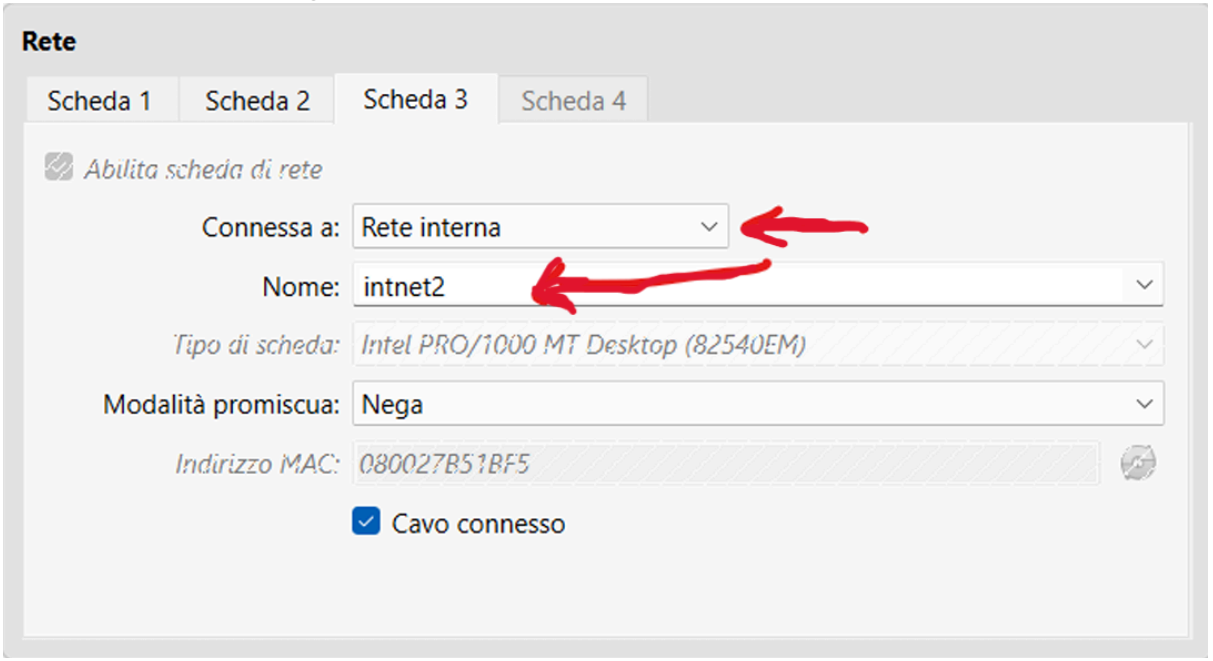
# REPORT S3/L5

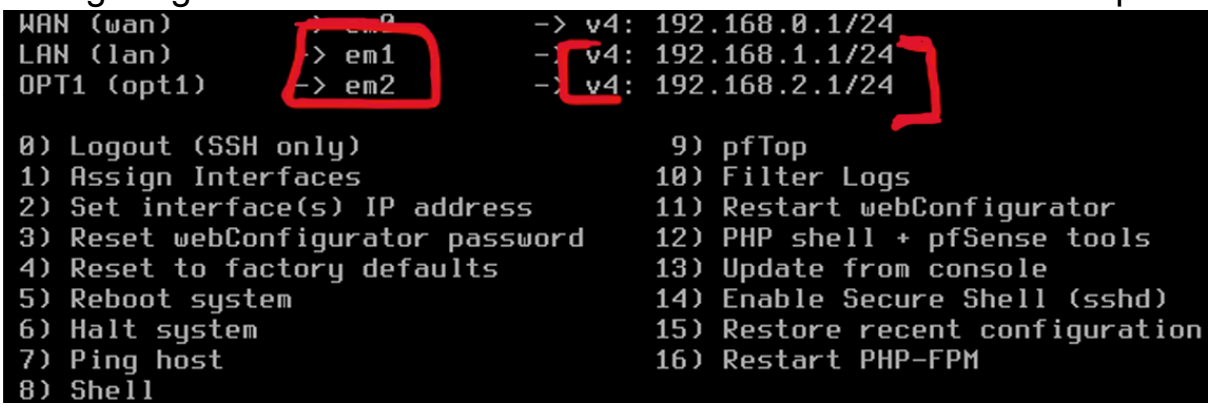
Obiettivo: creare una regola firewall che blocchi l'accesso alla DVWA (su metasploitable) dalla macchina Kali Linux e ne impedisca di conseguenza lo scan.

