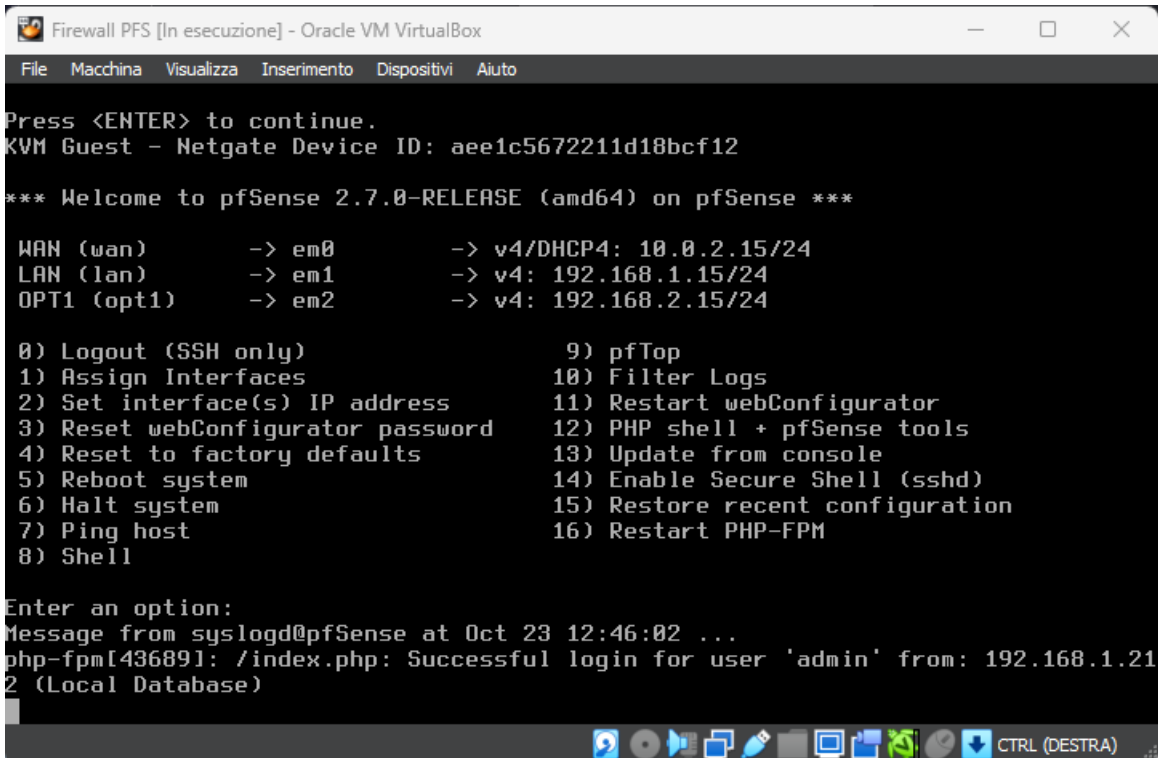


Pratica S5L1

Obiettivo: facciamo comunicare le macchine kali e metasploitable su reti diverse utilizzando il firewall PF-Sense come router GW. Successivamente andiamo a configurare una regola per impedire alla macchina Kali di puntare alla pagina web esposta su Metasploitable contenente la DVWA.

