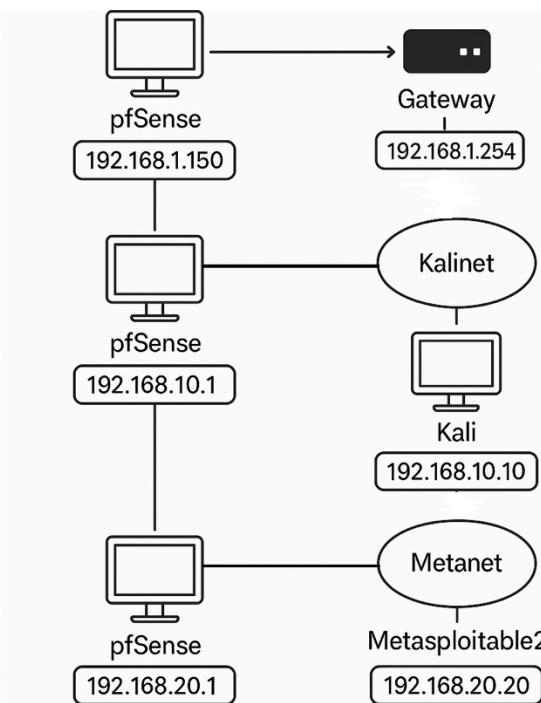


REPORT



L'esercizio richiede di creare una regola firewall che blocchi l'accesso alla DVWA di Metasploitable2 dalla macchina virtuale Kali Linux.

Per fare ciò, è necessario configurare la macchina virtuale pfSense su Virtual Box come nella figura affianco, ovvero:

- Dovrà avere l'interfaccia WAN nella rete locale del nostro gateway 192.168.1.254
- Una seconda scheda di rete configurata per fare da gateway a Kali Linux, in modo che il traffico diretto al di fuori della rete locale passi attraverso pfSense, che agirà come router firewall.

Per prima cosa, apro Virtual Box e seleziono la macchina virtuale di pfSense, che andrò a configurare come segue. Seleziono le impostazioni in modalità Esperto, in modo da poter accedere alle configurazioni avanzate di rete.

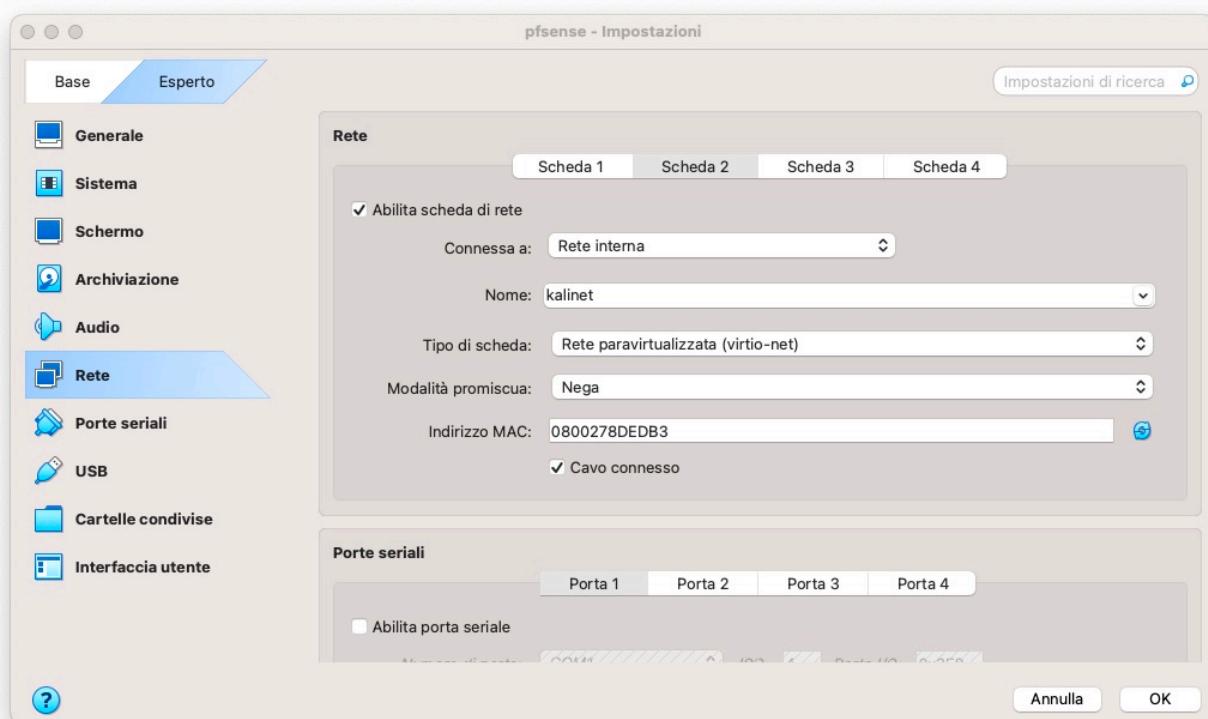
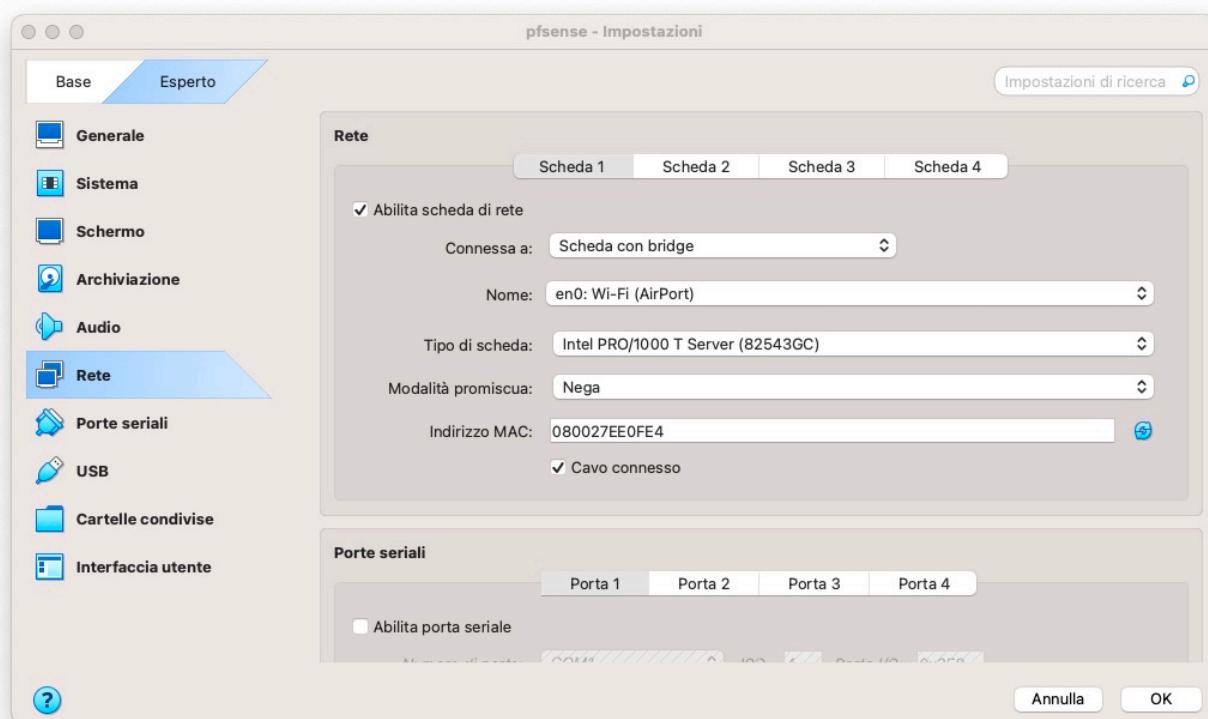
Nelle figure qui sotto si evince come andare a settare i parametri delle relative 3 schede di rete, che andranno attivate.

