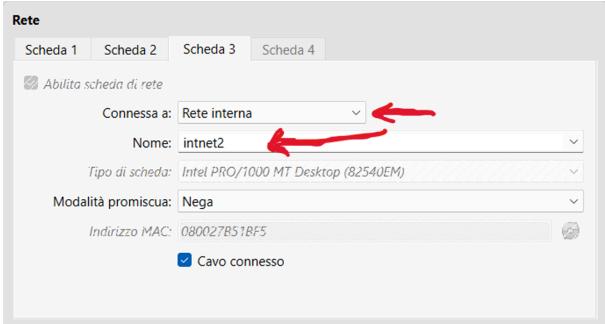
## REPORT S3/L5

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

## **SVOLGIMENTO**

Inizio creando una nuova interfaccia di rete per pfsense assegnandole il nome inet2 e configurandola in rete interna.



Configuro gli indirizzi IP delle due reti LAN disattivando anche il dhcp.

```
WAN (wan)
                                 v4: 192.168.0.1/24
LAN (lan)
                   em1
                                  v4: 192.168.1.1/24
OPT1 (opt1)
                                  v4: 192.168.2.1/24
0) Logout (SSH only)
                                       9) pfTop
1) Assign Interfaces
                                          Filter Logs
                                      11) Restart webConfigurator
2) Set interface(s) IP address
3) Reset webConfigurator password
                                      12) PHP shell + pfSense tools
                                      13) Update from console
4) Reset to factory defaults
5) Reboot system
                                      14) Enable Secure Shell (sshd)
                                      15) Restore recent configuration
6) Halt system
                                      16) Restart PHP-FPM
   Ping host
```

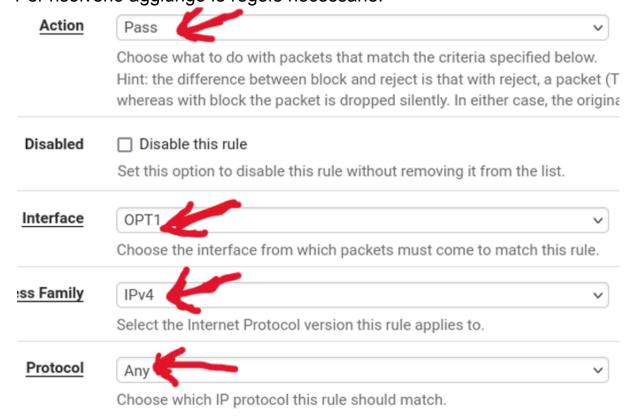
Successivamente assegno gli indirizzi IP a Kali e Metasploitable.

Kali IP: 192.168.1.10 Meta IP: 192.168.2.10

```
PS> ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.10 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 te80::2b3e:921a:2485:2557 prefixlen 64 scopeid 0×20<link>
    ether 08:00:27:ad:25:87 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 27 bytes 3070 (2.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

Instadmin@metasploitable:~$ ifconfig
eth0    Link encap:Ethernet HWaddr 08:00:27:69:e8:f2
    inet addr:192.168.2.10 Bcast:192.168.2.255 Mask:255.255.0
    inet6 addr: fe80::a00:27ff:fe69:e8f2/64 Scope:Link
    UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
```

Eseguendo dei ping per verificare la connessione tra le macchine, noto che Metasploitable non comunica correttamente. Il problema è causato da pfSense, che non ha regole per consentire il traffico. Per risolverlo aggiungo le regole necessarie.

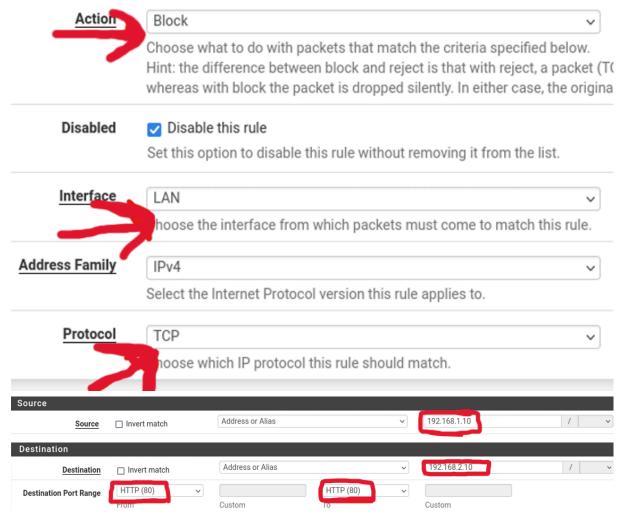


Dopo aver apportato queste modifiche, eseguo nuovamente il ping.

```
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ ping 192.168.2.1
PING 192.168.2.1 (192.168.2.1) 56(84) bytes of data.
64 bytes from 192.168.2.1: icmp_seq=1 ttl=64 time=11.7 ms
64 bytes from 192.168.2.1: icmp_seq=2 ttl=64 time=0.891 ms
64 bytes from 192.168.2.1: icmp_seq=3 ttl=64 time=0.467 ms
64 bytes from 192.168.2.1: icmp_seq=4 ttl=64 time=1.13 ms
```

Di seguito procedo col creare la regola che impedirà a Kali di accedere alla DVWA.

Torno sulla GUI del browser e accedo alla sezione Firewall > Rules > LAN1, imposto BLOCK per negare il traffico, seleziono l'interfaccia LAN, scelgo il protocollo TCP (per bloccare solo il traffico HTTP) e indico la porta 80, che dovrebbe essere quella usata da Metasploitable per DVWA.



Salvo la regola e verifico il funzionamento dal browser.

## Unable to connect

An error occurred during a connection to 192.168.2.10.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the web.

Try Again