U1W3 - Progetto

Creazione di una regola firewall

Richieste:

- creare una regola firewall che blocchi l'accesso alla DVWA (su metasploitable) dalla macchina Kali Linux e ne impedisca di conseguenza lo scan

Procedimento:

Ho anzitutto provveduto a configurare le schede di rete delle varie macchine da Virtual Box.

Per la *PFSense* ho configurato da rete, modalità esperti, tre schede di rete: la prima in *bridged*, la seconda e la terza in *rete interna*, nominate rispettivamente ***kalinet*** e ***metanet***.

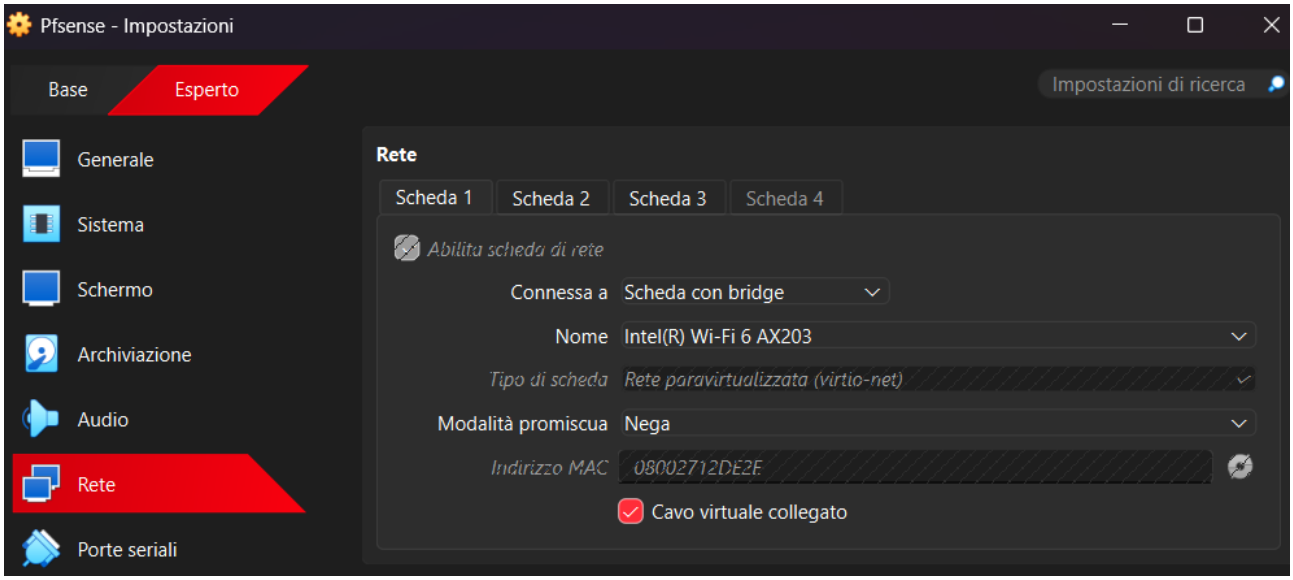

Figura 1 Scheda di rete 1 PFSense, scheda con bridge

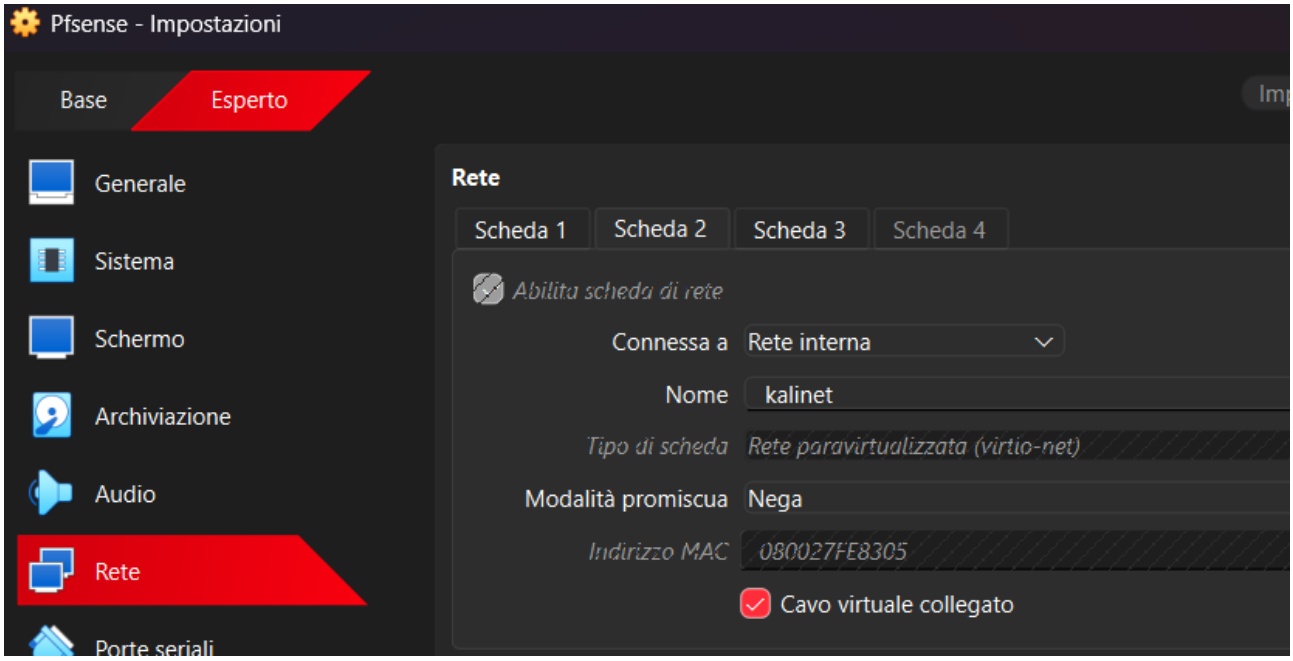

Figura 2 Scheda di rete 2 PFSense, rete interna kalinet

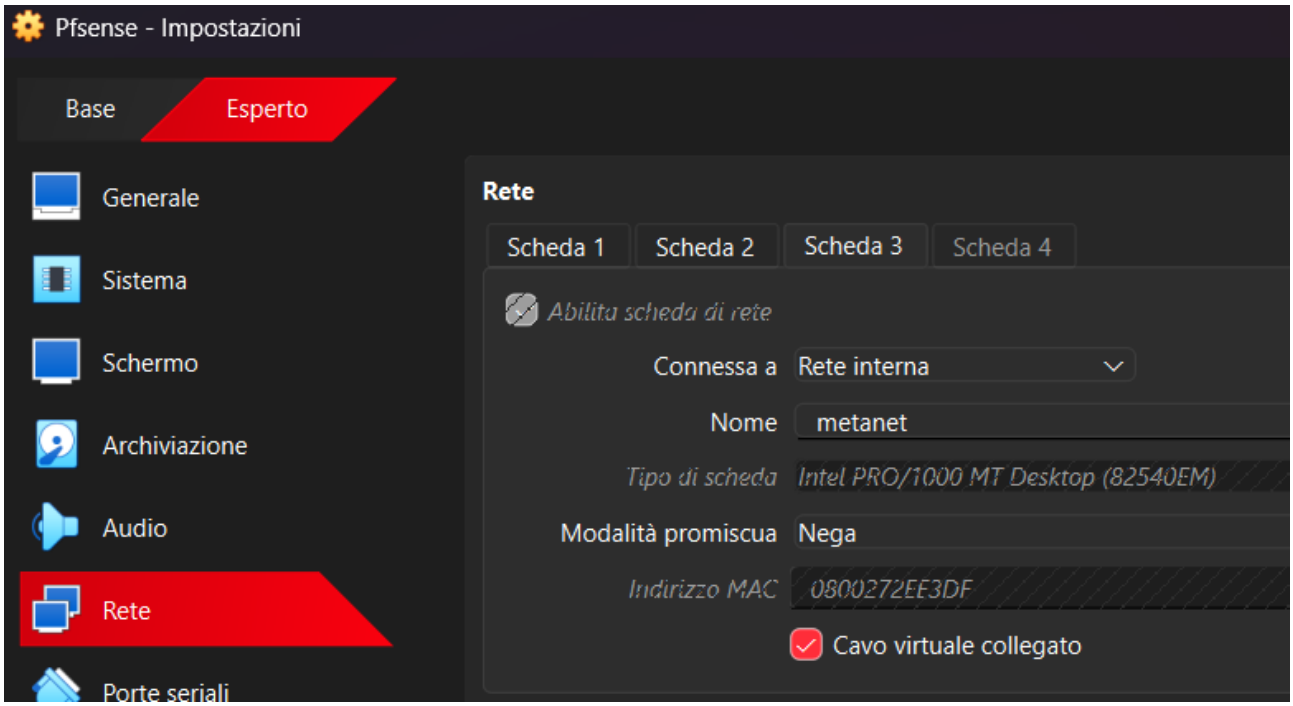

Figura 3 Scheda di rete 3 PFSense, rete interna metanet

Ho configurato poi le *schede di rete* della Kali e della Metasploitable, andando a settarle entrambe come **interne** e usando i **medesimi nomi** dati alle reti interne della PFSense: kalinet per la Kali, metanet per Metasploitable.