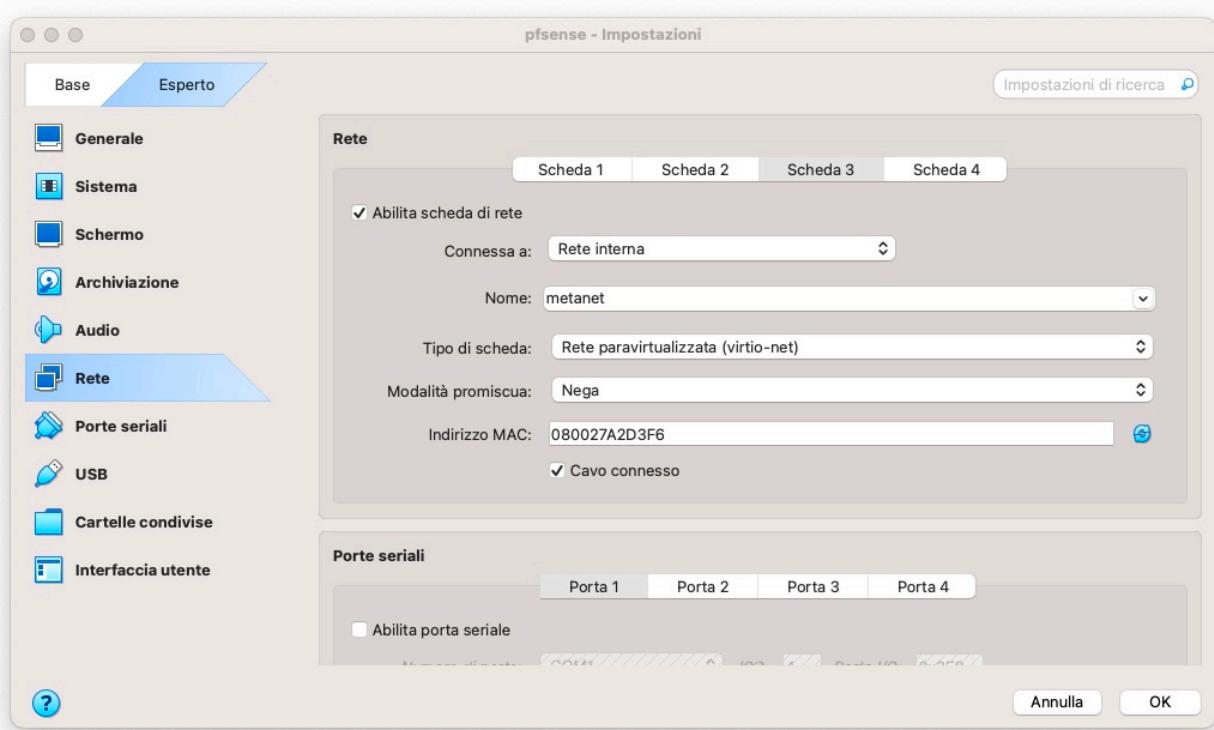
Prestare nota che la prima è stata settata come Bridge. La modalità scheda con **Bridge** (Bridged Adapter) permette alla VM di collegarsi direttamente alla rete locale tramite una scheda di rete virtuale che fa da ponte con una scheda di rete fisica del computer ospite. In questa modalità, la VM ottiene un indirizzo IP dalla stessa sottorete della rete locale, come se fosse un altro computer fisico.

Le schede di rete 2 e 3, invece, sono state configurate come rete interna. La modalità **rete interna** (Internal Network) permette alla VM di collegarsi a una rete virtuale interna creata da Virtual Box. In questa modalità, la VM ottiene un indirizzo IP da una sottorete interna definita dall'utente. La VM può comunicare solo con altre VM collegate alla stessa rete interna. Questa modalità **isola** la VM dalla rete locale e da internet, creando una rete virtuale privata tra le VM.

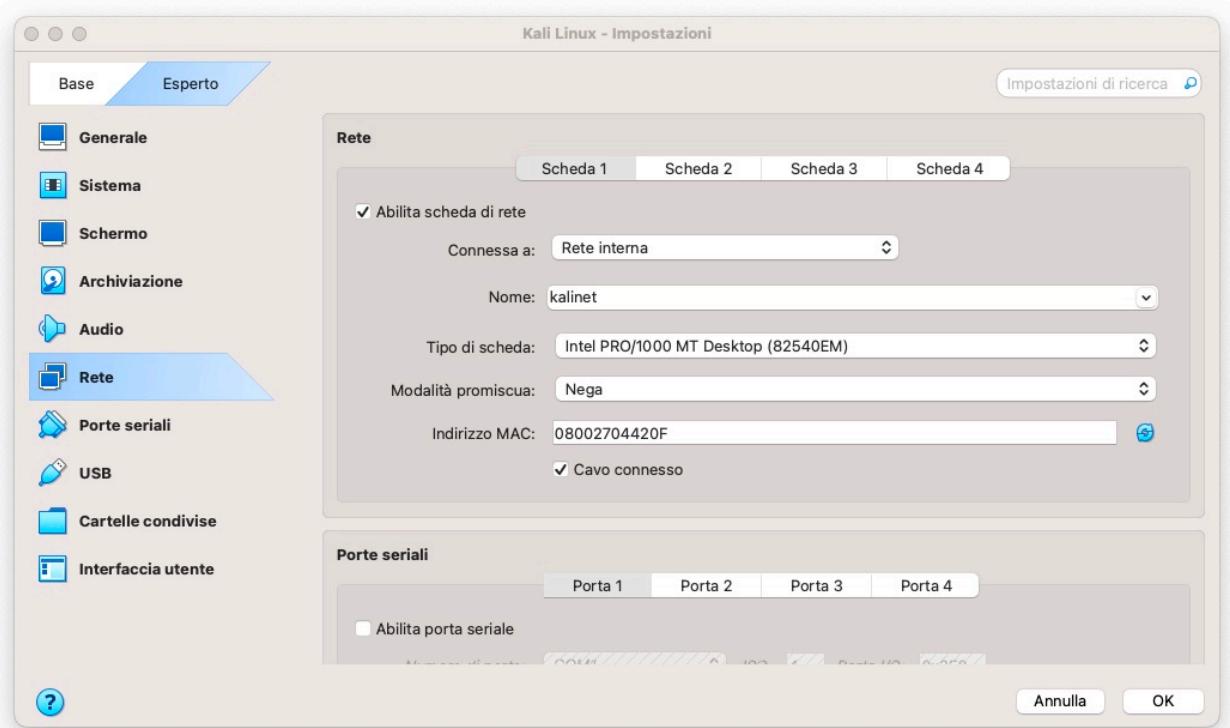
Da notare, anche, che la seconda scheda di rete della VM pfsense che andrà connessa alla VM di Kali Linux è stata impostata con nome di rete **kalinet** (scelto casualmente), che andrà impostato parimenti nelle impostazioni della scheda di rete della VM di Kali Linux come vedremo in seguito.

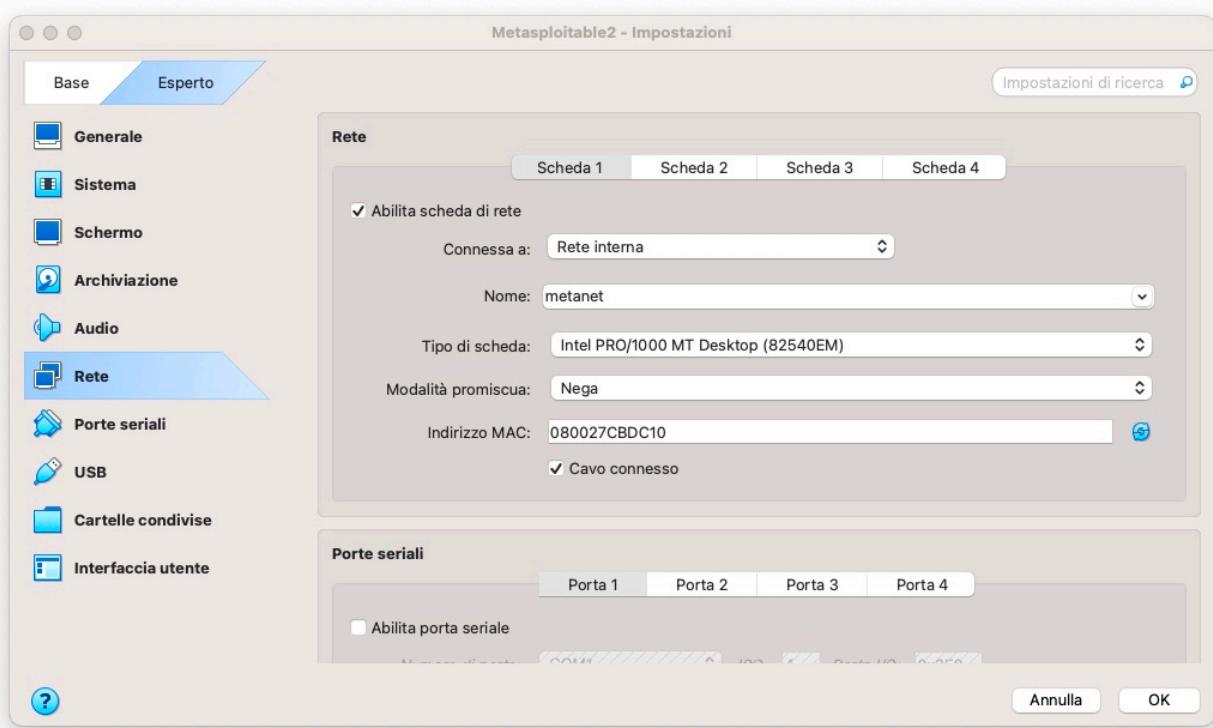
Lo stesso è stato fatto relativamente alla terza scheda di rete della VM di pfsense, con la differenza, ovviamente, di assegnarle un ulteriore nome (in questo caso ho scelto **metanet**), anch'esso da riportare parimenti nelle impostazioni di rete della VM di Metasploitable2.