## SVOLGIMENTO

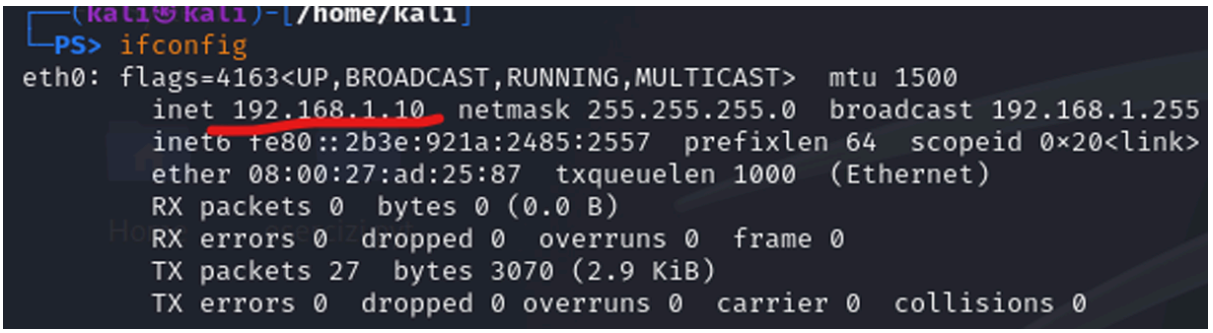
Inizio creando una nuova interfaccia di rete per pfsense assegnandole il nome inet2 e configurandola in rete interna.

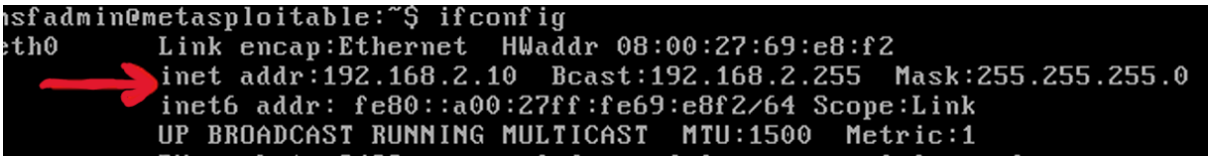



Configuro gli indirizzi IP delle due reti LAN disattivando anche il dhcp.

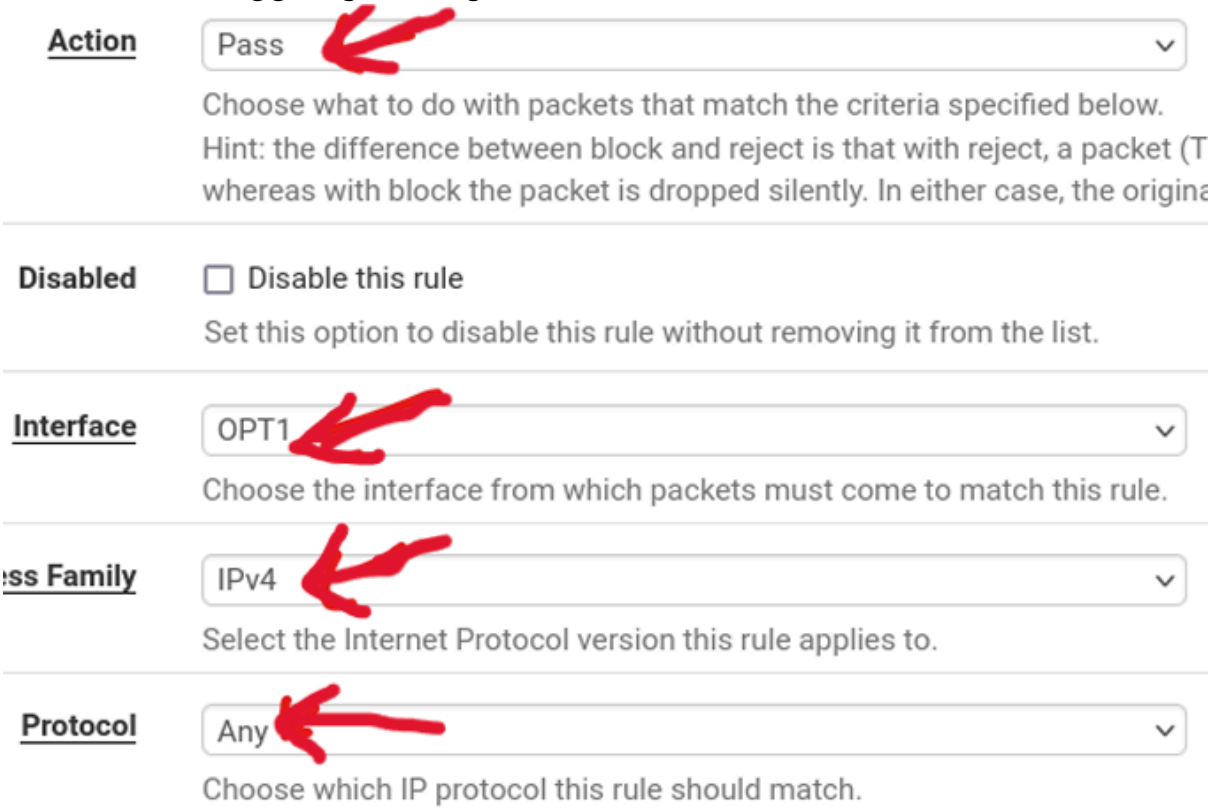


Successivamente assegno gli indirizzi IP a Kali e Metasploitable.
Kali IP: 192.168.1.10
Meta IP: 192.168.2.10