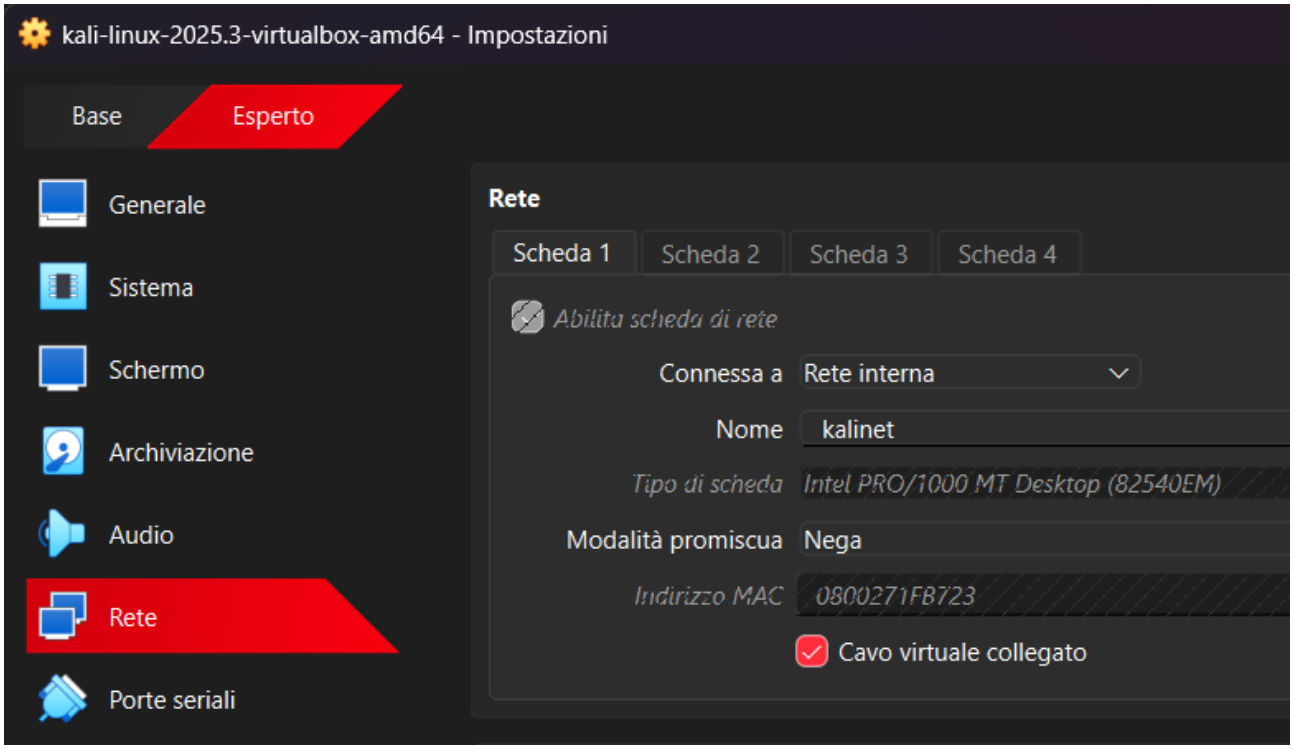

Figura 4 Scheda di rete 1 Kali, rete interna kalinet

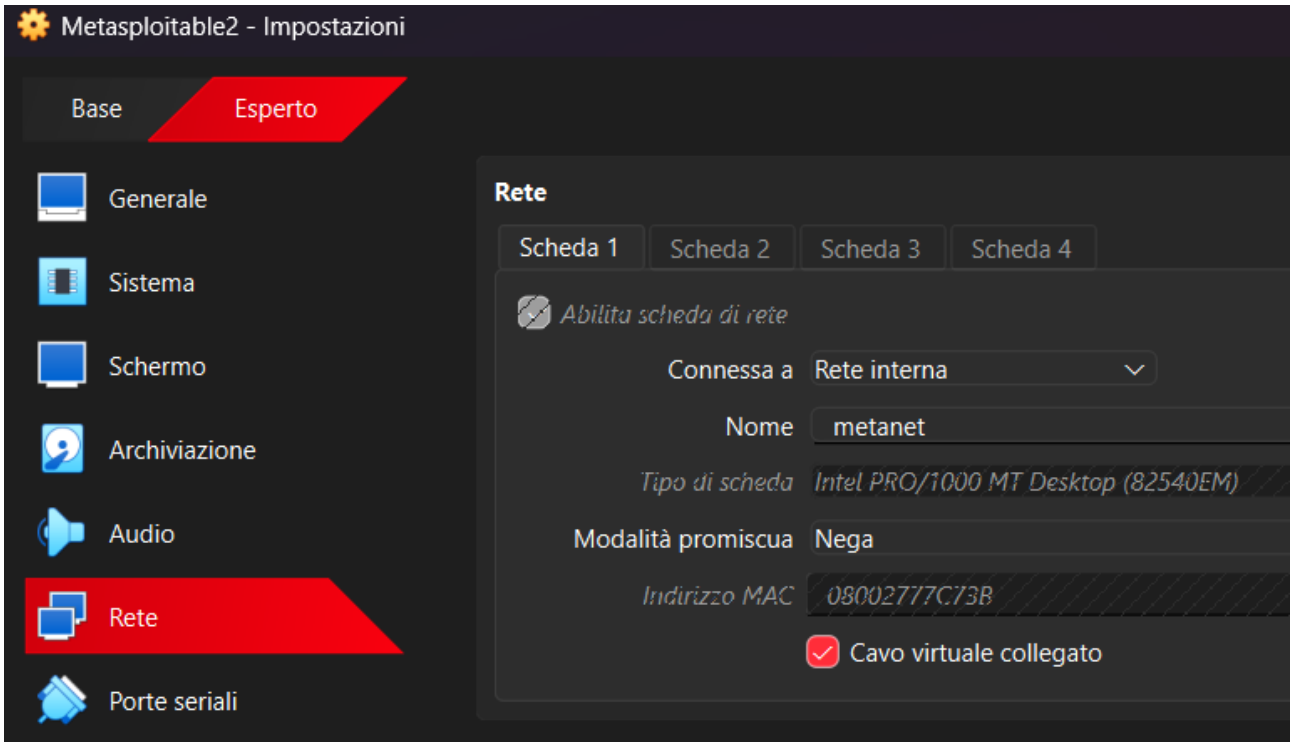

Figura 5 Scheda di rete 1 Metasploitable2, rete interna metanet

Una volta terminata questa configurazione, ho provveduto ad avviare tutte e tre le *VMs*, per poi concentrarmi sulla configurazione delle *interfacce* tramite *PFSense*.
Da *PFSense* ho configurato le *interfacce* delle prime due schede di rete: WAN e LAN.

Dal menù della *PFSense*, ho selezionato infatti **l'opzione 2**: *Set Interface(s) IP Address.*

E ho selezionato per prima **l'interfaccia 1**, quella collegata alla *WAN*.

