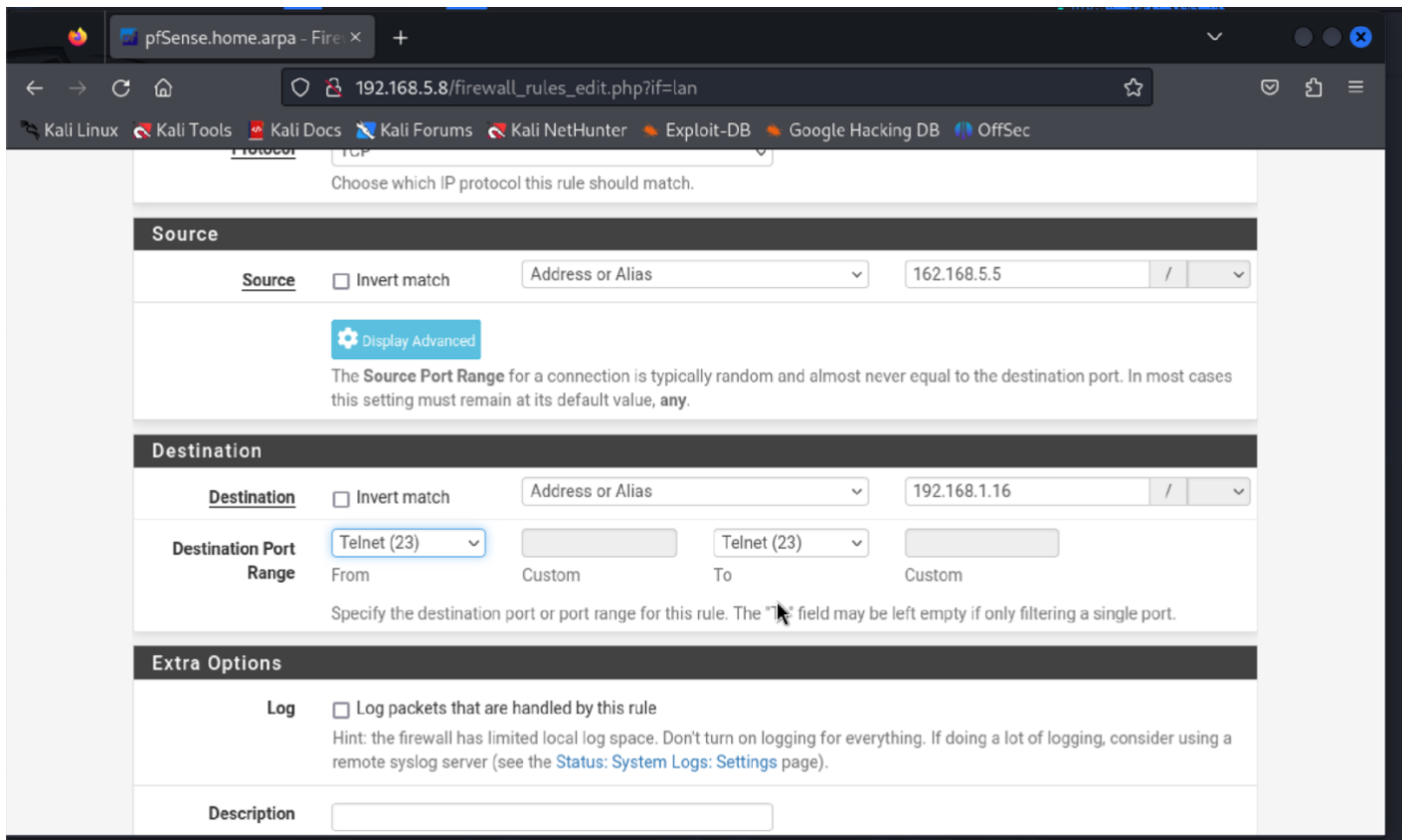


Per prima cosa action “block”, nell’interfaccia inseriamo LAN, address ipv4 ed infine protocollo TCP.

Una volta fatto questo, arriva la parte più importante, nella voce “source” dobbiamo inserire l’IP della nostra macchina Kali, mentre nella “destination” dobbiamo inserire l’indirizzo IP della nostra macchina metasploitable.

Infine in “destination port range” a noi interessa che venga bloccato l’accesso alla porta telnet, che sappiamo corrisponde alla porta numero 23. Perciò in quel range non dobbiamo fare altro che inserire da 23 a 23.

Inoltre inseriamo una breve descrizione per ricordarci “block telnet from kali to metasploitable”.



Una volta finito questo, salviamo e clicchiamo su apply changes, altrimenti le nostre modifiche non vanno a buon fine.

Adesso non ci resta che provare dal terminale.

Utilizziamo il comando telnet 192.168.1.16 per provare la connessione alla porta telnet da kali a metasploitable.

Se la nostra regola è andata a buon fine non dovrebbe riuscire la connessione:

```
francesco@kali: ~  
File Actions Edit View Help  
zsh: corrupt history file /home/francesco/.zsh_history  
(francesco@kali)~  
$ telnet 192.168.1.16  
Trying 192.168.1.16 ...  
telnet: Unable to connect to remote host: Network is unreachable  
(francesco@kali)~  
$
```

Come possiamo vedere la regola sembra essere stata impostata correttamente e quando proviamo a connetterci da kali alla porta 23 telnet di metasploitable, ci dice network unreachable e quindi la connessione viene bloccata.