Mostro qui sotto, rispettivamente, le impostazioni di rete da inserire per la VM di Kali Linux e per la VM di Metasploitable2.





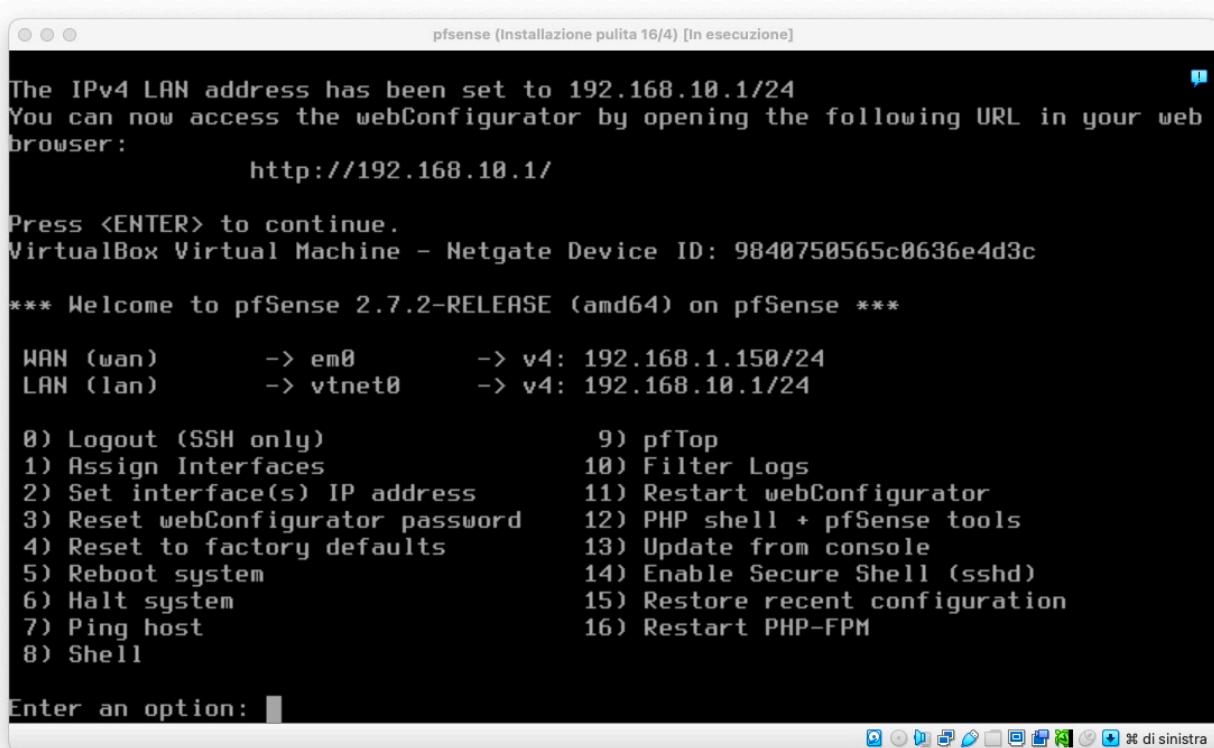
Una volta eseguite queste configurazioni di base, passo ad aprire la VM di pfSense, per procedere a configurare le schede di rete che abbiamo impostato sulla Virtual Box.

Come si può vedere dalla figura qui sotto, al momento la terza interfaccia di rete non è ancora visibile: andrà configurata successivamente.

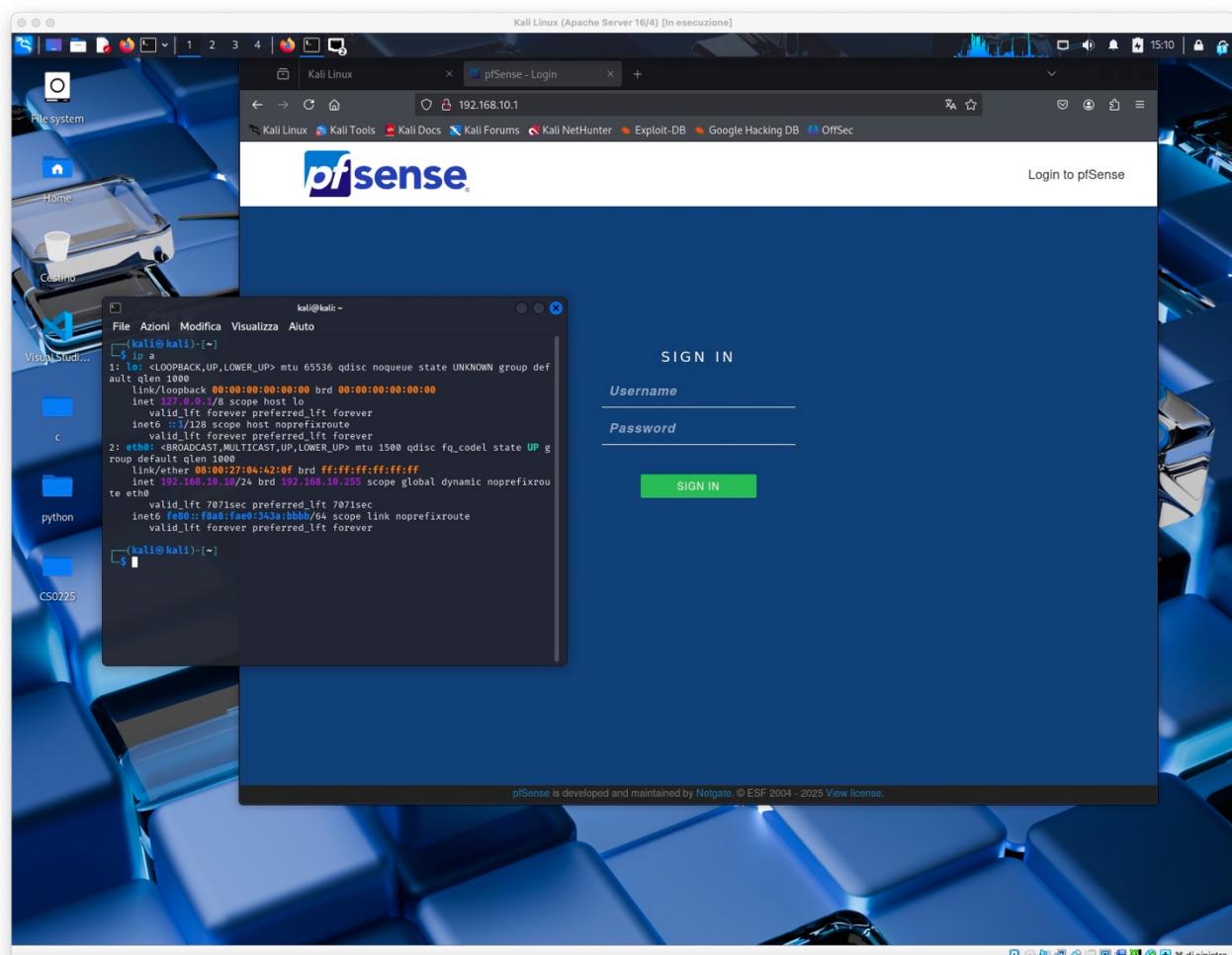
Cliccando sull'opzione 2, proseguo a configurare l'interfaccia WAN. Imposto come gateway predefinito il router 192.168.1.254 e, avendo abilitato sul router il server DHCP, ho scelto DHCP. Dallo screenshot si vede che il server DHCP del router ha assegnato, correttamente, un IP della sua subnet, ovvero 192.168.1.150.