Ho deciso di configurare *l'IPv4* attraverso il *DHCP*, mentre ho saltato la configurazione dell'*IPv6*.

```
 1) Assign Interfaces                10) Filter Logs
 2) Set interface(s) IP address      11) Restart webConfi
 3) Reset webConfigurator password   12) PHP shell + pfSe
 4) Reset to factory defaults        13) Update from cons
 5) Reboot system                    14) Enable Secure Sh
 6) Halt system                      15) Restore recent c
 7) Ping host                        16) Restart PHP-FPM
 8) Shell

Enter an option: 2

Available interfaces:

1 - WAN (vtnet0 - dhcp)
2 - LAN (vtnet1 - static)
3 - LAN2 (em0 - static)

Enter the number of the interface you wish to configure: 1

Configure IPv4 address WAN interface via DHCP? (y/n) y

Configure IPv6 address WAN interface via DHCP6? (y/n) n

Enter the new WAN IPv6 address.  Press <ENTER> for none:
>
```

Figura 6 Configurazione IP WAN, interfaccia 3 visibile in quanto già configurata

Ho proceduto con una configurazione simile per la *LAN*, ma andando a configurare un *IPv4 statico*, decidendo di assegnarvi l'IP di *gateway* 192.168.10.1 e selezionando il CIDR 24.

```
Enter an option: 2

Available interfaces:

1 - WAN (vtnet0 - dhcp)
2 - LAN (vtnet1)
3 - LAN2 (em0 - static)

Enter the number of the interface you wish to configure: 2

Configure IPv4 address LAN interface via DHCP? (y/n) n

Enter the new LAN IPv4 address.  Press <ENTER> for none:
> 192.168.10.1
```

Figura 7 Configurazione IP LAN (kalinet)

```
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address LAN interface via DHCP6? (y/n) n

Enter the new LAN IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 192.168.10.50
Enter the end address of the IPv4 client address range: 192.168.10.100
```

Figura 8 Configurazione subnet mask e servizio DHCP offerto con relativo range

Per quello che riguarda invece la scelta di **offrire** un ***servizio*** *DHCP*, ho deciso di **abilitarlo**, assegnando il *range* di IP da 192.168.10.50/24 a 192.168.10.100/24.

La terza interfaccia, da me chiamata LAN2, è stata configurata tramite la visualizzazione di *PFSense* da *browser* della *Kali*.

Dalla VM Kali, ho fatto l'accesso a PFSense tramite browser, puntando direttamente all'IP della PFSense dalla scheda di rete connessa in modalità bridged(192.168.1.16/24), e ho poi proceduto ad accedere a *Interfaces*, selezionando *Assignments*, e ho aggiunto un'interfaccia, denominata OPT1 di default.

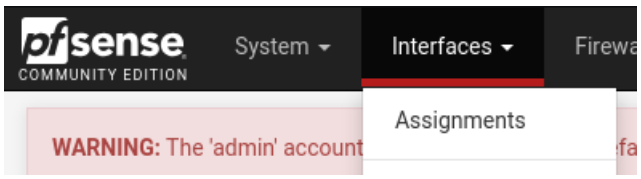

Figura 9 Accesso alla creazione e gestione delle interfacce

Una volta fatto l'accesso a *OPT1*, ho provveduto a rinominarla *LAN2*, ad **attivarla** e a **configurare** il suo *IP* e la sua *maschera di rete*, operazione che una volta abilitata l'interfaccia avrei potuto fare anche da **terminale** della *PFSense* stessa.