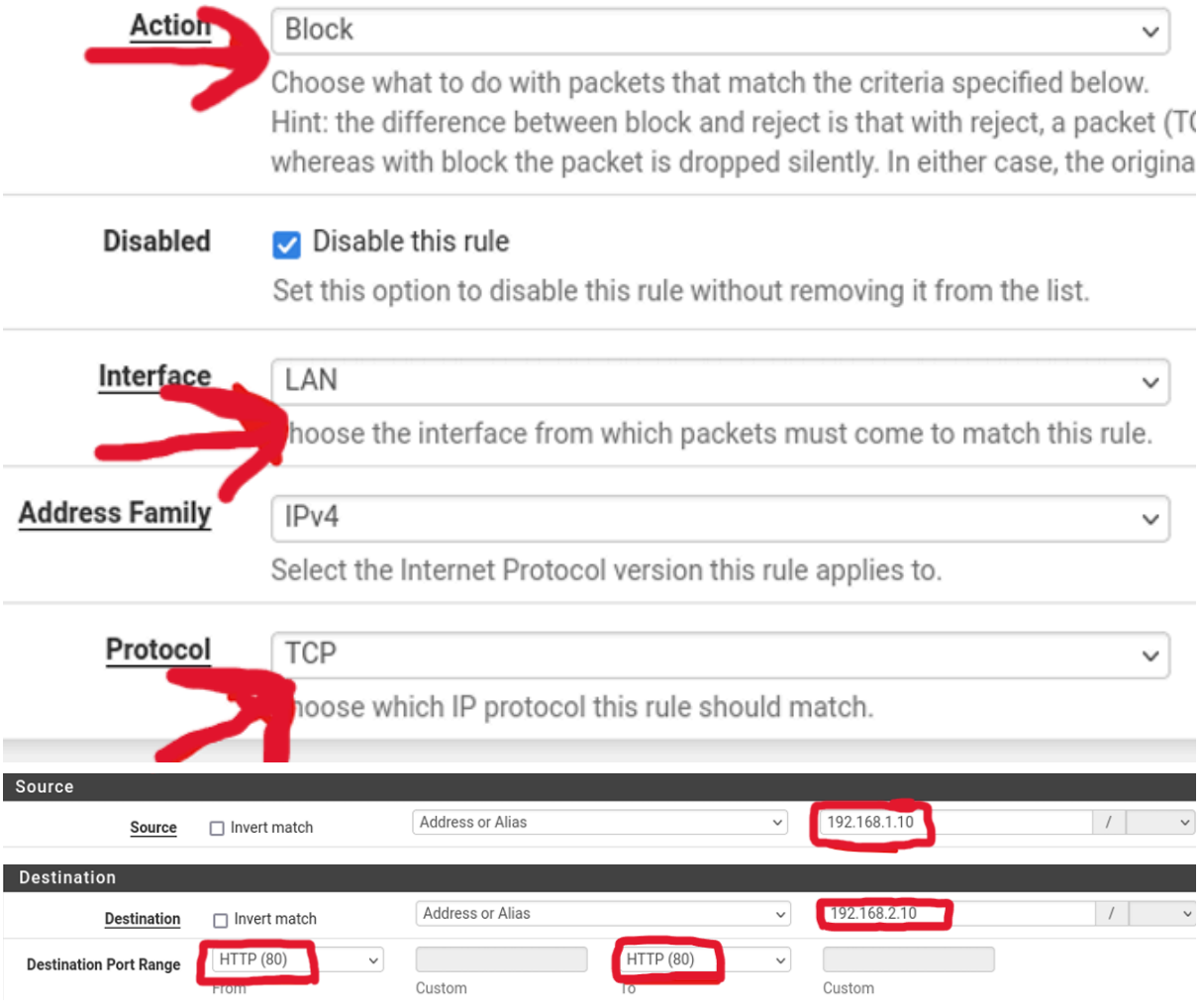

Eseguendo dei ping per verificare la connessione tra le macchine, noto che Metasploitable non comunica correttamente. Il problema è causato da pfSense, che non ha regole per consentire il traffico.
Per risolverlo aggiungo le regole necessarie.



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.