Poi procedo a configurare, sempre con l'opzione 2, la rete LAN. Poiché desidero che questa interfaccia abbia un indirizzo IP statico 192.168.10.1, in modo che possa fungere da gateway per la VM di Kali, scelgo indirizzo statico e lo digito, specificando il CIDR 24.

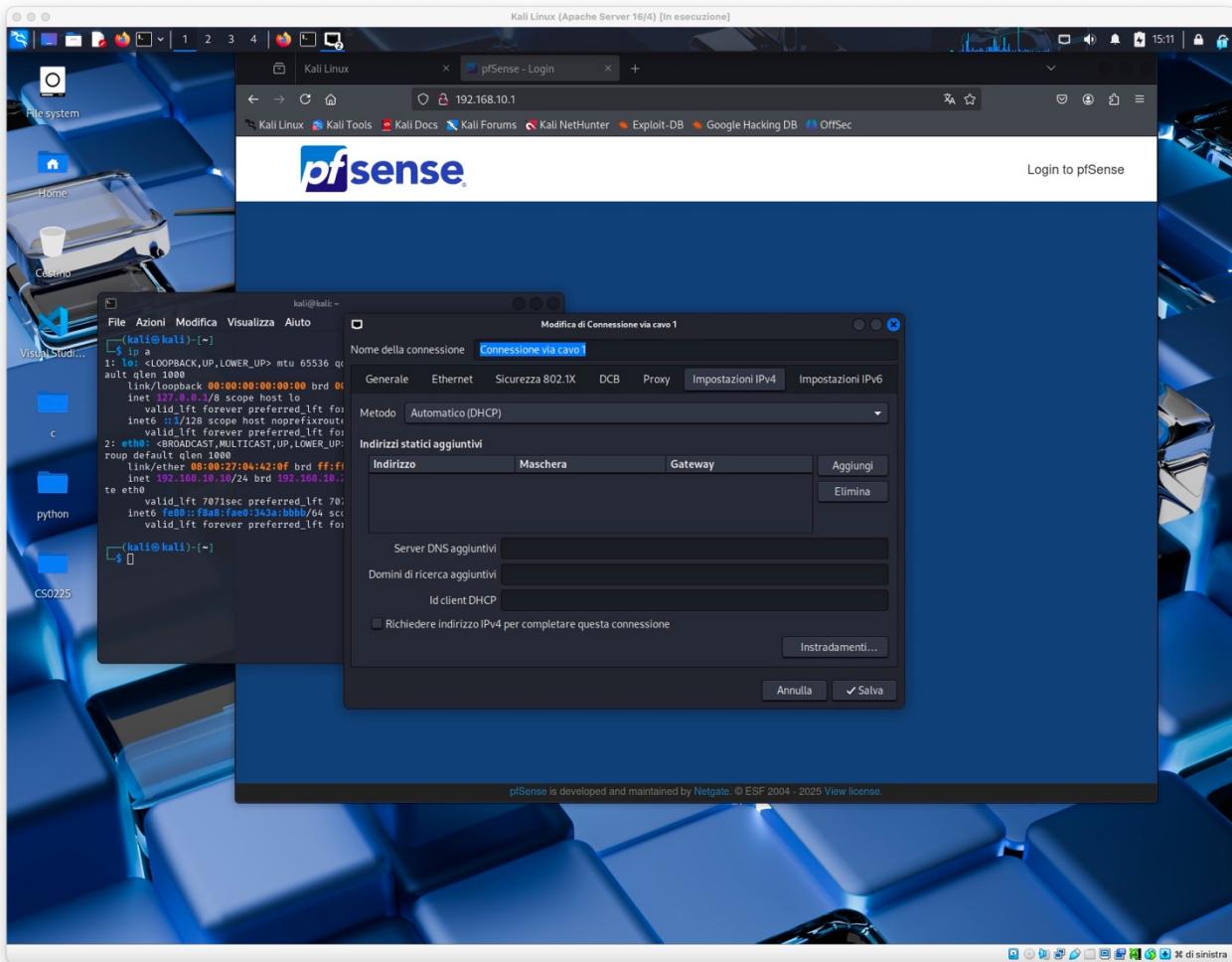
Non sono interessato all'IPv6, quindi scelgo no. Infine abilito il server DHCP per questa interfaccia, in modo che possa assegnare dinamicamente gli indirizzi IP ai computer connessi a questa rete interna (in questo caso la VM di Kali) dall'indirizzo IP 192.168.10.10 al 192.168.10.100. Qui sotto lo screenshot dopo questa configurazione.



Ora apro la VM di Kali. Vado a verificare che gli sia stato assegnato dal DHCP della pfsense un IP nella corretta subnet così come configurato pocanzi. Apro anche il browser per verificare che la pagina di gestione di pfsense sia raggiungibile all'indirizzo impostato 192.168.10.1.



Tutto funziona come previsto. A Kali Linux è stato assegnato dal DHCP della pfSense il primo indirizzo utile del range impostato 192.168.10.10.apro anche le impostazioni di rete di Kali per verificare che sia tutto correttamente impostato in DHCP.



Tutto funziona a dovere. Effettuo il login della pfSense, quindi entro nella scheda Interfaces ed abilito la terza scheda di rete chiamata OPT1. All'interno, alla voce IPv4 inserisco l'IP – 192.168.20.1 - che desidero assegnare all'interfaccia di rete di pfSense che fungerà da gateway per la VM di Metasploitable2 (in modo che poi sia anche visualizzata nella pfSense nella CLI). Seleziono nel menu a tendina il CIDR desiderato 24. Tecnicamente, questa operazione può essere fatta direttamente nella CLI già una volta attivata l'interfaccia.

Ora passo alla VM della pfSense. Visualizzo anche la terza scheda di rete, che ora posso configurare nel dettaglio.

Seleziono sempre l'opzione 2, quindi confermo la mia scelta a non volere l'indirizzo della scheda di rete di pfSense in DHCP in quanto dovrà fungere da gateway e serve statico. Quindi inserisco nuovamente 192.168.20.1 come indirizzo statico della stessa. Mi viene chiesto se desidero usare IPv6, scelgo no. Quindi, se desidero attivare il server DHCP per i computer collegati a questa subnet, scelgo sì, e come range imposto dal 192.168.20.20 al 192.168.20.100. Qui di seguito lo screenshot eseguito dopo questa configurazione.

```
pfSense (Installazione pulita 16/4) [In esecuzione]
The IPv4 OPT1 address has been set to 192.168.20.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
http://192.168.20.1/

Press <ENTER> to continue.
VirtualBox Virtual Machine - Netgate Device ID: 9840750565c0636e4d3c

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4: 192.168.1.150/24
LAN (lan)      -> vtne0     -> v4: 192.168.10.1/24
OPT1 (opt1)    -> vtne1     -> v4: 192.168.20.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults 13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                15) Restore recent configuration
7) Ping host                  16) Restart PHP-FPM
8) Shell

Enter an option: █
```



