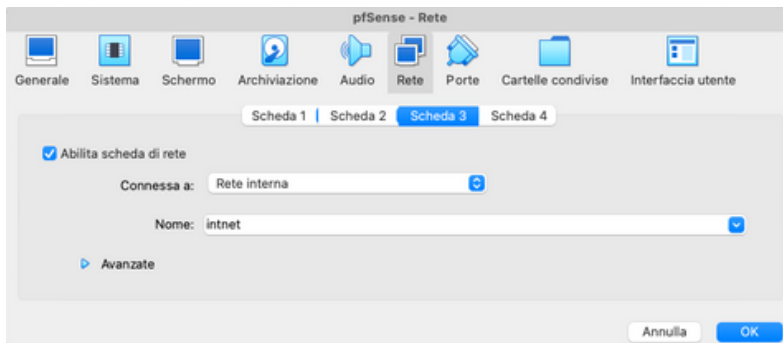


Creazione policy pfSense

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.

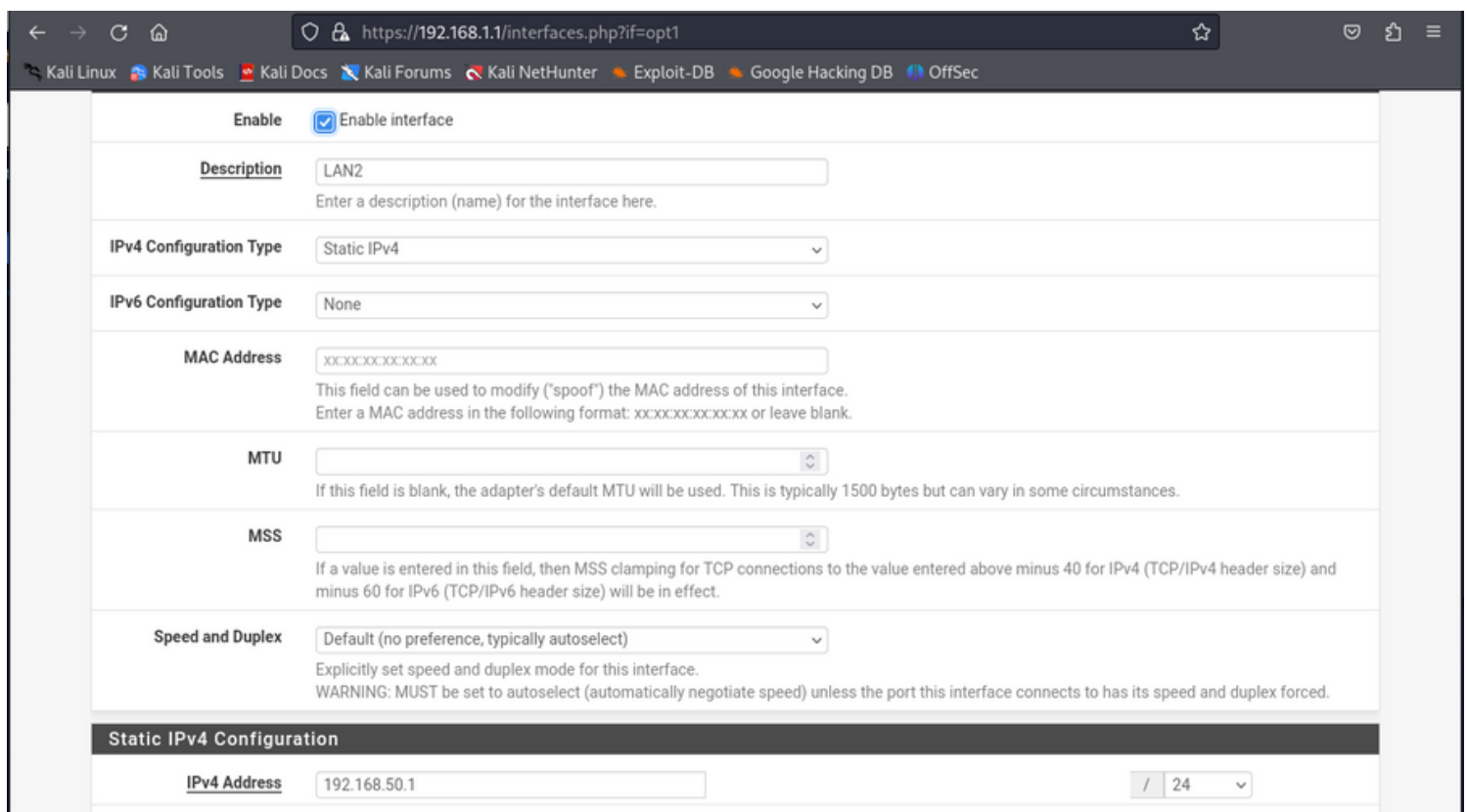
Terza scheda di rete Lan su pfSense:



Configuro su pfSense una terza scheda di rete dalle impostazioni della Virtual Machine. Avrò quindi:

- scheda con bridge
- scheda di rete LAN con indirizzo IPv4 192.168.1.1
- scheda di rete LAN2 appena creata

Sul browser di Kali accedo all'indirizzo di pfSense 192.168.1.1 e configuro l'interfaccia della LAN2 come nella figura in basso:



Notare che l'IP della macchina Meta è 192.168.50.101 quindi l'Ip inserito nella configurazione della LAN2 è il gateway di Meta.

