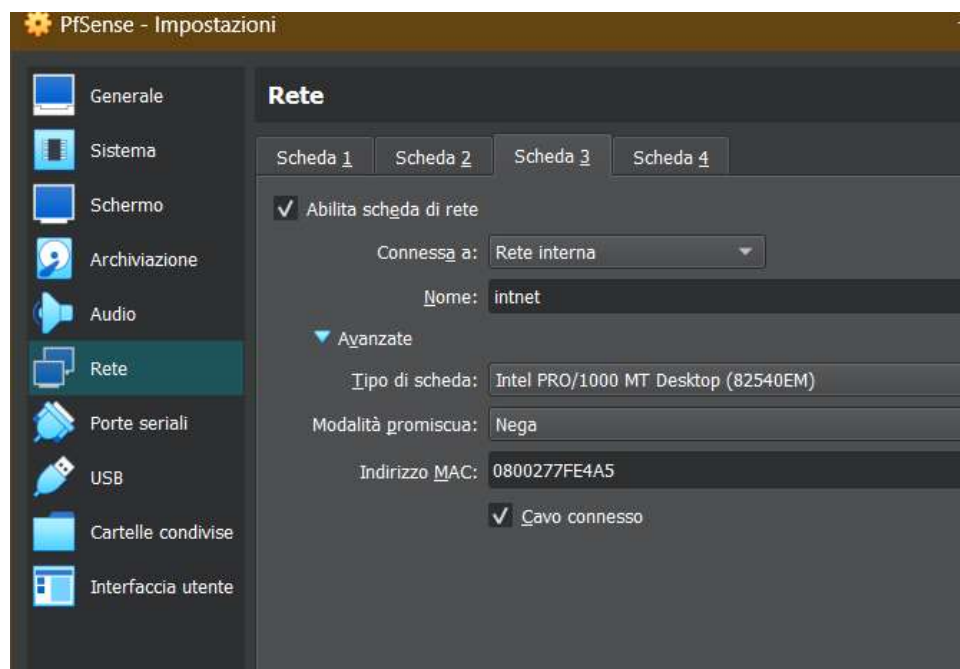


Esercizio:

Creare una regola firewall che blocchi l'accesso alla DVWA (su metasploitable) dalla macchina Kali Linux e ne impedisca di conseguenza lo scan (fare uno screenshot che dimostri che prima lo scan per DVWA funzionava e ora non funziona più). 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. Connettetevi poi in Web GUI per attivare la nuova interfaccia e configurarla.