Innanzitutto configuriamo gli indirizzi ip sul firewall pfSense:



```
Press <ENTER> to continue.
KVM Guest - Netgate Device ID: aee1c5672211d18bcf12

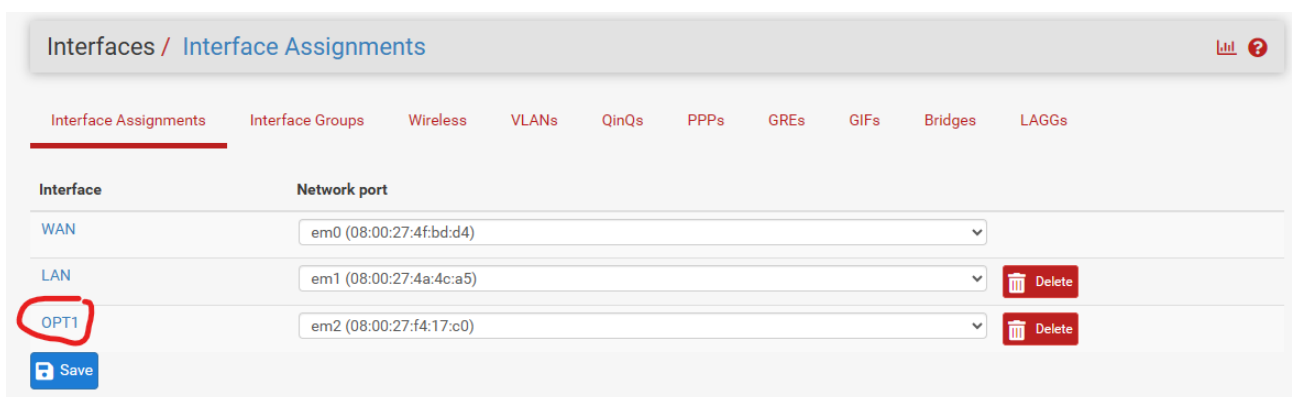
*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
LAN (lan)      -> em1      -> v4: 192.168.1.15/24
OPT1 (opt1)    -> em2      -> v4: 192.168.2.15/24

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:
Message from syslogd@pfSense at Oct 23 12:46:02 ...
php-fpm[436891]: /index.php: Successful login for user 'admin' from: 192.168.1.21
2 (Local Database)
```

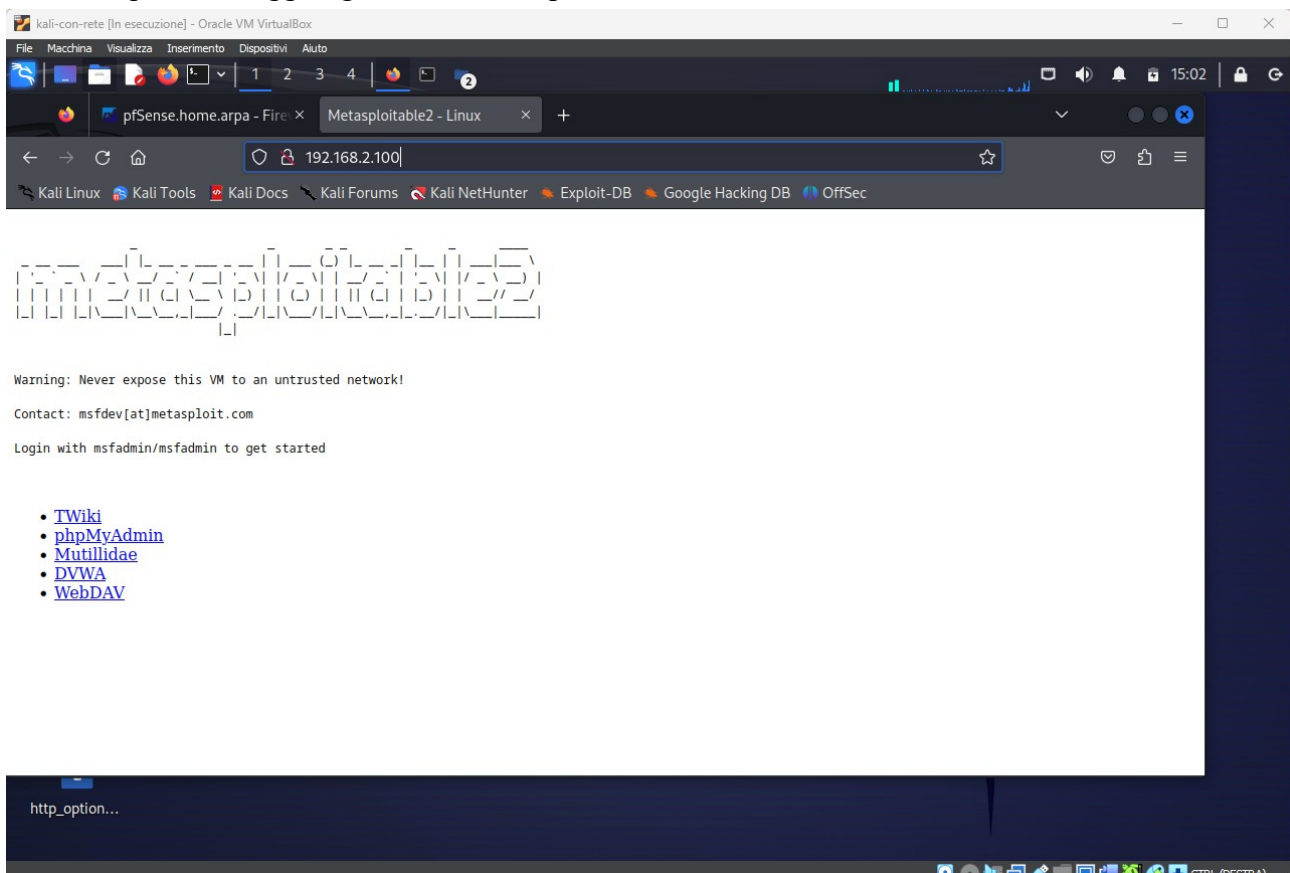
Ho configurato gli ip 192.168.1.15 e 192.168.2.15 seguendo la procedura guidata al punto 2 dopo aver configurato la macchina virtuale per accettare una seconda scheda di rete, ed aver configurato il firewall via GUI WEB attivando l'interfaccia sotto la scheda interface:



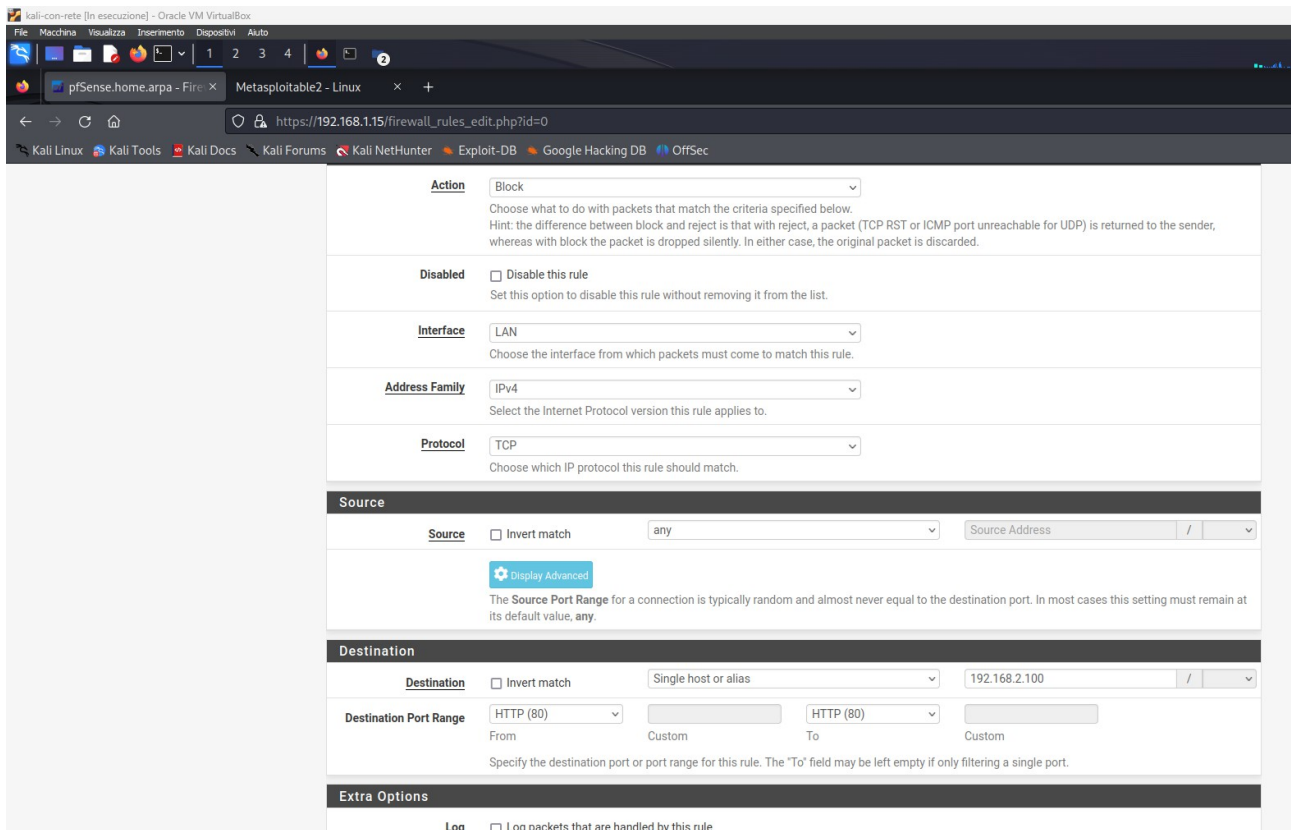
Da kali, aggiungo una rotta per specificare che le richieste verso la macchina Metasploit vanno indirizzate verso il Firewall (che risponde all'ip 192.168.1.15):

```
(luca@kali)-[/etc/network/interfaces.d]
$ route -n
Kernel IP routing table
Destination      Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0          192.168.1.254  0.0.0.0         UG    100    0      0 eth0
192.168.1.0      0.0.0.0        255.255.255.0   U     100    0      0 eth0
192.168.2.0      192.168.1.15  255.255.255.0   UG     0     0      0 eth0
```

