

## CREARE REGOLA PER BLOCCARE SCAN

Qui sotto nella prima immagine, vediamo come sia possibile sia pingare che effettuare lo scan su Metasploitable (192.168.90.100):

```
File Actions Edit View Help
64 bytes from 192.168.90.100: icmp_seq=2 ttl=63 time=0.812 ms
64 bytes from 192.168.90.100: icmp_seq=3 ttl=63 time=1.30 ms
64 bytes from 192.168.90.100: icmp_seq=4 ttl=63 time=0.983 ms
64 bytes from 192.168.90.100: icmp_seq=5 ttl=63 time=0.806 ms
64 bytes from 192.168.90.100: icmp_seq=6 ttl=63 time=0.980 ms
64 bytes from 192.168.90.100: icmp_seq=7 ttl=63 time=0.955 ms
64 bytes from 192.168.90.100: icmp_seq=8 ttl=63 time=1.20 ms
64 bytes from 192.168.90.100: icmp_seq=9 ttl=63 time=1.34 ms
^Z
zsh: suspended ping 192.168.90.100

(kali㉿kali)-[~]
$ nmap 192.168.90.100 -sS
You requested a scan type which requires root privileges.
QUITTING!

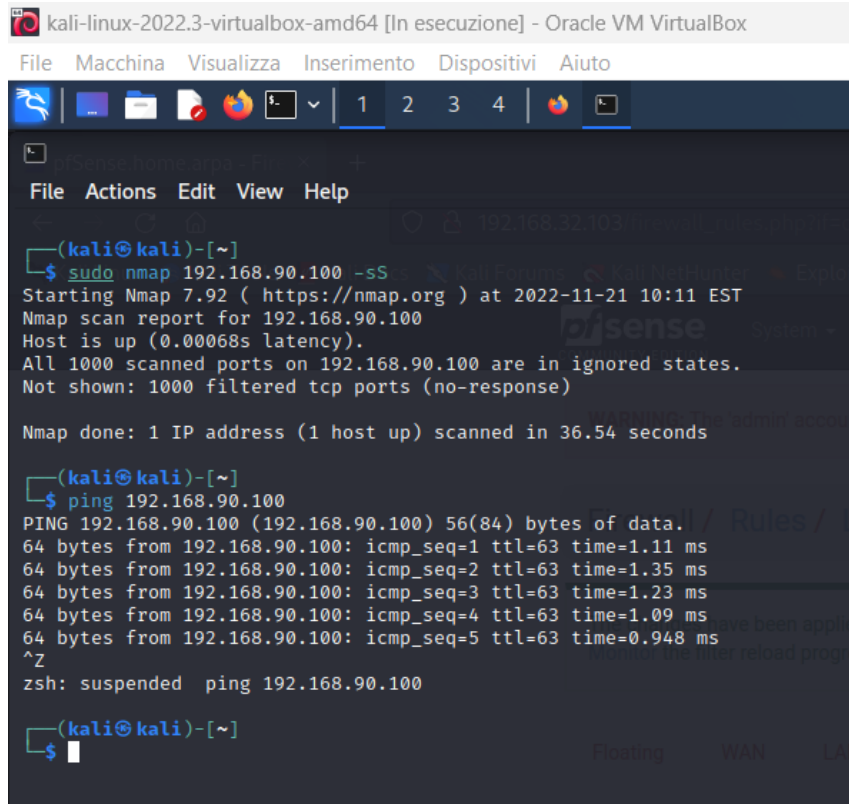
(kali㉿kali)-[~]
$ sudo nmap 192.168.90.100 -sS
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-21 09:46 EST
Nmap scan report for 192.168.90.100
Host is up (0.0014s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  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  ccproxy-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 13.40 seconds
```

Creiamo quindi una policy su PFSense tramite macchina virtuale Kali in questo modo:

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	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.		
Interface	LAN1		
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/UDP		
Choose which IP protocol this rule should match.			
Source			
Source	<input type="checkbox"/> Invert match	any	Source Address /
<input type="button" value="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	<input type="checkbox"/> Invert match	any	Destination Address /
Destination Port Range	any	any	
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			

Così facendo andiamo a bloccare solo i pacchetti TCP/UDP in arrivo dall'interfaccia LAN1, che in questo caso è Kali, lasciando passare tutti gli altri tipi di pacchetto, in modo tale da permettere ancora a Kali di pingare Metasploitable:



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

(kali㉿kali)-[~]
$ sudo nmap 192.168.90.100 -sS
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-21 10:11 EST
Nmap scan report for 192.168.90.100
Host is up (0.00068s latency).
All 1000 scanned ports on 192.168.90.100 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 36.54 seconds

(kali㉿kali)-[~]
$ ping 192.168.90.100
PING 192.168.90.100 (192.168.90.100) 56(84) bytes of data:
64 bytes from 192.168.90.100: icmp_seq=1 ttl=63 time=1.11 ms
64 bytes from 192.168.90.100: icmp_seq=2 ttl=63 time=1.35 ms
64 bytes from 192.168.90.100: icmp_seq=3 ttl=63 time=1.23 ms
64 bytes from 192.168.90.100: icmp_seq=4 ttl=63 time=1.09 ms
64 bytes from 192.168.90.100: icmp_seq=5 ttl=63 time=0.948 ms
^Z
zsh: suspended ping 192.168.90.100

(kali㉿kali)-[~]
$
```