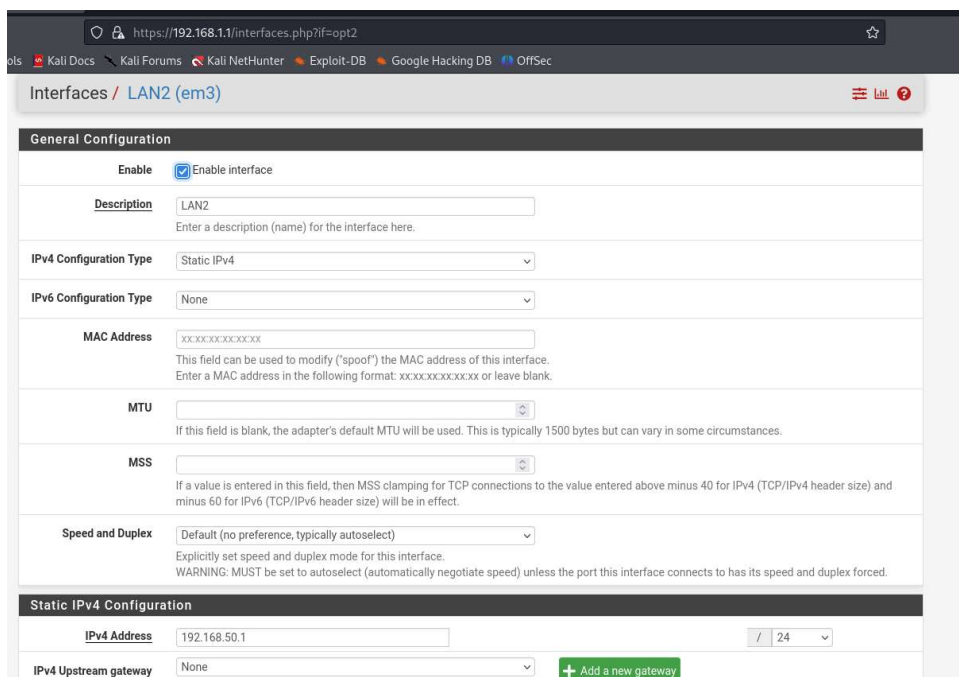
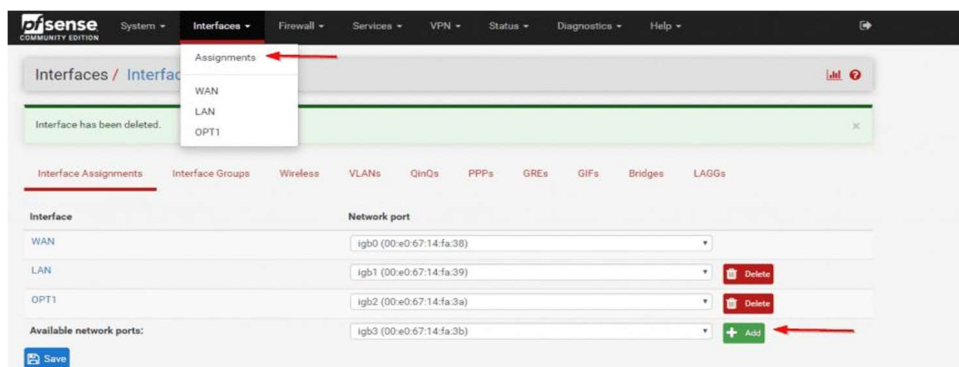
Per far in modo che le nostre macchine Kali e Metasploitable siano su reti diverse bisogna, per prima cosa, andare da Virtualbox nelle impostazioni di rete di PfSense e abilitare una nuova scheda di rete (interna), che attiveremo più avanti, in modo tale da avere una scheda connessa al NAT che si collegherà in internet e due schede connesse in rete interna che verranno utilizzate per donare una nuova interfaccia alle nostre macchine.



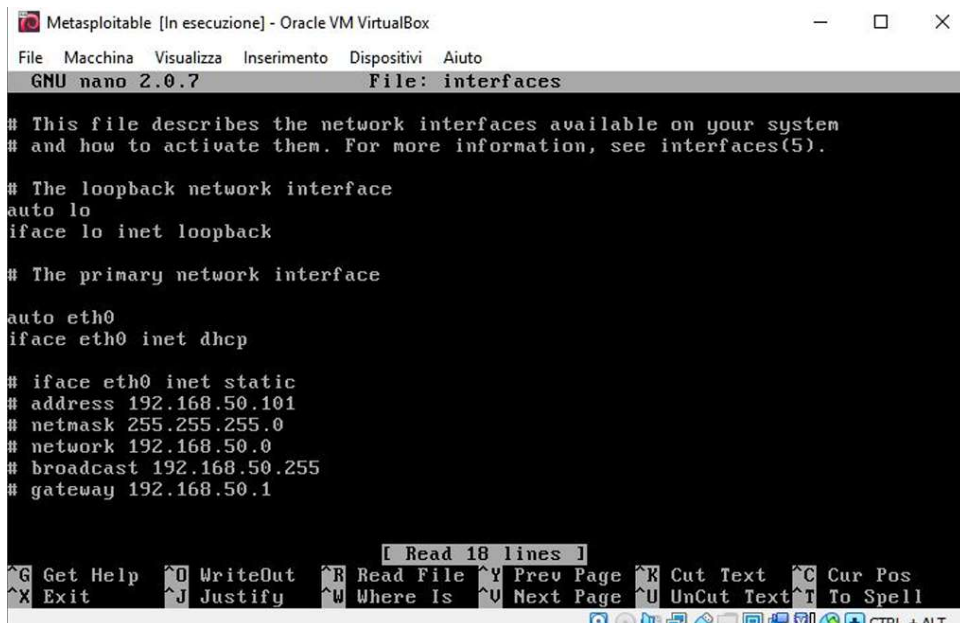
Fatto ciò impostiamo la nostra Kali in dhcp così che possa prendere come indirizzo una delle due interfacce di rete impostate su PfSense. Se facciamo un ip a possiamo notare che la nostra Kali ha preso come indirizzo 192.168.1.100.

```
kali@kali: ~  
File Actions Edit View Help  
ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host noprefixroute  
        valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 08:00:27:1e:36:4a brd ff:ff:ff:ff:ff:ff  
    inet 192.168.1.100/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0  
        valid_lft 4995sec preferred_lft 4995sec  
    inet6 fe80::2573:d5e5:9022:2517/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever
```

