

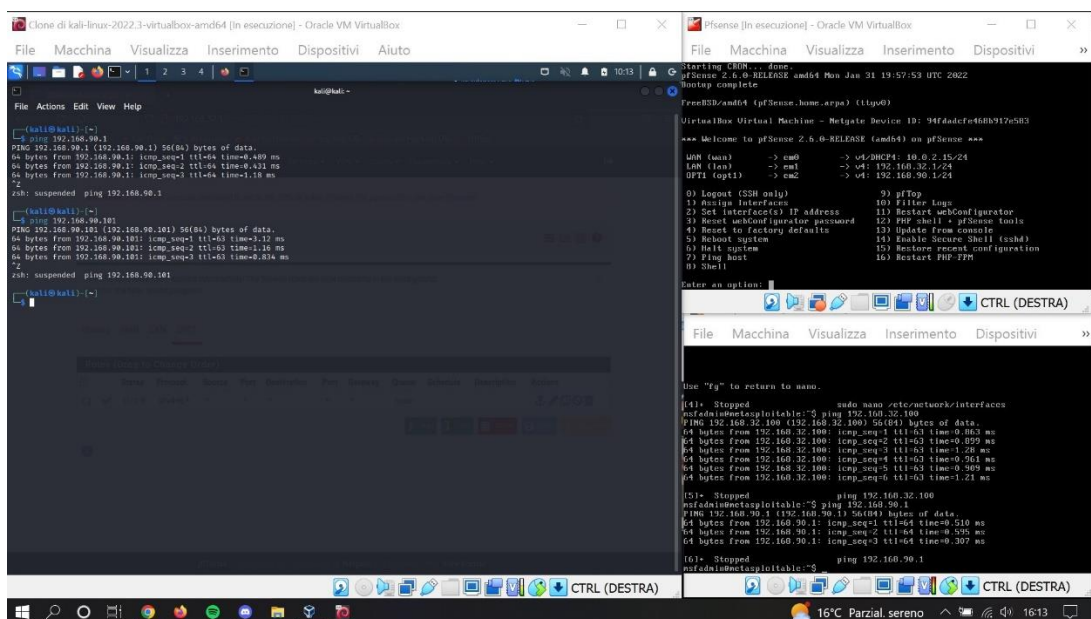
CREAZIONE POLICY PFSENSE

Per questo esercizio abbiamo scaricato la macchina virtuale Pfsense e l'abbiamo configurata in modo tale che abbia una rete WAN e due reti LAN.

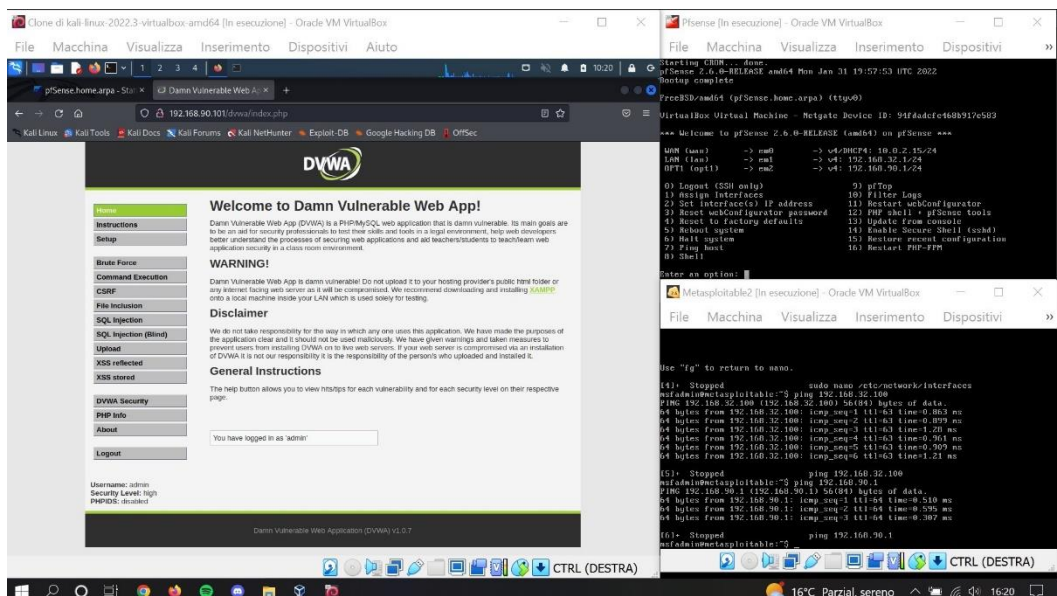
Le due reti LAN le abbiamo poi collegate alle macchine virtuali Kali (IP 192.168.32.100) e Metasploitable2 (IP 192.168.90.101), rispettivamente con gli IP:

