

Creazione rete firewall

1. Prefazione

Nel report di oggi, viene chiesto di creare una rete firewall all'interno della stessa rete, come da consegna dovremo creare una Policy avvalendoci dello strumento PFsense e negare, attraverso una rete sorgente, un IP di destinazione; gli IP della Kali e di Metasploitable devono essere su reti diverse

2. Strumenti

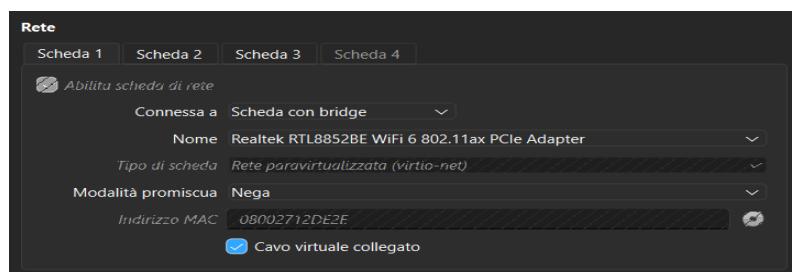
Per fare ciò che la consegna ci chiede, avremo bisogno di 3 Macchine virtuali:

- Kali linux: la macchina sorgente da cui dovremo operare per configurare PfSense e negare il traffico alla macchina Metasploitable.
- PfSense: che farà da router a cui dovremo impartire gli ordini di bloccare il traffico della Metasploitable
- Metasploitable: la macchina target da bloccare

3. Configurazione

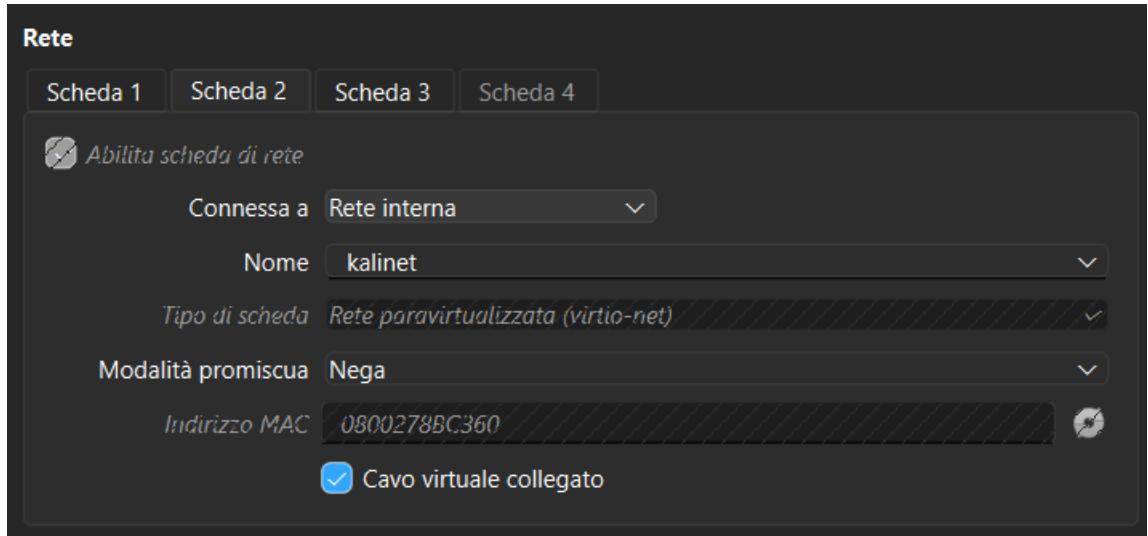
Per poter configurare i dispositivi come da consegna, dobbiamo aprire innanzitutto Oracle Virtual Box per poter gestire le nostre VM, andare in impostazioni della PFsense e assegnarle 3 schede di rete:

- Scheda rete1:



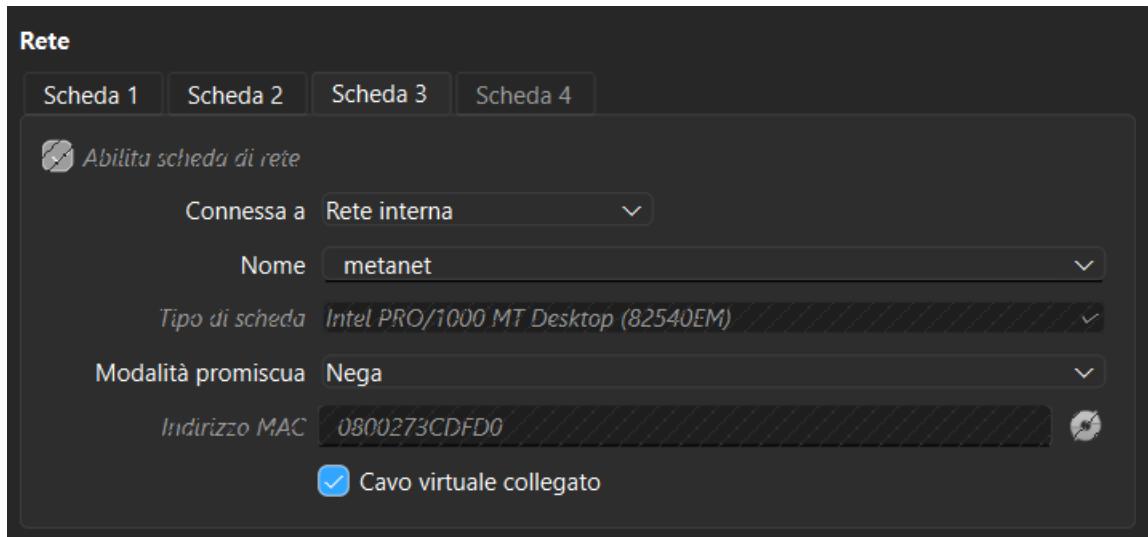
Scheda in Bridge, in modo da far condividere l'IP del nostro router di casa alla PFsense, sarà quindi la nostra rete WAN.

- Scheda rete2:



Creiamo una rete LAN per connettere la Kali con la PFsense

- Scheda rete3:



Creiamo una rete LAN per connettere la Metasploitable con la PFsense

Una volta create le 3 schede di rete, apriamo rispettivamente PFsense e Kali per avere le configurazioni desiderate per la Kali e per la Metasploitable.

Aprendo PFsense, prendiamo l'indirizzo IP

```
Starting CRON... done.
pfSense 2.7.2-RELEASE amd64 20231206-2010
Bootup complete

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

VirtualBox Virtual Machine - Netgate Device ID: 4cbef61eed7e76828d8

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

WAN (wan)      -> vtnet0      -> v4/DHCP4: 192.168.1.137/24
LAN (lan)      -> vtnet1      -> v4: 192.168.50.1/24
OPT1 (opt1)    -> em0        -> v4: 192.168.40.1/24

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: █
```

Prendiamo l'IP della PFsense e utilizziamo il browser della Kali:

192.168.1.137.

Facciamo l'accesso e andiamo nel menù, andiamo in “Interfces” e andiamo in “Assignments”, dovrebbe portarci la voce ADD, selezioniamo OPT1, e successivamente riguardando nella PFsense, ora abbiamo 3 schede, come da Screen; andiamo nella opzione 2, e configuriamo in modo che venga assegnato il DHCP alla Metasploitable.

Apriamo Metasploitable per modificare il file di rete con sudo nano
/etc/network/interfaces

Poi modifichiamo static a DHCP.

