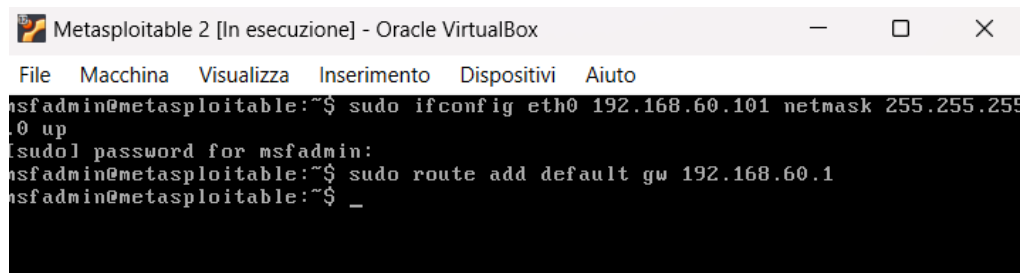


PROGETTOS3L5:

1. **ESERCIZIO:** creare una regola firewall che blocchi l'accesso alla DVWA (su metasploitable) dalla macchina Kali Linux e ne impedisca di conseguenza lo scan. Un requisito fondamentale dell'esercizio è che le macchine Kali e Metasploitable siano su reti diverse, potete aggiungere una nuova interfaccia di rete a Pfsense in modo tale da gestire una ulteriore rete. Connettetevi poi in Web Gui per attivare la nuova interfaccia e configurarla.

- Impostare **manualmente l'indirizzo IP** sulla macchina Metasploitable in modo temporaneo (si resetta al riavvio):

- Una volta loggato, ho eseguito i seguenti comandi per assegnare l'indirizzo IP e gateway(pfSense):
 - `sudo ifconfig eth0 192.168.60.101 netmask 255.255.255.0 up`
 - `sudo route add default gw 192.168.60.1`



```
Metasploitable 2 [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
msfadmin@metasploitable:~$ sudo ifconfig eth0 192.168.60.101 netmask 255.255.255.0 up
msfadmin@metasploitable:~$ sudo! password for msfadmin:
msfadmin@metasploitable:~$ sudo route add default gw 192.168.60.1
msfadmin@metasploitable:~$ _
```

- Su PfSense, dopo essere entrato in <http://192.168.50.1/> ed effettuato il login, ho aggiunto e modificato le interfacce di rete in questo modo:
 - L'interfaccia **LAN** la ho soprannominata, per semplicità mia, **Kali**;
 - Ho aggiunto una nuova interfaccia chiamata METASPLOITABLE con le seguenti configurazioni:
 - Enable: yes
 - Description: METASPLOITABLE
 - IPv4 Configuration Type: Static IPv4

- IPv4 Address: 192.168.60.1/24

Static IPv4 Configuration

IPv4 Address: 192.168.60.1 / 24

IPv4 Upstream gateway: None [+ Add a new gateway](#)

If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the 'Add' button.
On local area network interfaces the upstream gateway should be "none".
Selecting an upstream gateway causes the firewall to treat this interface as a **WAN type interface**.
Gateways can be managed by [clicking here](#).

pfSense COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Interfaces / **METASPLOITABLE (em0)**

General Configuration

Enable ☒ Enable interface

Description METASPLOITABLE
Enter a description (name) for the interface here.

IPv4 Configuration Type Static IPv4

IPv6 Configuration Type None

MAC Address xxxxxxxxxxxx
This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xxxxxxxxxxxx or leave blank.

MTU
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Speed and Duplex Default (no preference, typically autoselect)
Explicitly set speed and duplex mode for this interface

192.168.50.1/interfaces.php?if=opt1#

- Su Firewall>Rules ho aggiunto una regola firewall per far riuscire a comunicare Metasploitable con Pfsense, le configurazioni sono:
 - Action: Pass
 - Interface: METASPLOITABLE
 - Address Family: IPv4
 - Protocol: any (ho scoperto che non riuscivo a pingare da metasploitable a Pfsense perchè non rilevava IP protocol ICMP)
 - Source: METASPLOITABLE Subnets
 - Destinatio: any

Firewall / Rules / **Edit**

Edit Firewall Rule

Action Pass
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 ☐ Disable this rule
Set this option to disable this rule without removing it from the list.

Interface METASPLOITABLE
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 Any
Choose which IP protocol this rule should match.

