

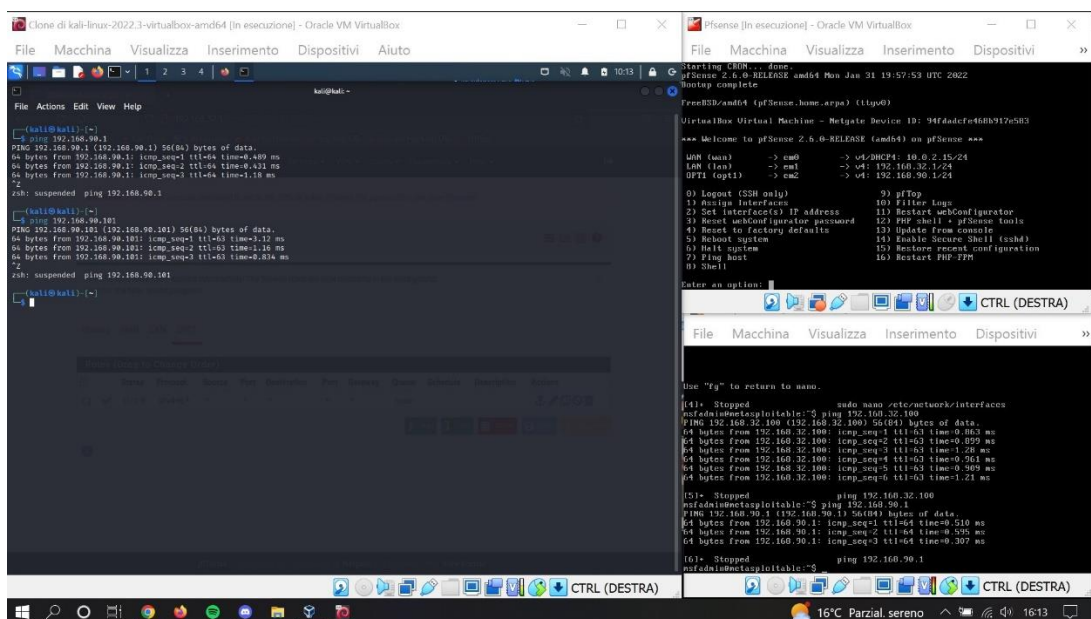
# CREAZIONE POLICY PFSENSE

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.

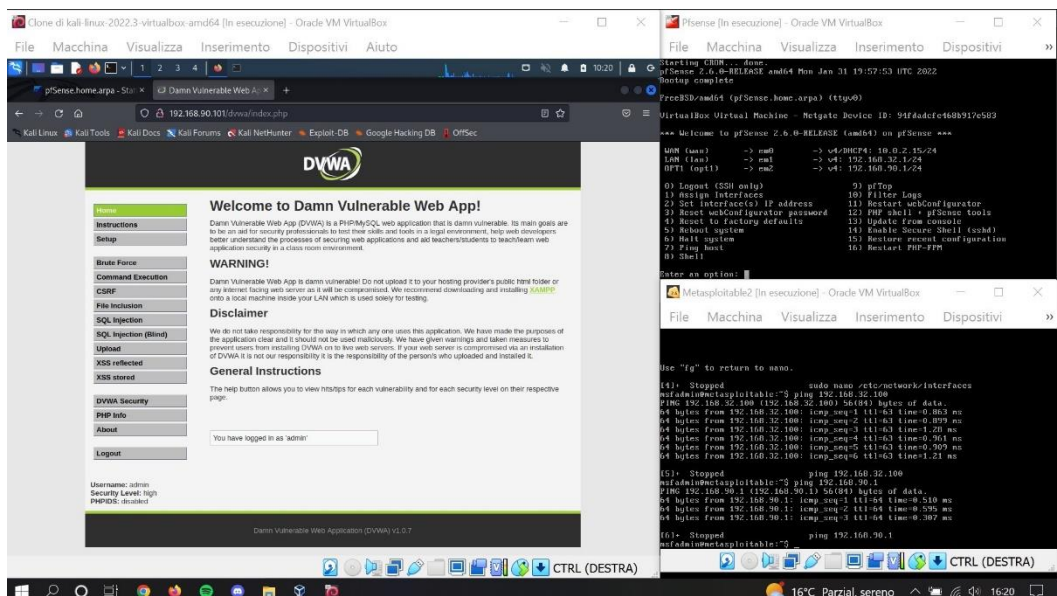
Le due reti LAN le abbiamo poi collegate alle macchine virtuali Kali (IP 192.168.32.100) e Metasploitable2 (IP 192.168.90.101), rispettivamente con gli IP:

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

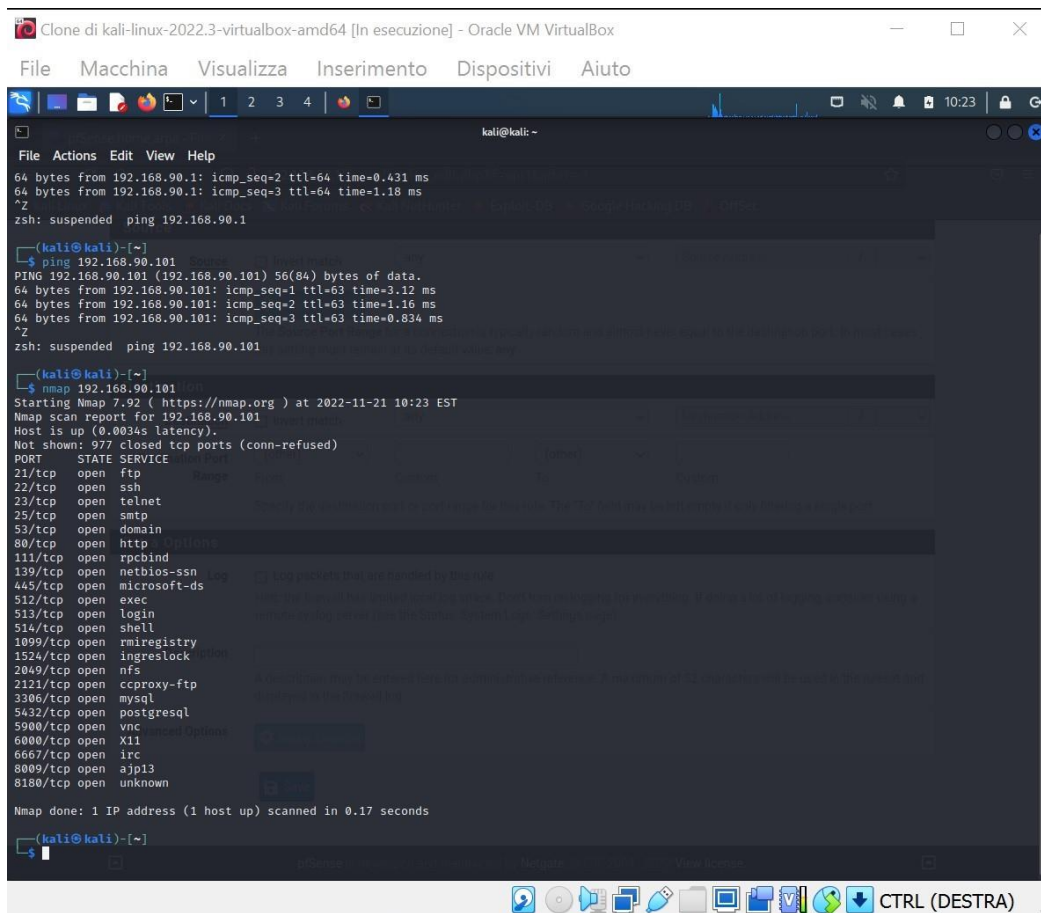
Abbiamo poi controllato che le tre macchine riuscissero a fare ping tra loro:



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

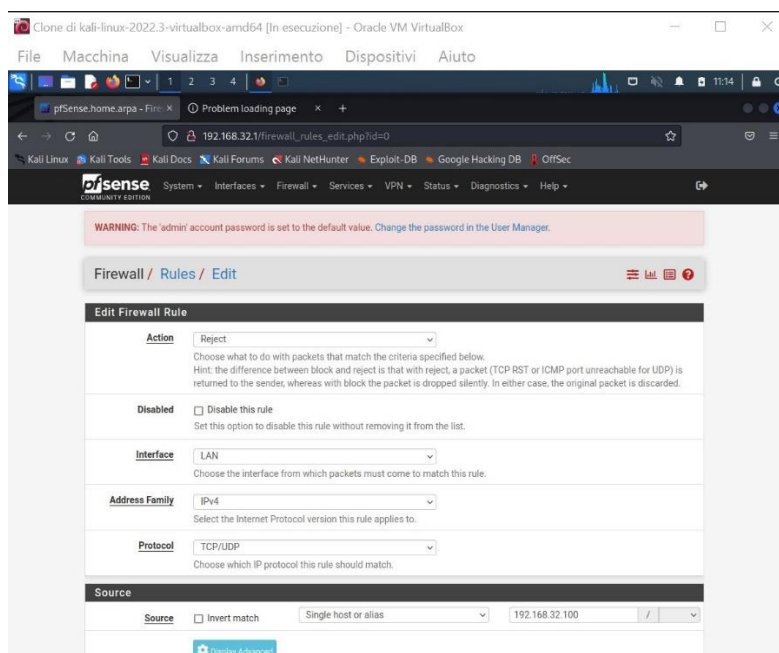
(kali@kali)~$ nmap 192.168.90.101
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-21 10:23 EST
Nmap scan report for 192.168.90.101
Host is up (0.0034s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    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:



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   /

**Destination Port Range**

From   To

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).

**Description**

A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

**Advanced Options** [Display Advanced](#)

**Rule Information**

Tracking ID	1669045546
Created	11/21/22 15:45:46 by admin@192.168.32.100 (Local Database)
Updated	11/21/22 15:48:35 by admin@192.168.32.100 (Local Database)

[Save](#)

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Firewall / Rules / LAN

The firewall rule configuration has been changed.  
The changes must be applied for them to take effect. [Apply Changes](#)

Floating WAN LAN OPT1

**Rules (Drag to Change Order)**

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/> 0 /630 KIB	*	*	*	LAN Address	80	*	*	*	Anti-Lockout Rule	<a href="#">Edit</a> <a href="#">Delete</a>
<input type="checkbox"/> 0 /120 B	IPv4 TCP/UDP	192.168.32.100	*	192.168.90.101	80 (HTTP)	*	none			<a href="#">Edit</a> <a href="#">Delete</a>
<input checked="" type="checkbox"/> 0 /867 KIB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	<a href="#">Edit</a> <a href="#">Delete</a>
<input type="checkbox"/> 0 /0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	<a href="#">Edit</a> <a href="#">Delete</a>

[Add](#) [Add](#) [Delete](#) [Save](#) [Separate](#)

```
(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=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)-[~]
$
```