Tutto funziona a dovere. Quindi proseguo ad aprire la VM di Metasploitable2. Una volta aperta, con il comando ip a verifico l'indirizzo IP della VM. Dalla figura qui sotto, risulta correttamente assegnato dal DHCP della pfsense appena configurato il primo indirizzo IP utile del range, ovvero 192.168.20.20 .

```
Metasploitable2 (Installazione pulita 30/3) [In esecuzione]
Last login: Thu Apr 10 08:21:22 EDT 2025 on ttym1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

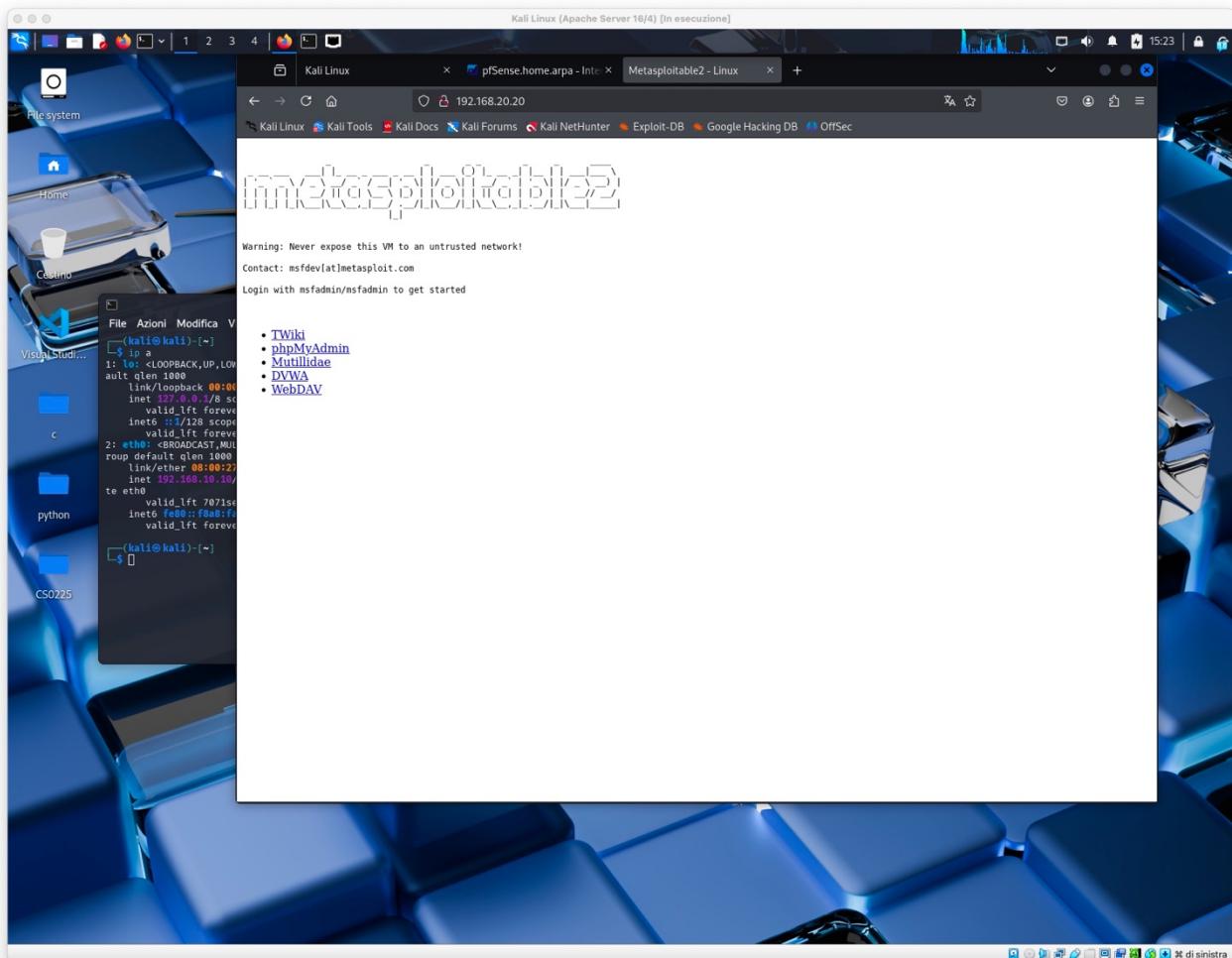
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.

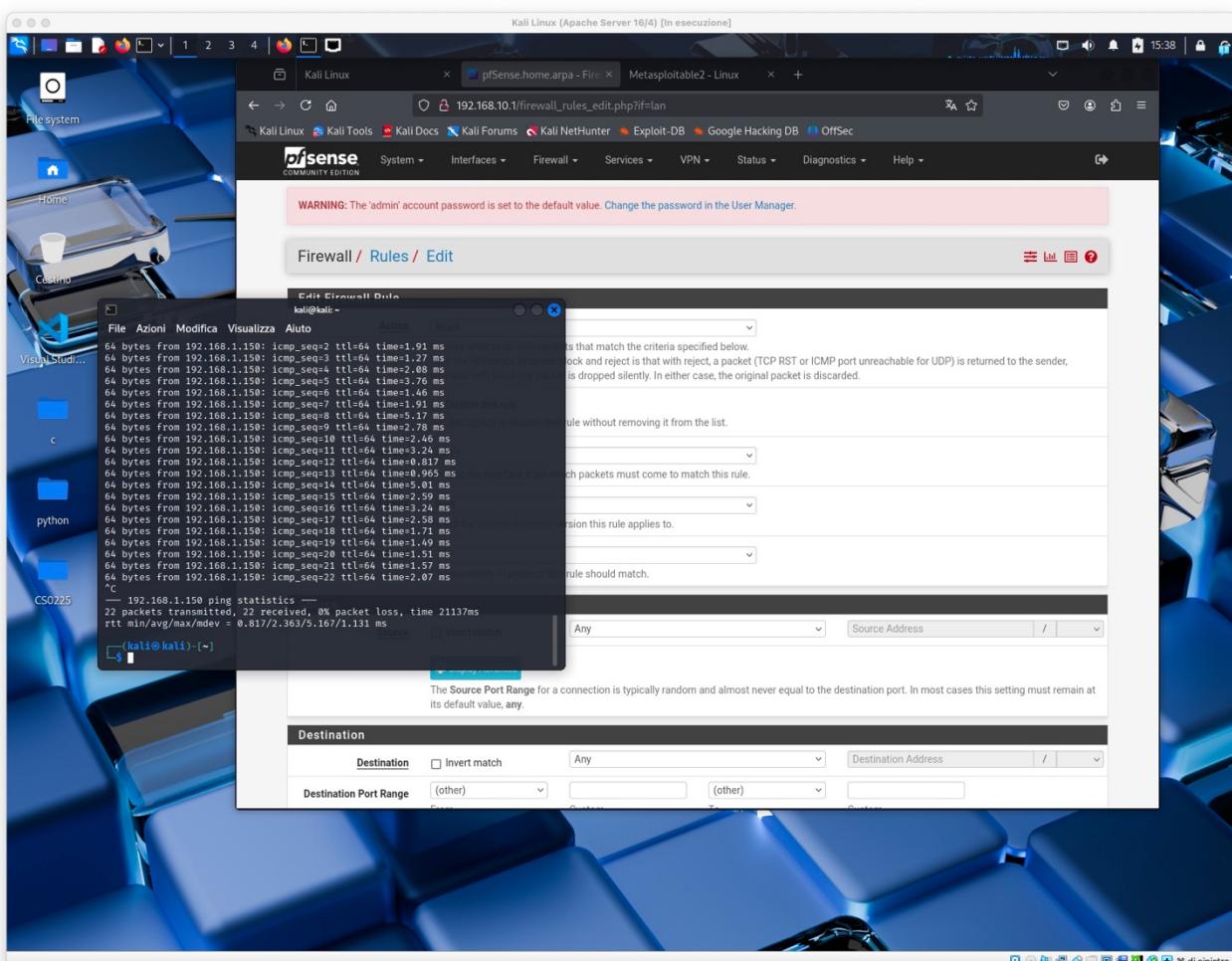
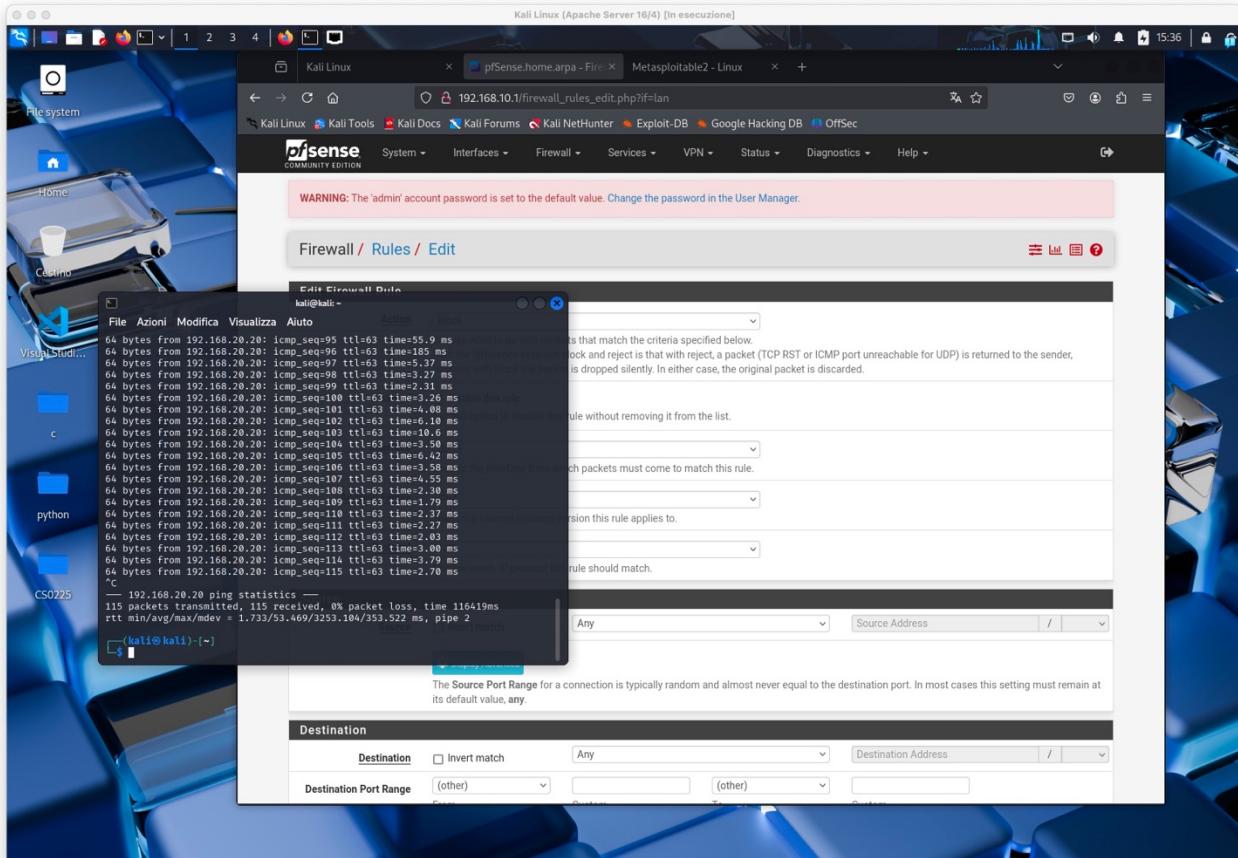
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:cb:dc:10 brd ff:ff:ff:ff:ff:ff
    inet 192.168.20.20/24 brd 192.168.20.255 scope global eth0
        inet6 fe80::a00:27ff:fecb:dc10/64 scope link
            valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ _
```