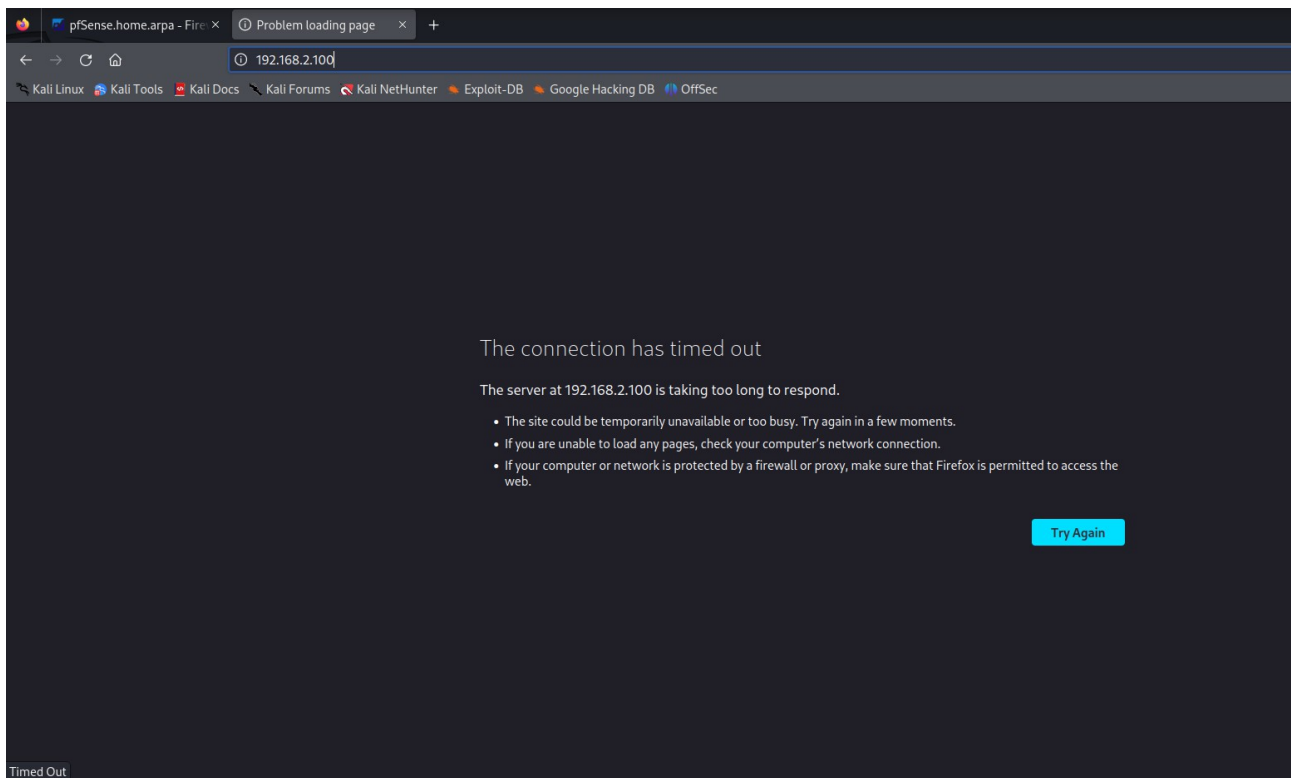
Verifico quindi la raggiungibilità di Metasploit da Kali:



Successivamente vado quindi ad impostare una regola sul firewall per impedire il traffico verso la macchina Metasploit sulla porta 80 (HTTP), come da immagine nella pagina successiva. Notare che la regola accetta il traffico da qualsiasi ip (any) ma nega il traffico HTTP verso il 192.168.2.100:



Vado quindi a provare nuovamente la raggiungibilità, ricordandomi di salvare la configurazione e fare “apply changes” nella pagina successiva:



Questa volta la pagina contenente la DVWA su Metasploit non viene raggiunta.