Source

Source ☐ Invert match METASPLOITABLE subnets Source Address /

Destination

Destination ☐ Invert match Any Destination Address /

Infine, sulla macchina metasploitable ho cercato di pingare PFsense con questo comando:

- ping 192.168.60.1

```
msfadmin@metasploitable:~$ ping 192.168.60.1
PING 192.168.60.1 (192.168.60.1) 56(84) bytes of data:
64 bytes from 192.168.60.1: icmp_seq=1 ttl=64 time=0.227 ms
64 bytes from 192.168.60.1: icmp_seq=2 ttl=64 time=0.202 ms
64 bytes from 192.168.60.1: icmp_seq=3 ttl=64 time=0.052 ms
64 bytes from 192.168.60.1: icmp_seq=4 ttl=64 time=0.232 ms
64 bytes from 192.168.60.1: icmp_seq=5 ttl=64 time=0.290 ms
64 bytes from 192.168.60.1: icmp_seq=6 ttl=64 time=0.249 ms

--- 192.168.60.1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 4995ms
rtt min/avg/max/mdev = 0.052/0.208/0.290/0.076 ms
msfadmin@metasploitable:~$
```

- Ho creato una regola firewall che blocchi l'accesso alla DVWA (su metasploitable) dalla macchina Kali Linux e ne impedisca di conseguenza lo scan:

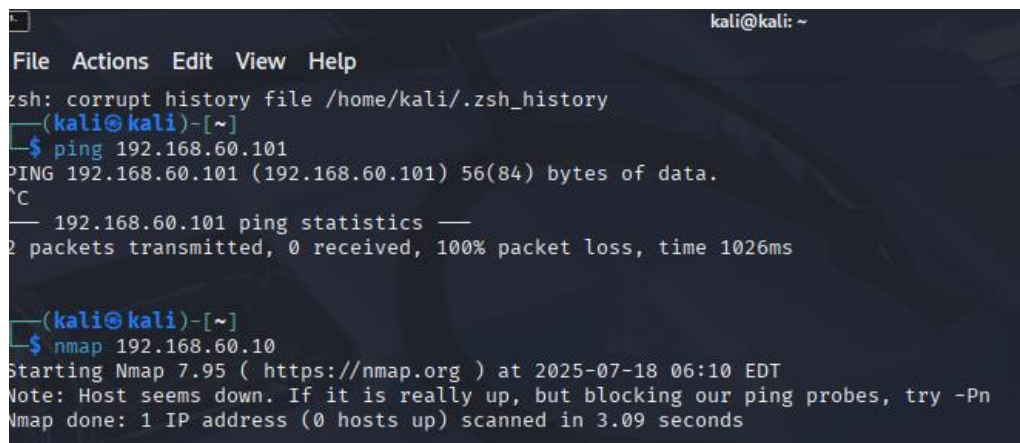
- Su Firewall>Rules>Kali ho aggiunto una regola firewall configurata in questo modo:
 - Action: Block
 - Interface: Kali
 - Address Family: IPv4
 - Protocol: Any
 - Source: Kali subnets
 - Destination: Address > 192.168.60.101

The screenshot shows the pfSense web interface for editing a firewall rule. The breadcrumb navigation is 'Firewall / Rules / Edit'. The rule is named 'Kali'. The configuration is as follows:

- Action:** Block (dropdown menu)
- Disabled:** ☐ Disable this rule. 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.
- Interface:** KALI (dropdown menu). Choose the interface from which packets must come to match this rule.
- Address Family:** IPv4 (dropdown menu). Select the Internet Protocol version this rule applies to.
- Protocol:** Any (dropdown menu). Choose which IP protocol this rule should match.
- Source:** ☐ Invert match. KALI subnets (dropdown menu). Source Address: / (dropdown menu).
- Destination:** ☐ Invert match. Address or Alias (dropdown menu). 192.168.60.101 (dropdown menu).

- Quindi facendo lo scan Kali non riuscirà a collegarsi con Metasploitable:

- nmap 192.168.60.101



```
kali@kali: ~  
File Actions Edit View Help  
zsh: corrupt history file /home/kali/.zsh_history  
(kali@kali)-[~]  
$ ping 192.168.60.101  
PING 192.168.60.101 (192.168.60.101) 56(84) bytes of data.  
^C  
--- 192.168.60.101 ping statistics ---  
2 packets transmitted, 0 received, 100% packet loss, time 1026ms  
  
(kali@kali)-[~]  
$ nmap 192.168.60.10  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-18 06:10 EDT  
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn  
Nmap done: 1 IP address (0 hosts up) scanned in 3.09 seconds
```

- **Considerazioni finali:**

- Cosa ho imparato con questo esercizio:
 - Separazione delle reti = Sicurezza:
 - Separare dispositivi su reti diverse è una buona pratica di sicurezza: limita i danni in caso di compromissione e consente una gestione più granulare del traffico.
 - Il firewall come punto di controllo centrale:
 - pfSense, agendo da firewall tra Kali e Metasploitable, ti permette di controllare e filtrare il traffico in modo centralizzato, invece di affidarti alla configurazione locale delle macchine
 - Regole precise = maggiore controllo
 - Impedire lo scan e l'accesso a DVWA
 - Simulazione realistica di un attacco:
 - Questa configurazione simula un contesto realistico di un attaccante (Kali) che tenta di accedere a un'app vulnerabile in un'altra rete. Questo è uno degli scenari classici in penetration testing.