Da Kali, usando il browser, proviamo a collegarci alla DVWA di Metasploitable, puntandolo all'indirizzo IP della stessa 192.168.20.20 . Tutto funziona, come si vede nello screenshot qui sotto.



Per ulteriore conferma, provo ad effettuare un ping da Kali a Metasploitable2, e da Kali alla pfSense. Rispettivamente, qui sotto i relativi screenshot.

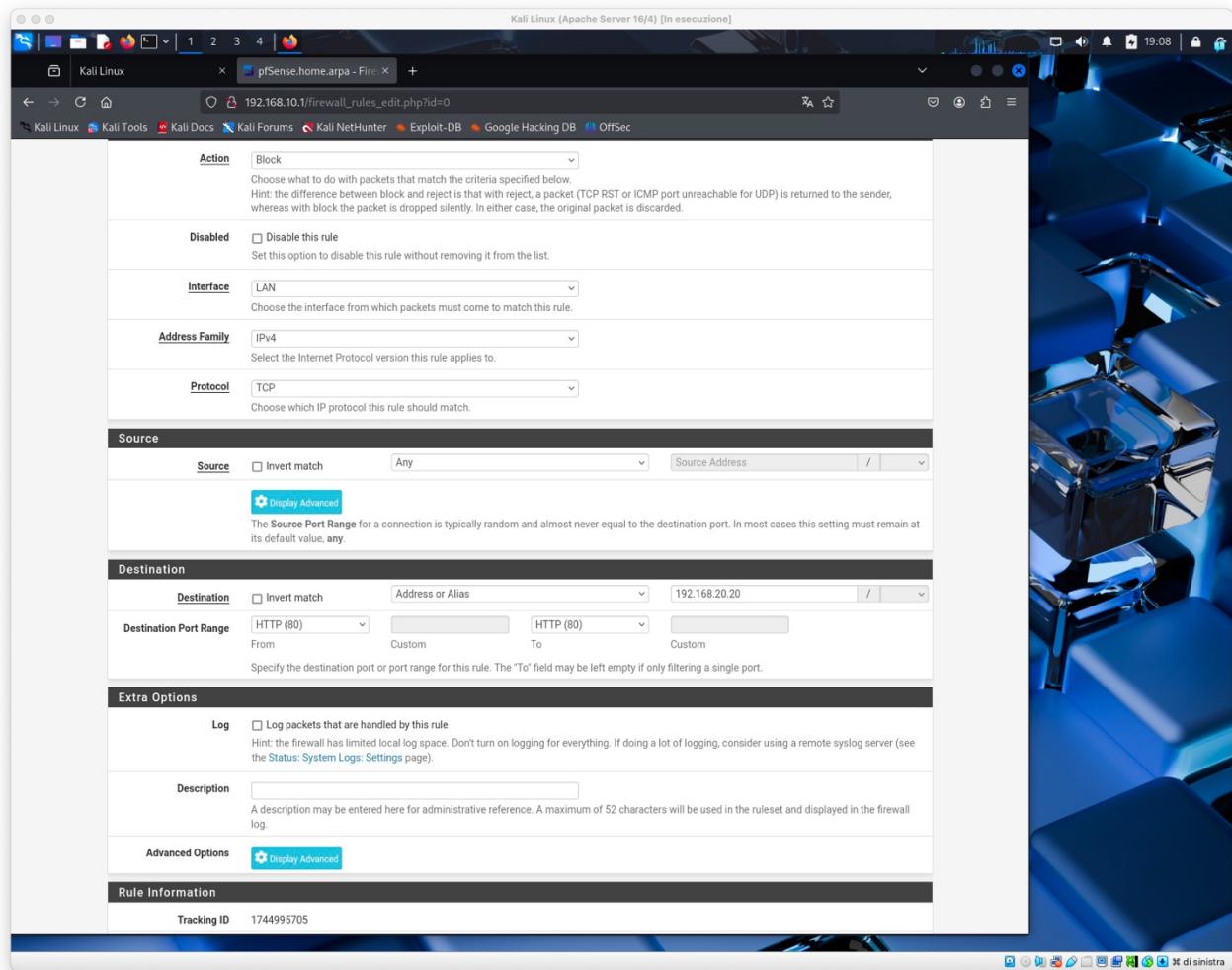


Ora passo a configurare le regole.

Dalla GUI di pfsense in Kali, tramite il browser, seleziono Firewall e poi Rules. Quindi seleziono la scheda LAN. Clicco su Add con freccia in su, perché è una regola di blocco a cui voglio attribuire priorità sul resto delle regole, e procedo alla configurazione.

Imposto come tipologia di regola il valore Block. Lascio indirizzo IPv4, su Interfaccia da cui voglio che i pacchetti vengano filtrati seleziono LAN, seleziono quindi TCP come protocollo in quanto la DVWA di Metasploitable utilizza http su porta 80 che rientra in quest'ultimo.

Alla sezione Destination, seleziono Address or Alias, e inserisco l'IP 192.168.20.20 che corrisponde alla DVWA, quindi la porta 80. Salvo tutto. Qui sotto lo screenshot.



Allego qui sotto anche i 3 screenshot di come appaiono, adesso, le pagine relative alla configurazione delle regole per WAN, LAN e OPT1.

Kali Linux (Apache Server 10/4) [In esecuzione]

Kali Linux pfSense.home.apra - Fire 192.168.10.1/firewall_rules.php?f=lan

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

pfSense COMMUNITY EDITION

System Interfaces Firewall Services VPN Status Diagnostics Help

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Firewall / Rules / LAN

The firewall rule configuration has been changed.
The changes must be applied for them to take effect.

Apply Changes

Floating WAN LAN OPT1

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 1/1.11 MB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
✗ 0/0 B	IPv4 TCP	*	*	192.168.20.20	80 (HTTP)	*	none			
✓ 0/0 B	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
✓ 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add Add Delete Toggle Copy Save Separator

pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 View license.