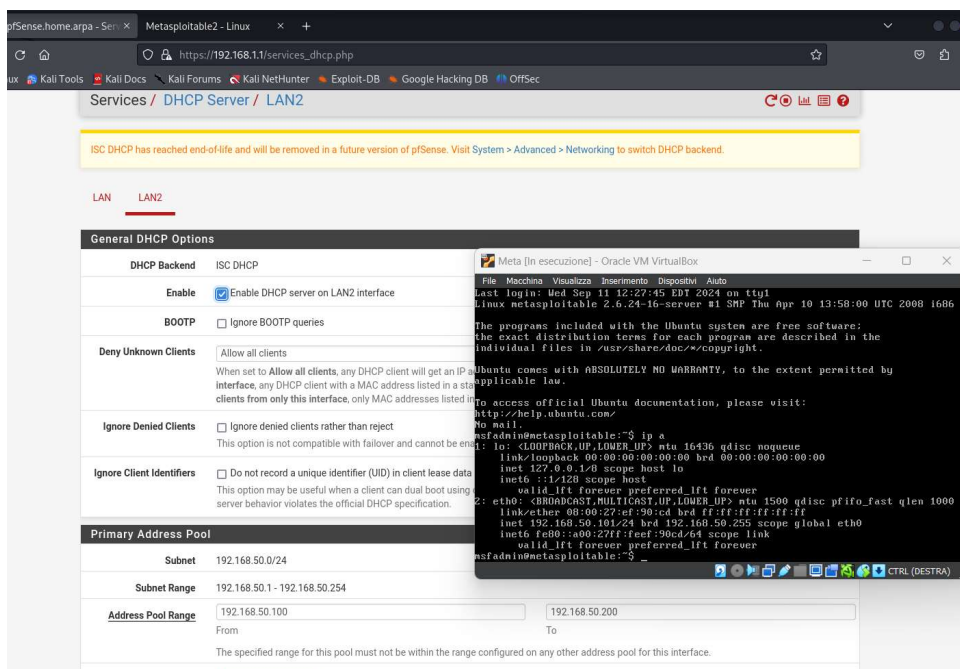
Ora connettiamoci in Web Gui inserendo l'indirizzo IP di PfSense da LAN (192.168.1.1), ci chiederà di inserire Username e Password, rispettivamente "admin" e "pfsense" e una volta entrati potremo attivare e configurare l'interfaccia di rete creata in precedenza. Ci basterà seguire questi pochi passaggi per aggiungere e abilitare la nostra nuova interfaccia.



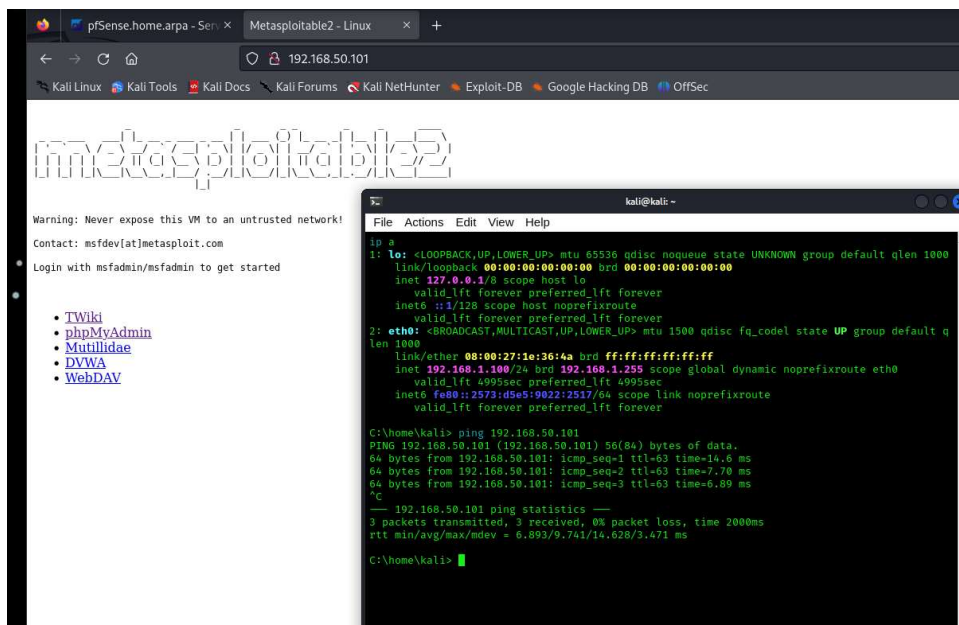
Fatto ciò apriamo la nostra Meta e modifichiamo le impostazioni di rete da statica a dhcp e commentiamo gli indirizzi sotto



