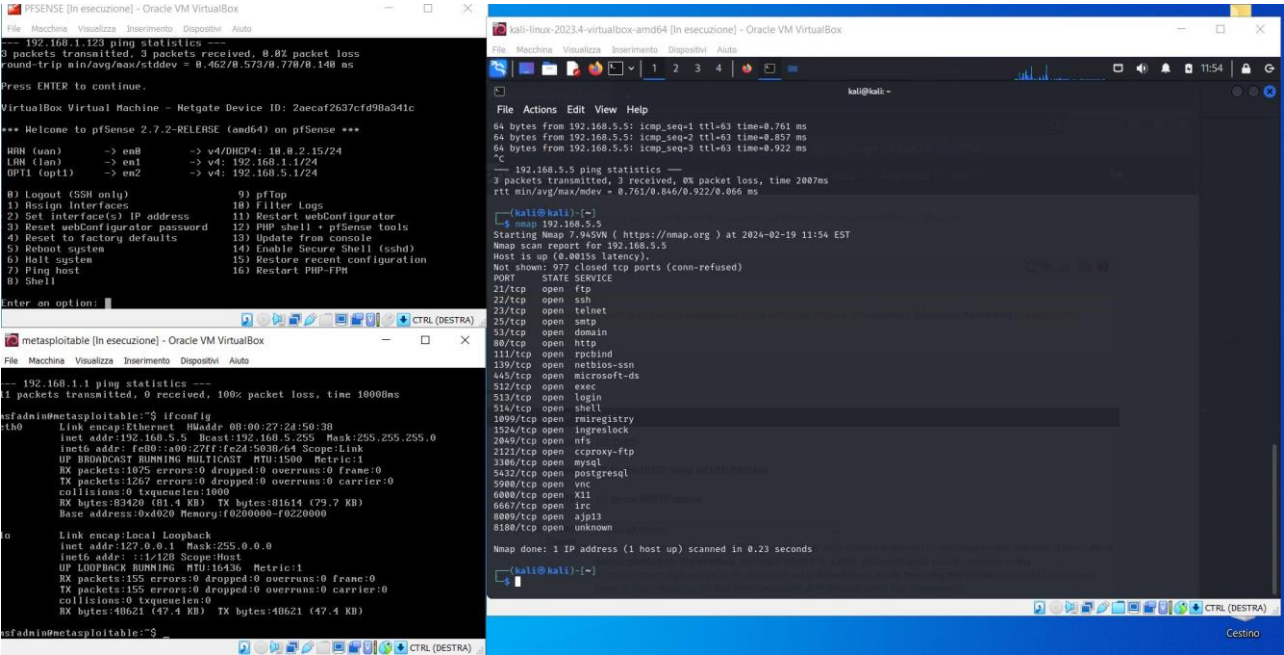


IP Kali Linux: 192.168.1.123
IP Metasploitable: 192.168.5.5
IP PFSense: 192.168.1.1 (LAN) 192.168.5.1 (OPT1)

Non impostando nessuna regola sul firewall di PFSense come si può ben vedere è possibile fare uno scan da Kali Linux senza problemi:



Invece, dopo aver applicato la seguente regola sul firewall:

Firewall / Rules / LAN

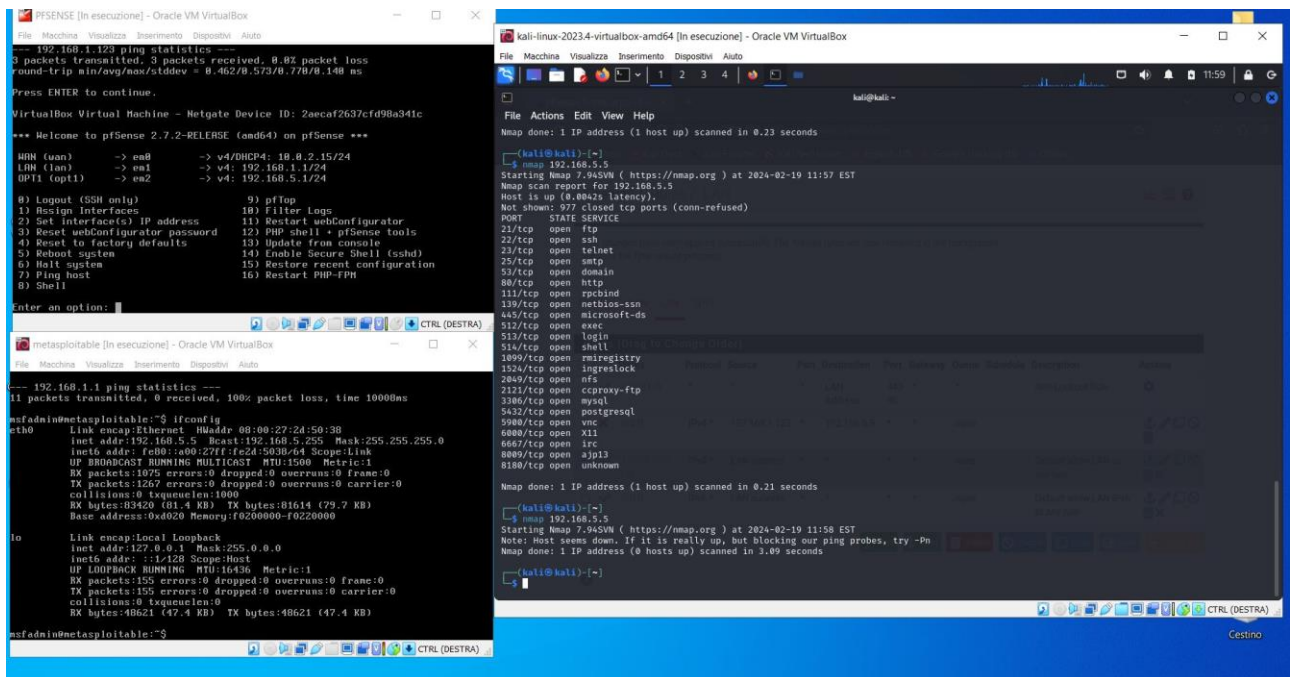
The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.

Floating WAN LAN OPT1

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 1/929 KiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	⚙️
<input type="checkbox"/>	✗ 0/0 B	IPv4 *	192.168.1.123	*	192.168.5.5	*	*	none			🔗 ✎️ 🗑️ 🚫
<input checked="" type="checkbox"/>	✓ 1.003K/507 KiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	🔗 ✎️ 🗑️ 🚫
<input type="checkbox"/>	✓ 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	🔗 ✎️ 🗑️ 🚫

Add Add Delete Toggle Copy Save Separator

la scansione viene bloccata con successo dal firewall:



Forzando lo scan con nmap -Pn vediamo che la macchina Metasploitable è effettivamente attiva ma ci viene bloccata la connessione con essa per via del firewall:

```
(kali@kali)-[~]
$ nmap -Pn 192.168.5.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-19 12:13 EST
Nmap scan report for 192.168.5.5
Host is up.
All 1000 scanned ports on 192.168.5.5 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 203.86 seconds

(kali@kali)-[~]
$
```