Kali Linux pfSense.home.apra - Fire 192.168.10.1/firewall_rules.php?f=wlan

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

pfSense COMMUNITY EDITION

System Interfaces Firewall Services VPN Status Diagnostics Help

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Firewall / Rules / WAN

Floating WAN LAN OPT1

Rules (Drag to Change Order)

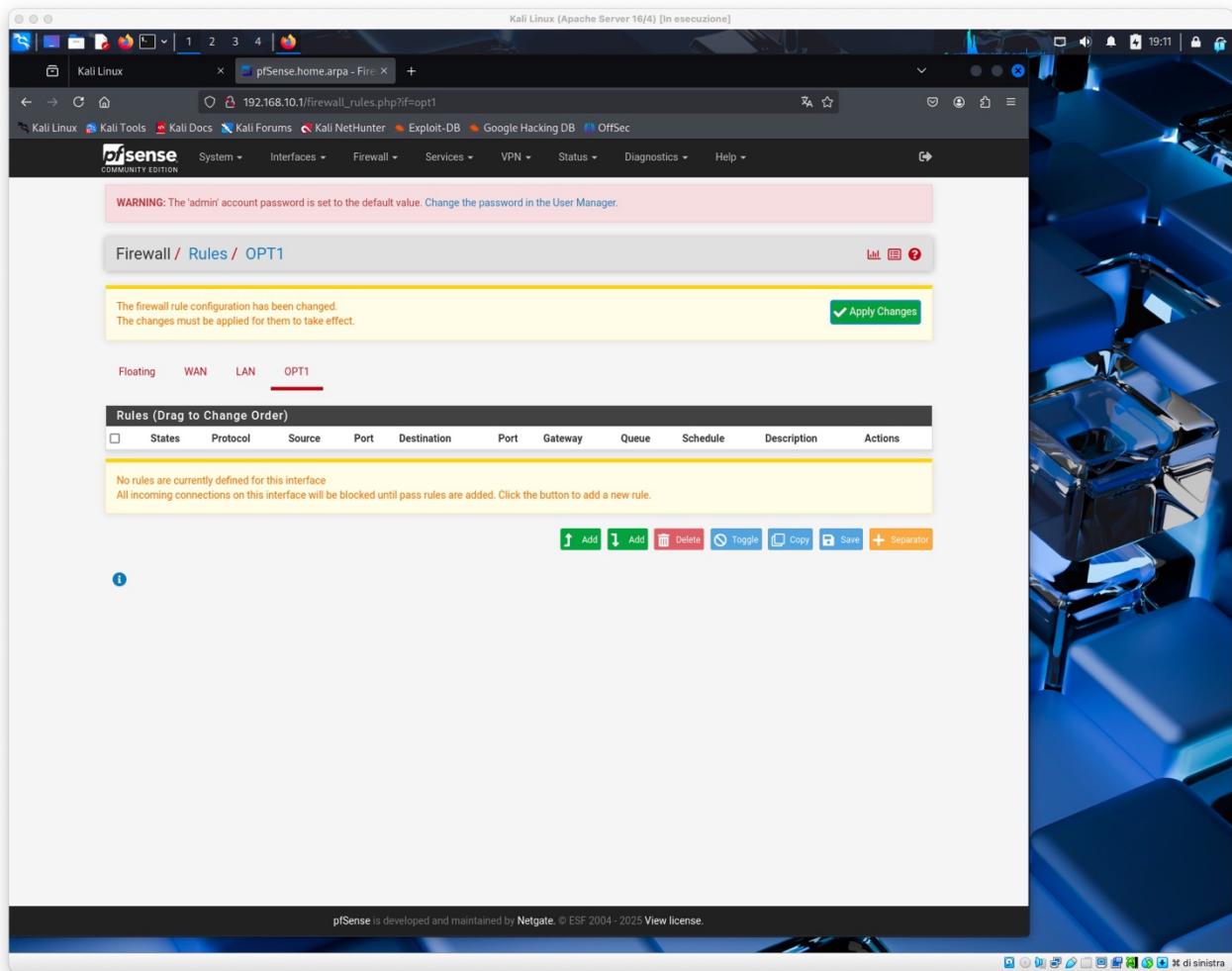
States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✗ 0/10 KB	*	Reserved Not assigned by IANA	*	*	*	*	*	*	Block bogon networks	

No rules are currently defined for this interface.
All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.

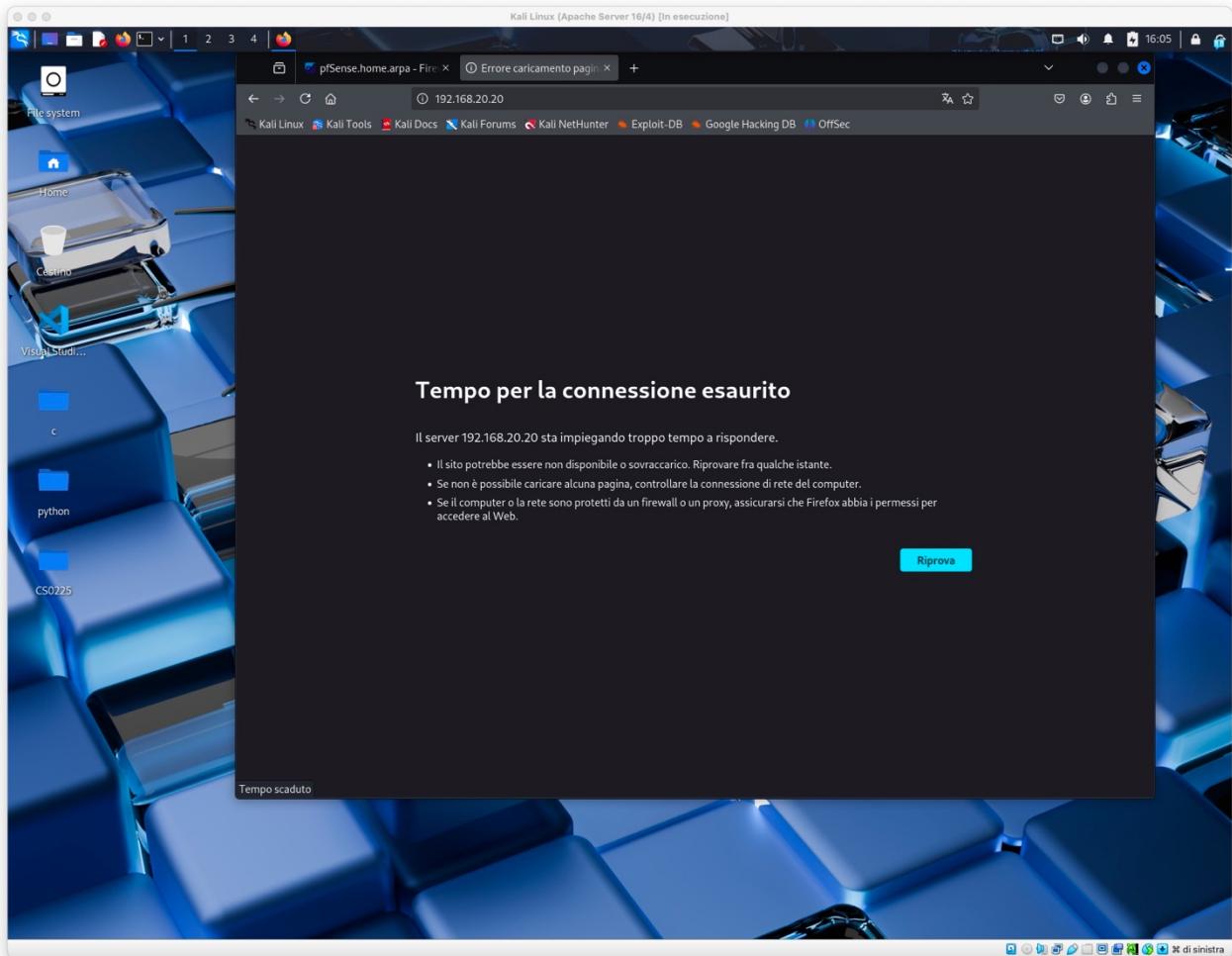
Add Add Delete Toggle Copy Save Separator

pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 View license.