Una volta fatto ciò, dovrebbe essere tutto collegato, facciamo il ping dalla Kali alla Meta.

```

Session Actions Edit View Help
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=1.15 ms
64 bytes from 192.168.20.1: icmp_seq=2 ttl=64 time=0.808 ms
64 bytes from 192.168.20.1: icmp_seq=3 ttl=64 time=0.489 ms
64 bytes from 192.168.20.1: icmp_seq=4 ttl=64 time=0.485 ms
64 bytes from 192.168.20.1: icmp_seq=5 ttl=64 time=0.393 ms
64 bytes from 192.168.20.1: icmp_seq=6 ttl=64 time=0.497 ms
64 bytes from 192.168.20.1: icmp_seq=7 ttl=64 time=0.585 ms
64 bytes from 192.168.20.1: icmp_seq=8 ttl=64 time=0.495 ms
64 bytes from 192.168.20.1: icmp_seq=9 ttl=64 time=0.514 ms
64 bytes from 192.168.20.1: icmp_seq=10 ttl=64 time=0.495 ms
64 bytes from 192.168.20.1: icmp_seq=11 ttl=64 time=0.491 ms
64 bytes from 192.168.20.1: icmp_seq=12 ttl=64 time=0.441 ms
64 bytes from 192.168.20.1: icmp_seq=13 ttl=64 time=0.435 ms
64 bytes from 192.168.20.1: icmp_seq=14 ttl=64 time=0.335 ms
64 bytes from 192.168.20.1: icmp_seq=15 ttl=64 time=0.627 ms
```
192.168.40.1 ping statistics:
15 packets transmitted, 15 received, 0% packet loss, time 14665ms
rtt min/avg/max/mdev = 0.393/0.478/1.15/0.189 ms

```

E' apposto, Metasploitable è contattabile.

#### 4. Policy Firewall

Come ultimo step, attraverso PFSense dobbiamo implementare un firewall in grado di bloccare il traffico dalla Kali alla Meta, quindi ritorniamo sul browser della Kali, entriamo in Pfsense e andiamo in “Firewall”, “Rules”; avremo 4 Opzioni:

Floating, WAN, LAN e OPT1.

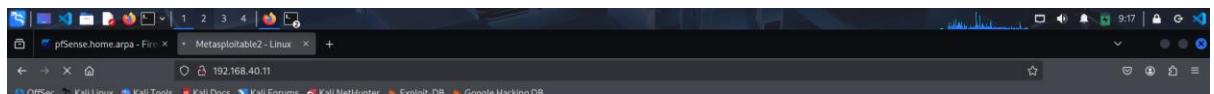
A noi interessa interrompere il traffico all'interno della LAN, quindi clicchiamo lì e dovremo trovarci davanti una cosa del genere:

| Rules (Drag to Change Order)        |            |          |               |      |               |           |         |       |          |                                    |         |
|-------------------------------------|------------|----------|---------------|------|---------------|-----------|---------|-------|----------|------------------------------------|---------|
|                                     | States     | Protocol | Source        | Port | Destination   | Port      | Gateway | Queue | Schedule | Description                        | Actions |
| <input checked="" type="checkbox"/> | 0/0 B      | *        | *             | *    | LAN Address   | 80        | *       | *     | *        | Anti-Lockout Rule                  |         |
| <input checked="" type="checkbox"/> | 0/1 KiB    | IPv4/TCP | 192.168.50.10 | *    | 192.168.40.11 | 80 (HTTP) | *       | *     | *        |                                    |         |
| <input checked="" type="checkbox"/> | 1/6.56 MiB | IPv4 *   | LAN subnets   | *    | *             | *         | *       | *     | *        | Default allow LAN to any rule      |         |
| <input checked="" type="checkbox"/> | 0/0 B      | IPv6 *   | LAN subnets   | *    | *             | *         | *       | *     | *        | Default allow LAN IPv6 to any rule |         |

Andiamo in ADD e creiamo una nuova regola, consci del fatto che per poter funzionare, la regola deve essere in alto, come da screen.

Le azioni saranno le seguenti:

- In “Action” spuntiamo block: non solo non vogliamo far passare i pacchetti, ma non vogliamo notificare l’altra parte dello scambio fallito. (Abbiamo pass per far passare i pacchetti, Reject per bloccarli e notificare, e Block per non notificare).
- Interface: LAN: noi vogliamo ancora una volta confermare che vogliamo bloccare un dato indirizzo nella rete LAN di cui facciamo parte
- Address Family IPV4: la famiglia di configurazione a cui siamo interessati
- Protocol: quale tipo di protocollo vogliamo respingere
- Source: Address or Alias; la sorgente è la macchina che sta puntando il traffico da bloccare, in questo caso è la nostra Kali
- Destination: Address or Alias; la macchina puntata.  
Ed è la nostra Metasploitable.  
Salviamo e verifichiamo



Warning: Never expose this VM to an untrusted network!

Contact: msfdev@metasploit.com

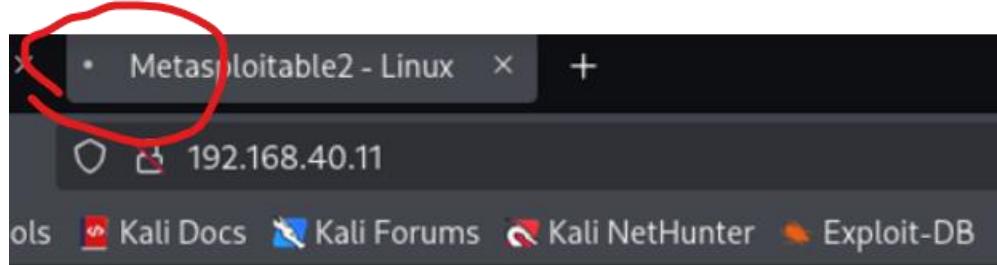
Login with msfadmin/msfadmin to get started

- T00ki
- shhMyAdmin
- Multilidate
- DVWA
- WebDAV

192.168.40.11

Questo è prima di applicare la regola.

Successivamente, applicata la regola non lo sarà più.



[\wedge\|/\-\{\}\|\wedge\|/\-\{\}\|\wedge\|/\-\{\}\|