Abilitiamo in dhcp l'interfaccia attivata in precedenza e impostiamo un range di indirizzi IP, dato che a noi serve che le nostre due macchine siano su reti diverse, se Kali ha come indirizzo "192.168.1.1", per la nostra Meta imposteremo un range che vada dal 192.168.50.100 al 192.168.50.200. Dopo aver salvato la configurazione, riavviamo la macchina Metasploitable in modo che possa richiedere il suo nuovo indirizzo a PfSense e facciamo un ip a per vedere se la procedura è andata a buon fine.



Adesso tramite Kali proviamo a fare un ping al nuovo indirizzo di Meta per verificare se c'è connettività e se le due macchine comunicano, per un'ulteriore verifica apriamo un web server e cerchiamo l'indirizzo ip di Meta, qui possiamo vedere che la DVWA in questo momento è accessibile.



Fatto tutto ciò.. possiamo ora all'esercizio di oggi, cioè:

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

Per fare ciò basta andare su <Firewall> - <Rules> e premere la freccia in verde con su scritto <Add> (ci sono due freccette, una punta verso l'alto e crea la regola in cima al policy set e l'altra invece verso il basso). Ora aggiungiamo le informazioni necessarie per creare la nostra regola

Firewall / Rules / Edit

Edit Firewall Rule

Action Block
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled ☐ Disable this rule
Set this option to disable this rule without removing it from the list.

Interface LAN
Choose the interface from which packets must come to match this rule.

Address Family IPv4
Select the Internet Protocol version this rule applies to.

Protocol TCP
Choose which IP protocol this rule should match.

Source

Source ☐ Invert match Address or Alias 192.168.1.100 /
[Display Advanced](#)
The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

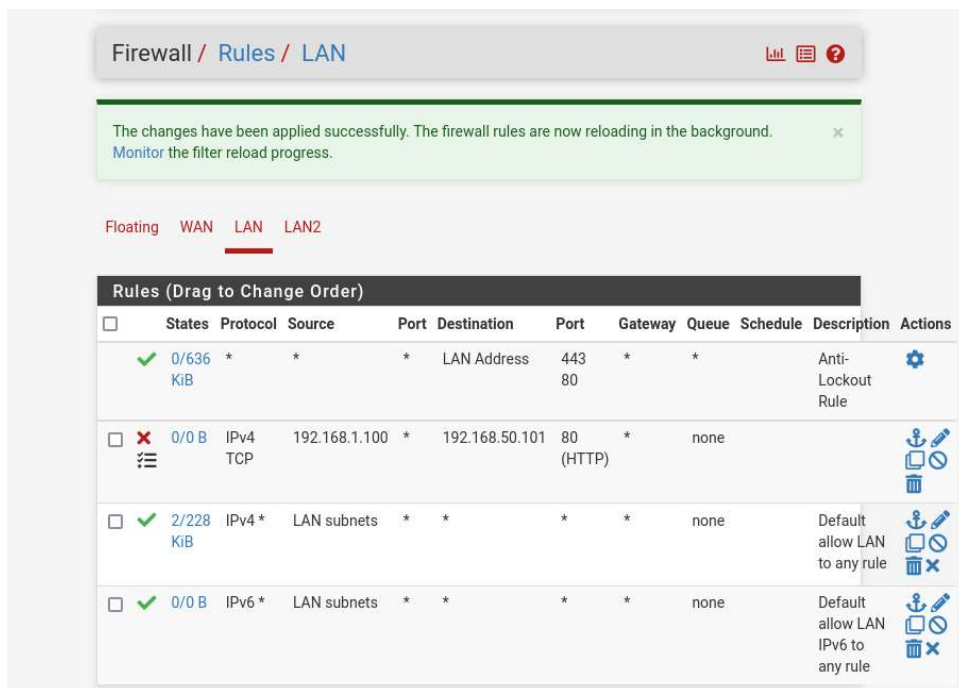
Destination ☐ Invert match Address or Alias 192.168.50.101 /