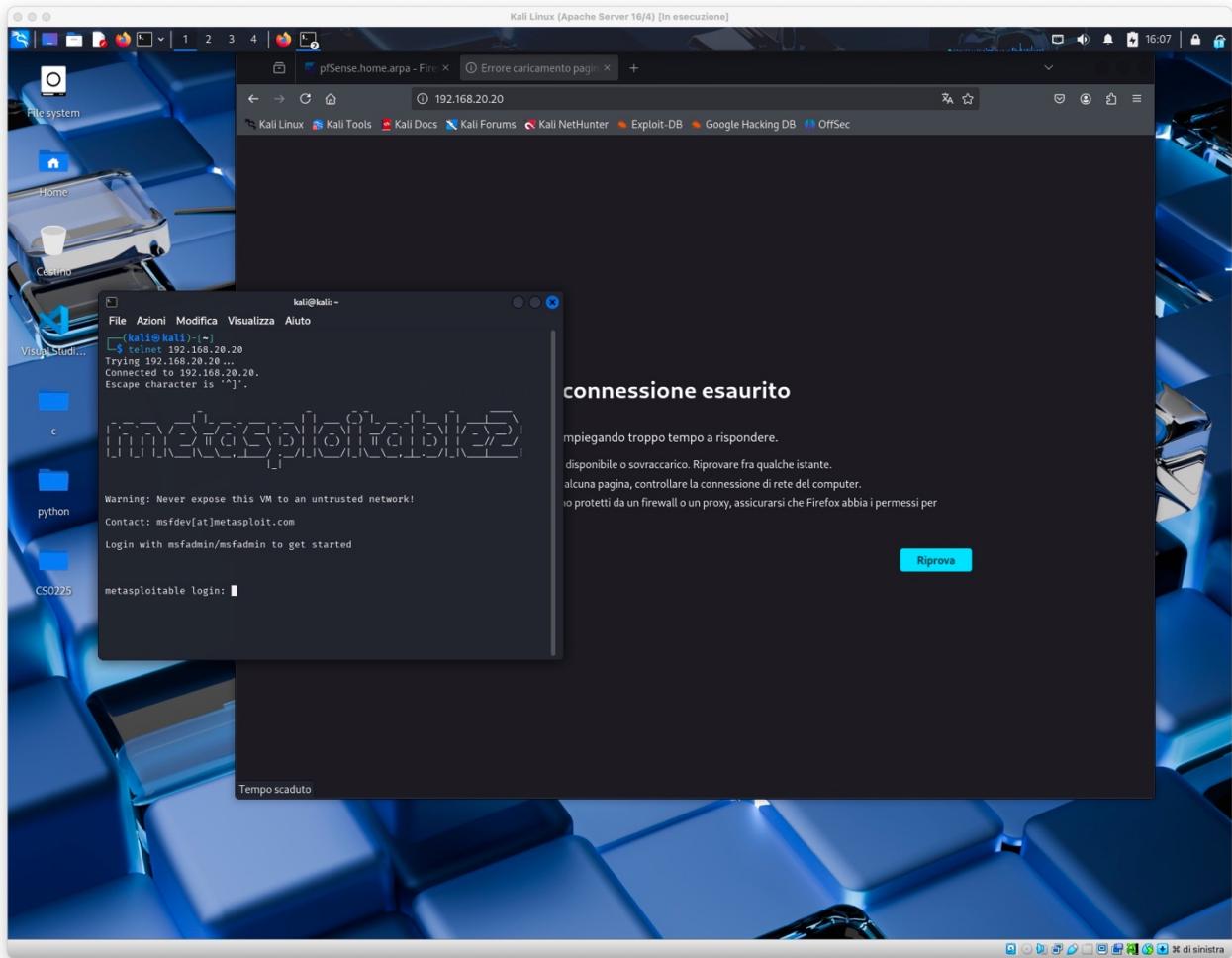
Vado a verificare che Kali non si connette a Metasploitable2 tramite il browser, puntando sempre su 192.168.20.20. La DVWA, come si vede nello screenshot qui sotto, non si connette.



ESERCIZIO BONUS

L'esercizio bonus chiede di bloccare il traffico Telnet da Kali a Metasploitable2.

Come prima cosa, verifico che attualmente, senza regole, il protocollo Telnet funzioni e scambi dati. Per fare questa prova, apro il terminale di Kali e digito il comando telnet 192.168.20.20. La connessione è OK, come riportato dallo screenshot qui sotto.

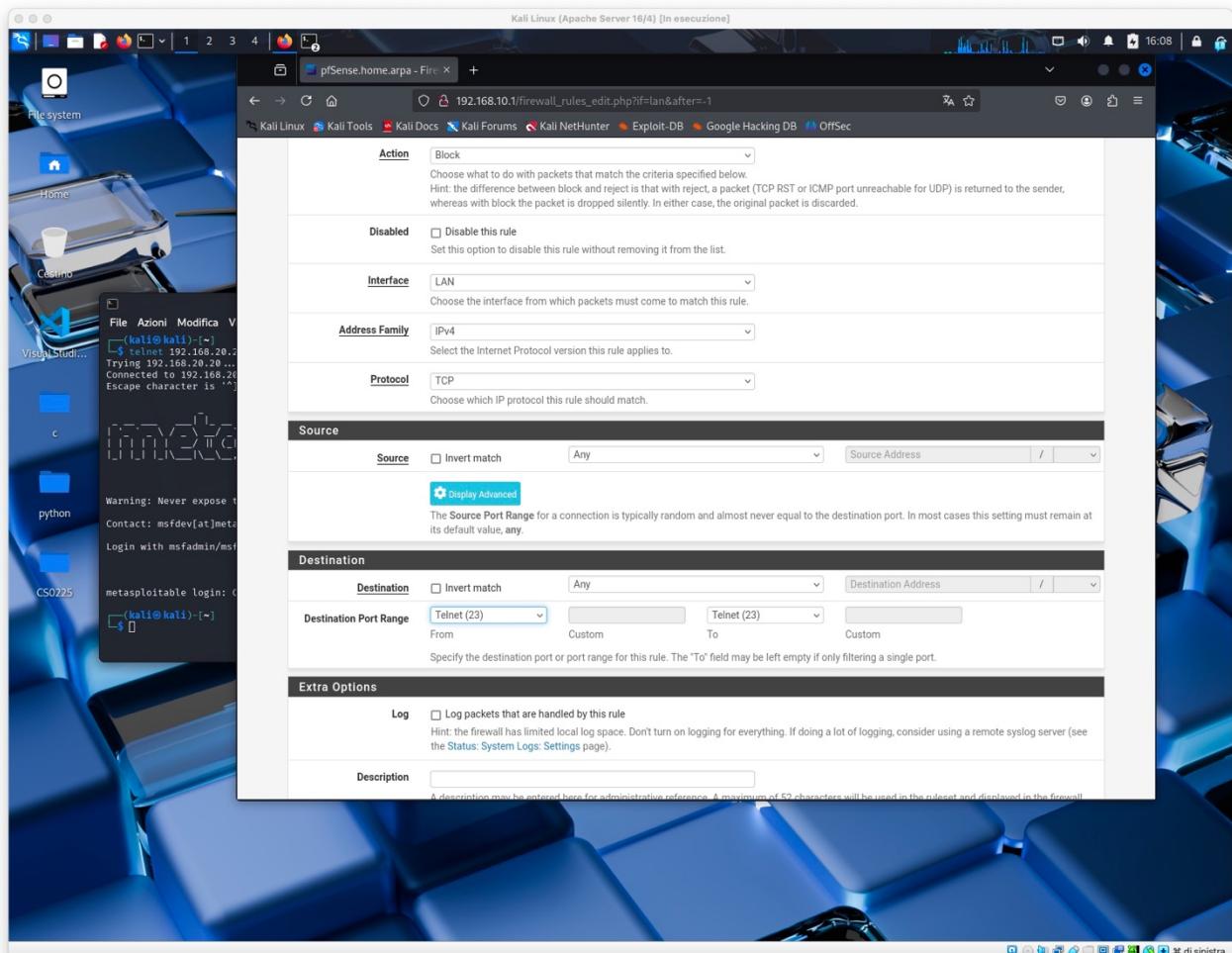


Ora riapro la GUI di pfSense su Kali tramite il browser, e vado ad impostare la regola.

Come Action seleziono Block, come interfaccia lascio LAN in quanto si tratta sempre di bloccare Kali che è su questa scheda di rete, lascio IPv4 come tipologia di IP e seleziono TCP come protocollo in quanto Telnet ne fa parte.

Nella sezione Destination, clicco su Telnet, che occupa la porta 23. Come Address or Alias inserisco l'indirizzo della DVWA, ovvero 192.168.20.20. Procedo, quindi, a salvare il tutto.

Qui sotto lo screenshot della regola impostata.



Usando il Terminale, eseguo nuovamente il comando telnet 192.168.20.20. Come si vede dallo screenshot qui sotto, adesso il traffico Telnet non è più funzionante.