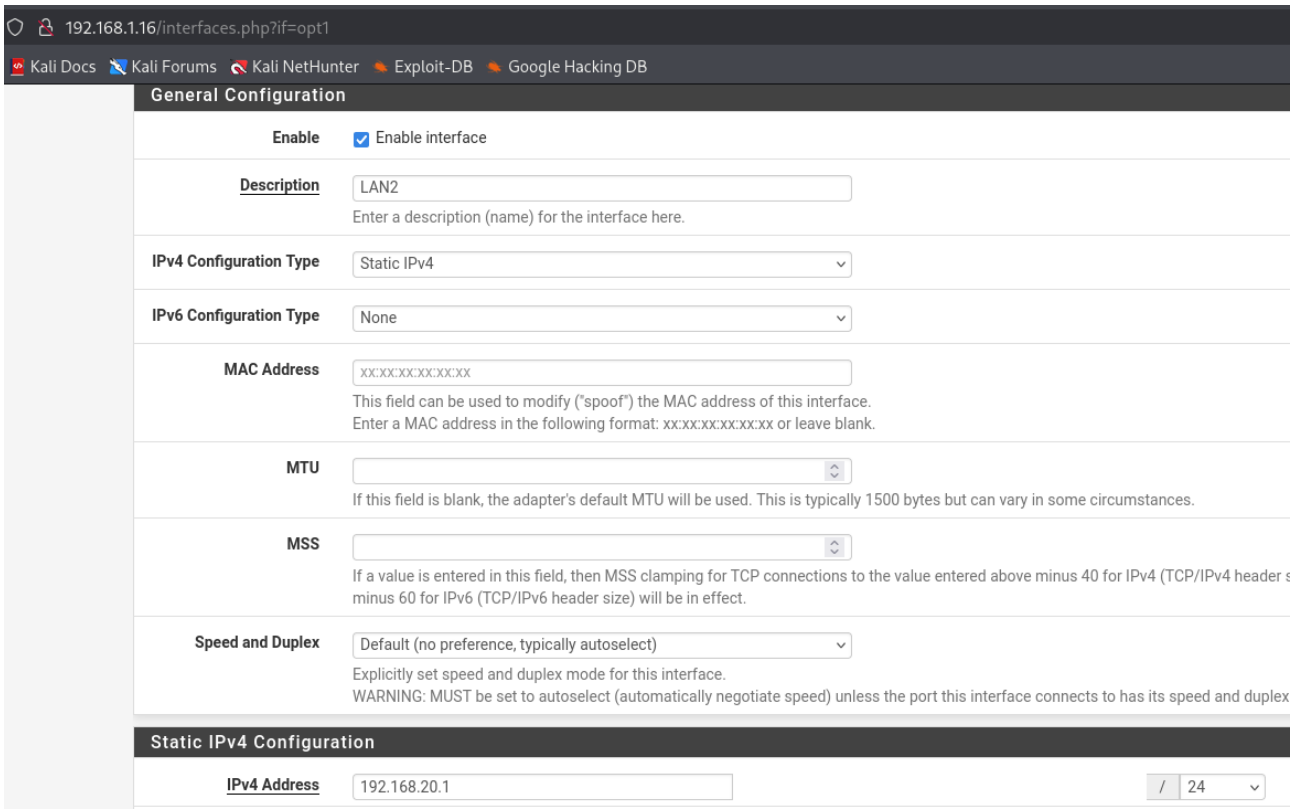

Figura 10 Configurazione LAN2 (metanet) da sito PFSense

Da *Services*, selezionando *DHCP Server*, sono entrata nel menù della LAN2.

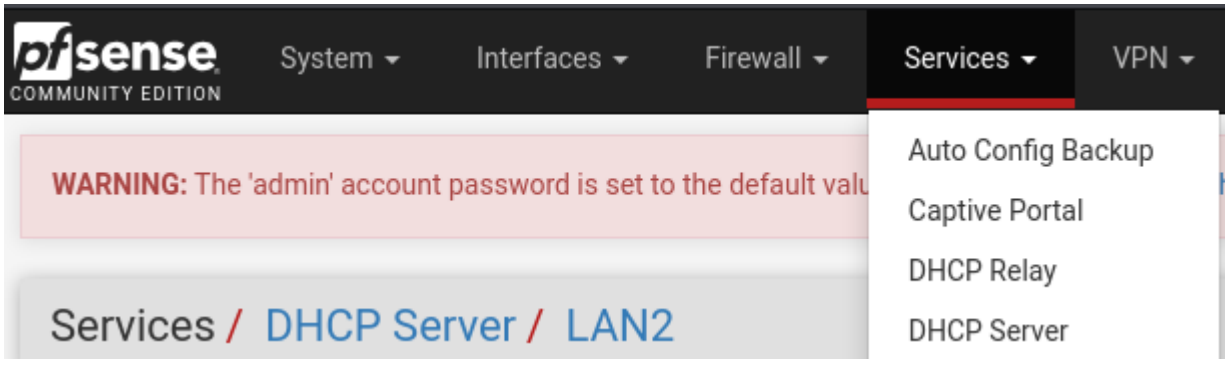

Figura 11 DHCP Service, abilitazione da PFSense su browser

E da qui sono andata ad abilitare il *servizio DHCP* per la rete locale "metanet".

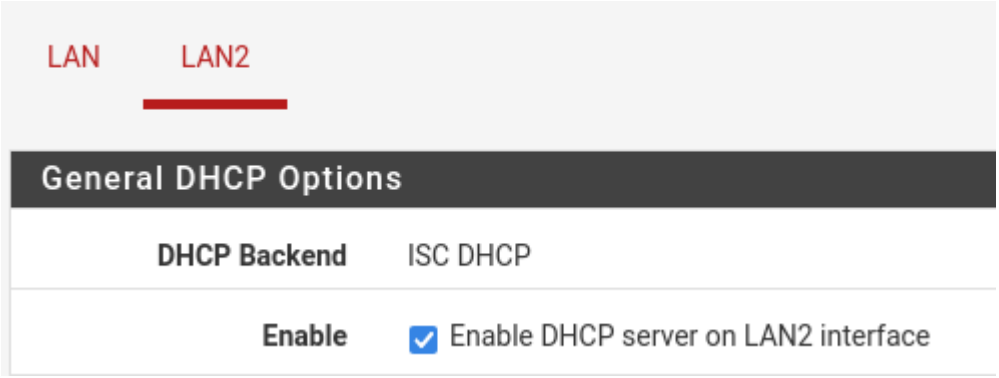

Figura 12 Attivazione DHCP per LAN2 da PFSense tramite browser

Una volta fatte queste configurazioni, ho controllato dalla *PFSense* le configurazioni delle tre *schede di rete* e degli *IP* ad esse associati.

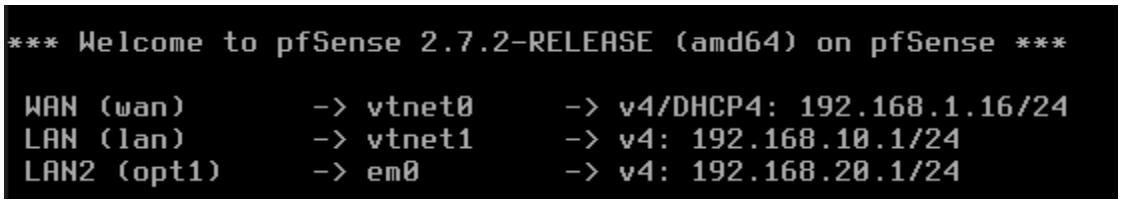

Figura 13 Tre schede di rete e IP associati

Una volta configurato il tutto in questo modo, ho proceduto a controllare le regole del *firewall* e se la pagina della *DVWA* sulla *Metasploitable* fosse visualizzabile dal *browser* della *Kali*.

Le regole applicate alla LAN (rete interna kalinet) sono quelle di *default*, il sito risulta raggiungibile tramite il *browser firefox* della *Kali*.