Su pfSense avrò quindi:

```
pfSense [Running]
ERROR: It was not possible to determine pkg remote version
pfSense 2.7.2-RELEASE amd64 20231206-2010
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: a2ab5d3c2e4fb40e2a3b

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

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.29/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24
LAN2 (opt1)    -> em2      -> v4: 192.168.50.1/24

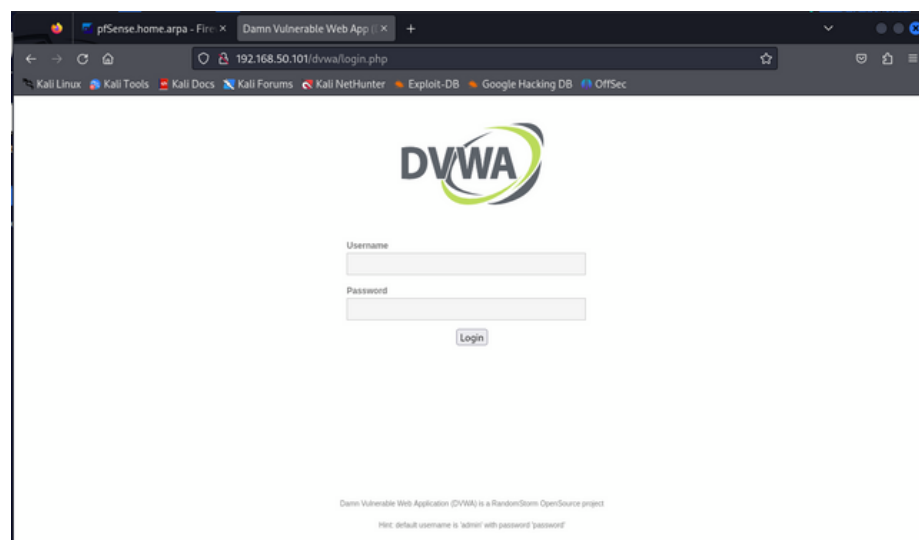
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults    13) Update from console
5) Reboot system               14) Enable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

Enter an option: 
```

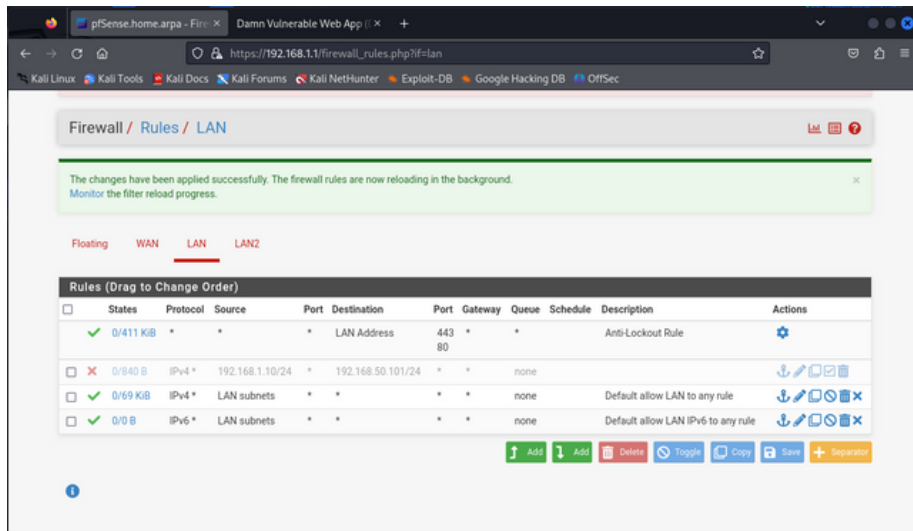
Imposto nella scheda di rete di Kali l'IP della LAN di pfSense come gateway. Tutto ciò per permettere alle 3 macchine di comunicare nonostante Kali e Meta non abbiano la stessa sottorete. Il ping sarà possibile grazie alle configurazioni fatte su pfSense. Ad esempio ping da Kali verso Meta:

```
(kali@Host-010)-[~]
$ ping 192.168.50.101
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data.
64 bytes from 192.168.50.101: icmp_seq=1 ttl=63 time=2.59 ms
64 bytes from 192.168.50.101: icmp_seq=2 ttl=63 time=21.4 ms
64 bytes from 192.168.50.101: icmp_seq=3 ttl=63 time=197 ms
64 bytes from 192.168.50.101: icmp_seq=4 ttl=63 time=4.22 ms
^C
--- 192.168.50.101 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3010ms
rtt min/avg/max/mdev = 2.591/56.258/196.854/81.505 ms
```

Visitando l'IP di Meta dal browser di Kali potrò quindi accedere ai servizi web di Meta.



Dal browser di Kali visito le configurazioni di pfSense: nella sezione Rules del Firewall, sulla LAN, vado a creare una nuova regola per bloccare l'accesso alla DVWA (su Meta) dalla macchina Kali.



Ora non sarà più possibile visualizzare la pagina dei servizi web di Meta e lanciando il comando ping da Kali notiamo che non possiamo ricevere i pacchetti trasmessi.

```
(kali@Host-010)-[~]
$ ping 192.168.50.101
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data.
^C
— 192.168.50.101 ping statistics —
10 packets transmitted, 0 received, 100% packet loss, time 9197ms
```