Destination Port Range HTTP (80) From Custom To Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

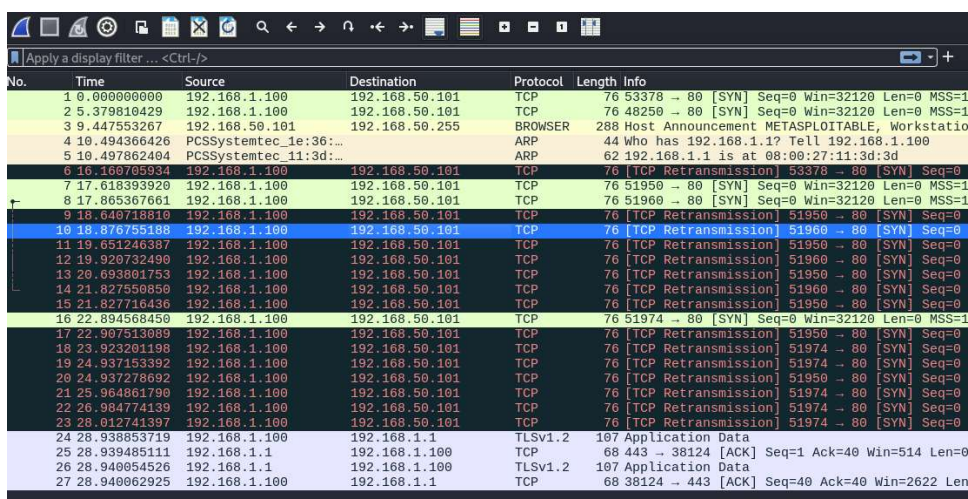
Extra Options

Log ☒ Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Come possiamo vedere dall'immagine, abbiamo detto di creare una regola che **Blocchi** il traffico **TCP** da, indirizzo **sorgente**, quello di Kali quindi, **192.168.1.100** a, indirizzo di **destinazione**, quello di Meta **192.168.50.101**, sulla porta **http(80)** e abbiamo abilitato i **Log** così da poter vedere il traffico che viene gestito dalla regola creata.



Se provassimo ora a raggiungere la DVWA vedremo che non riusciremmo ad avere alcuna risposta dalla destinazione e il browser continuerà ad effettuare tentativi di connessione.



Ora osservando i Log del Firewall abbiamo la conferma che la regola creata stia effettivamente bloccando il traffico da Kali verso la DVWA di Meta.

58 Matched Firewall Log Entries. (Maximum 500)						
Action	Time	Interface	Rule	Source	Destination	Protocol
✗	Sep 14 20:57:21	LAN	USER_RULE (1726347413)	192.168.1.100:50796	192.168.50.101:80	TCP:S
✗	Sep 14 20:57:21	LAN	USER_RULE (1726347413)	192.168.1.100:50804	192.168.50.101:80	TCP:S
✗	Sep 14 20:57:22	LAN	USER_RULE (1726347413)	192.168.1.100:50796	192.168.50.101:80	TCP:S
✗	Sep 14 20:57:22	LAN	USER_RULE (1726347413)	192.168.1.100:50804	192.168.50.101:80	TCP:S
✗	Sep 14 20:57:23	LAN	USER_RULE (1726347413)	192.168.1.100:50796	192.168.50.101:80	TCP:S
✗	Sep 14 20:57:23	LAN	USER_RULE (1726347413)	192.168.1.100:50804	192.168.50.101:80	TCP:S