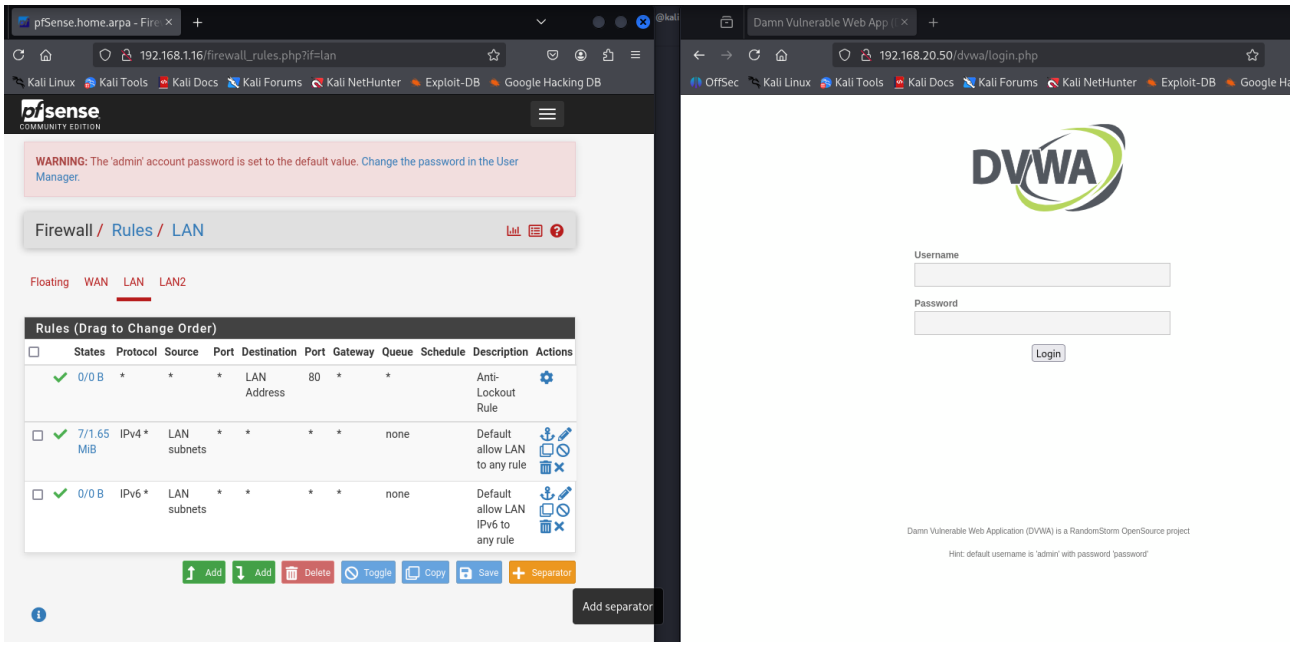

Figura 14 Accesso dalla Kali al sito DVWA sulla metasploitable, visione delle regole applicate sulla kalinet

Sempre con le regole settate in quel modo, ho controllato che la Kali fosse in grado di *pingare* sia il *gateway* che *l'indirizzo IP* specifico della *Metasploitable2*.

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.20.50
PING 192.168.20.50 (192.168.20.50) 56(84) bytes of data.
64 bytes from 192.168.20.50: icmp_seq=1 ttl=63 time=4.92 ms
64 bytes from 192.168.20.50: icmp_seq=2 ttl=63 time=3.74 ms
^C
── 192.168.20.50 ping statistics ──
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 3.736/4.327/4.918/0.591 ms