- 192.168.32.1 (per Kali)
- 192.168.90.1 (per Meta)

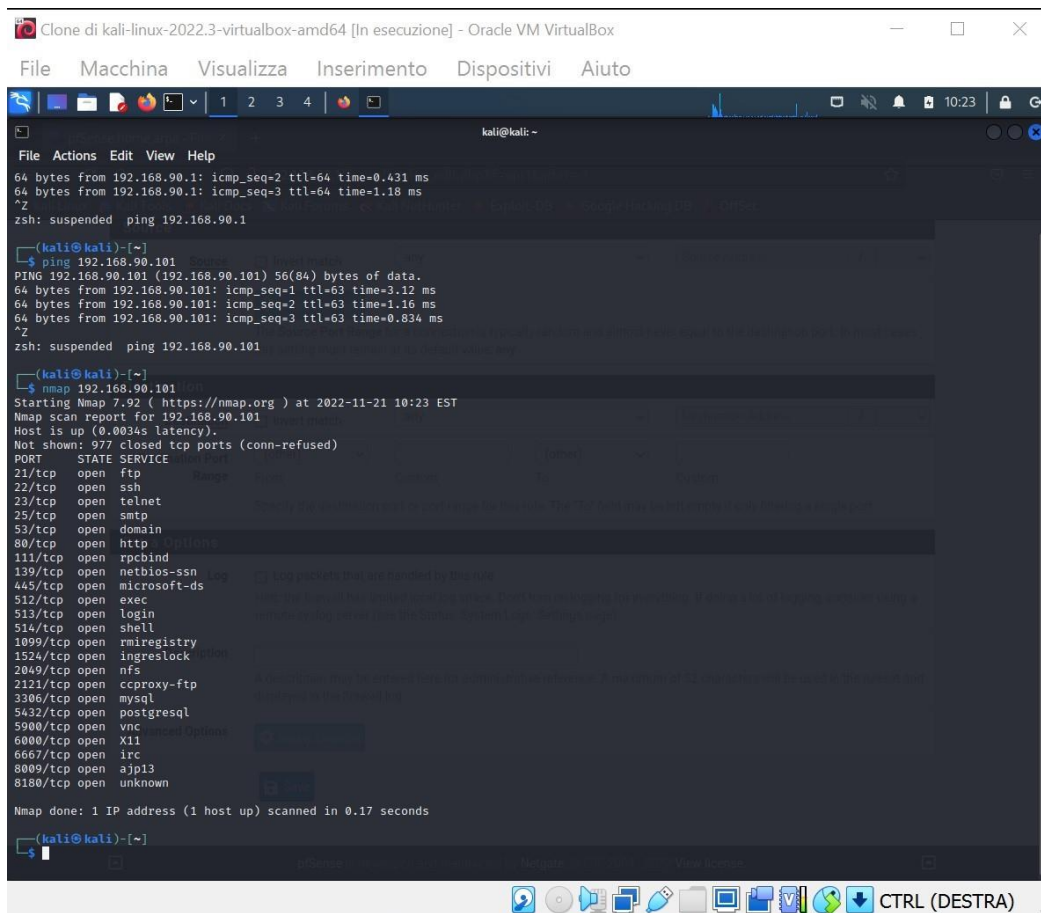
Abbiamo poi controllato che le tre macchine riuscissero a fare ping tra loro:



Una volta controllato il ping, dalla macchina Kali siamo andati sulla DVWA di Metasploitable2:



Per poi farne una scansione con nmap:



```
Clone di kali-linux-2022.3-virtualbox-amd64 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

kali@kali: ~
File Actions Edit View Help
64 bytes from 192.168.90.1: icmp_seq=2 ttl=64 time=0.431 ms
64 bytes from 192.168.90.1: icmp_seq=3 ttl=64 time=1.18 ms
^Z
zsh: suspended ping 192.168.90.1

(kali@kali)~$ ping 192.168.90.101
PING 192.168.90.101 (192.168.90.101) 56(84) bytes of data.
64 bytes from 192.168.90.101: icmp_seq=1 ttl=63 time=3.12 ms
64 bytes from 192.168.90.101: icmp_seq=2 ttl=63 time=1.16 ms
64 bytes from 192.168.90.101: icmp_seq=3 ttl=63 time=0.834 ms
^Z
zsh: suspended ping 192.168.90.101

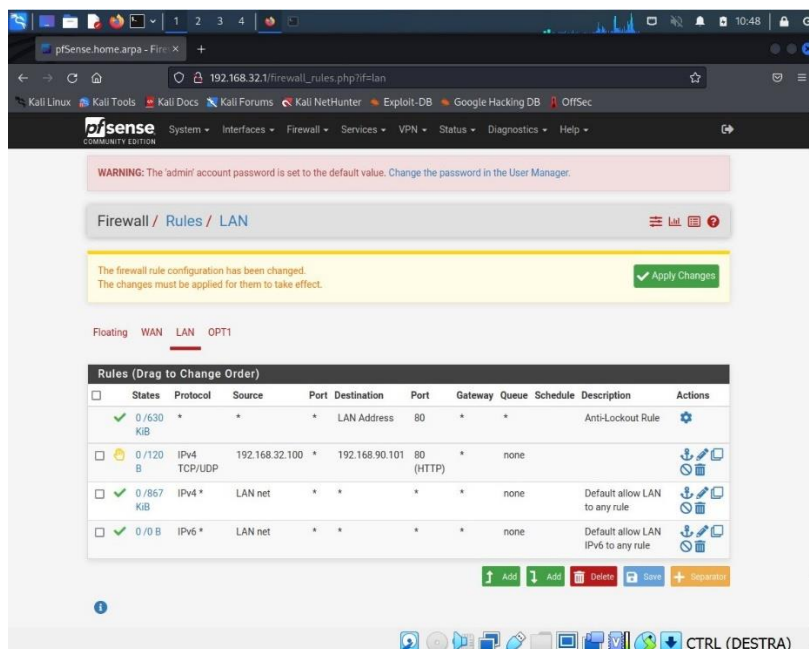
(kali@kali)~$ nmap 192.168.90.101
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-21 10:23 EST
Nmap scan report for 192.168.90.101
Host is up (0.0034s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  cproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds

(kali@kali)~$
```

Sulla base di quanto visto ora abbiamo dovuto creare una regola firewall, su PfSense, che blocchi l'accesso alla DVWA su Metasploitable dalla macchina Kali e che ne impedisca di conseguenza lo scan.

Abbiamo quindi creato la nuova regola seguendo il percorso: Firewall>>Rules>>LAN>>add per poi controllarne il giusto funzionamento:



```
(kali㉿kali)-[~]  
$ ping 192.168.90.101  
PING 192.168.90.101 (192.168.90.101) 56(84) bytes of data: 192.168.90.101: icmp_seq=1 ttl=63 time=0.956 ms  
64 bytes from 192.168.90.101: icmp_seq=1 ttl=63 time=0.956 ms  
64 bytes from 192.168.90.101: icmp_seq=2 ttl=63 time=1.34 ms  
64 bytes from 192.168.90.101: icmp_seq=3 ttl=63 time=1.42 ms  
64 bytes from 192.168.90.101: icmp_seq=4 ttl=63 time=1.29 ms  
^Z  
zsh: suspended ping 192.168.90.101  
  
(kali㉿kali)-[~]  
$ nmap 192.168.90.101 -p 80  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-21 10:46 EST  
Nmap scan report for 192.168.90.101  
Host is up (0.00070s latency).  
  
PORT      STATE SERVICE  
80/tcp    closed http  
  
Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds  
  
(kali㉿kali)-[~]  
$ █
```