┌──(kali㉿kali)-[~]
└─$ ping 192.168.20.1
PING 192.168.20.1 (192.168.20.1) 56(84) bytes of data.
64 bytes from 192.168.20.1: icmp_seq=1 ttl=64 time=1.43 ms
64 bytes from 192.168.20.1: icmp_seq=2 ttl=64 time=3.61 ms
^C
── 192.168.20.1 ping statistics ──
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 1.429/2.518/3.607/1.089 ms
```

Figura 15 Ping alla metasploitable da Kali

Ho successivamente provveduto ad aggiungere la mia regola personalizzata per poter bloccare **dalla** *Kali* l'accesso **alla** *DVWA* sulla Metasploitable.

Da *PFSense* sul browser della Kali, sono andata nella sezione *Firewall*, ho selezionato *Rules* e ho selezionato LAN, la rete legata alla mia Kali.

All'interno, ho aggiunto una regola tramite il bottone *add*, andando a configurarla come segue.

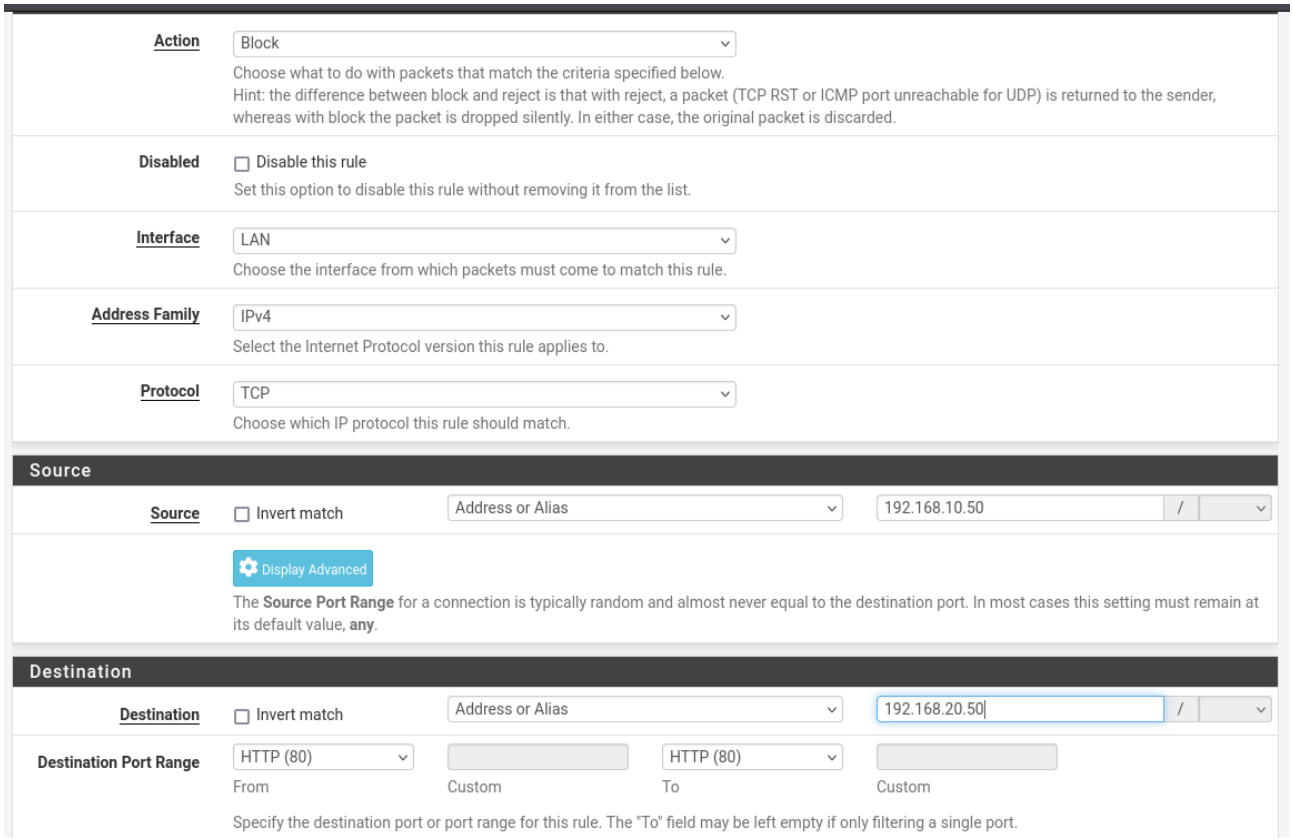

Figura 16 Configurazione regola di Firewall - blocco della Metasploitable DVWA per la Kali

L'action scelta è *Block* in quanto desidero che non ci sia risposta, né negativa, né positiva. Ho settato *l'IP Source* (sorgente) con quello specifico della *Kali* (192.168.10.50/24), *mittente* della mia richiesta verso la pagina DVWA della Metasploitable. Per *l'IP Destination* (destinazione) ho inserito quello della

Metasploitable (192.168.20.50/24), andando però a specificare di voler bloccare solamente il *traffico HTTP* tramite la selezione della *porta 80*.

Mi sono infine assicurata che la regola fosse **in alto**, in modo da venire messa in atto **prima** di quelle di *Pass* generali.

Salvata la regola e confermata l'applicazione dei cambiamenti, ho provato nuovamente a raggiungere la DVWA all'indirizzo IP 192.168.20.50 per assicurarmi che la richiesta andasse in *timeout*.

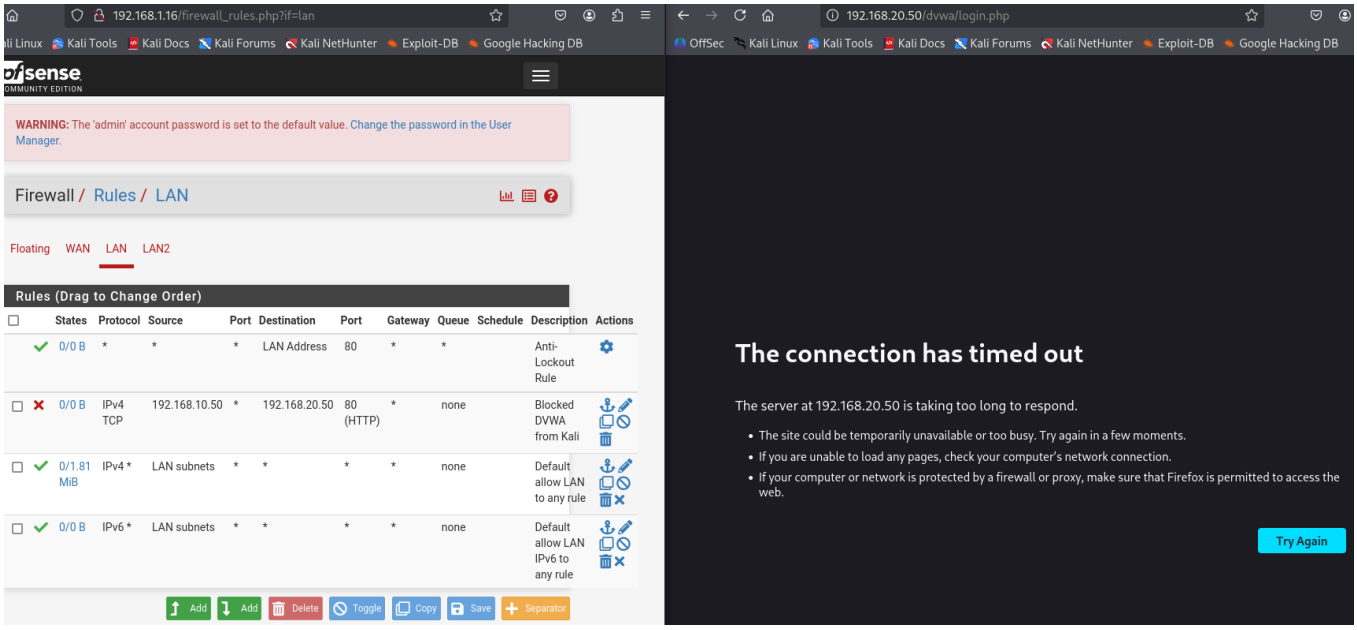

Figura 17 Risultato applicazione regola di block

Ho infine provveduto a controllare che il *ping* dalla *Kali* alla *Metasploitable* ancora funzionasse correttamente nonostante la regola messa in atto.

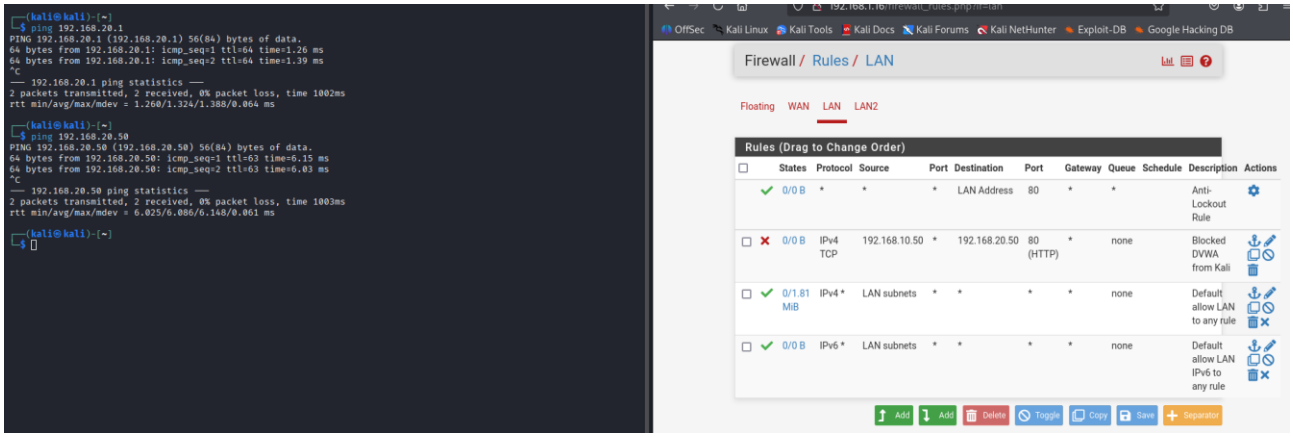

Figura 18 Ping alla Metasploitable dopo l'applicazione della regola

Le configurazioni **finali** delle regole dei *firewall* sono le seguenti:

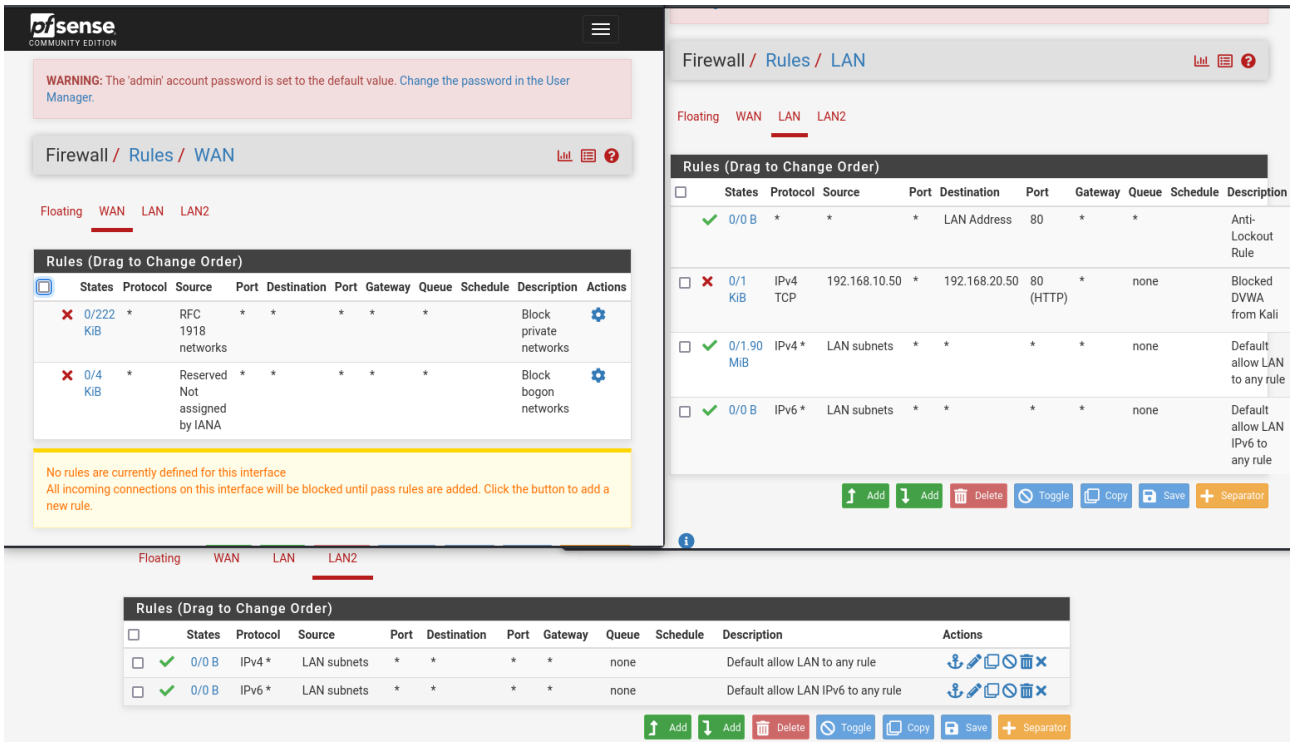

Figura 19 Configurazioni Firewall