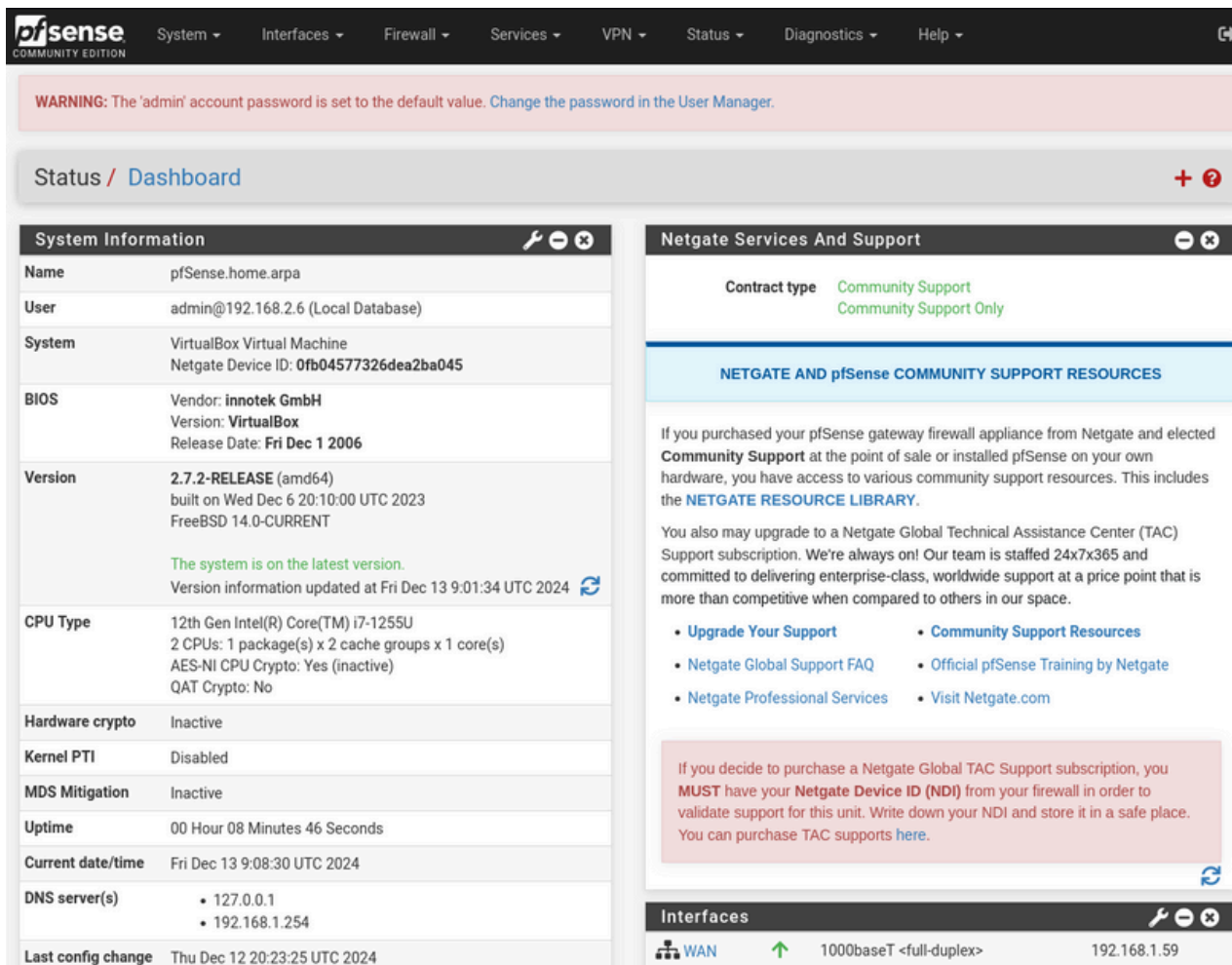
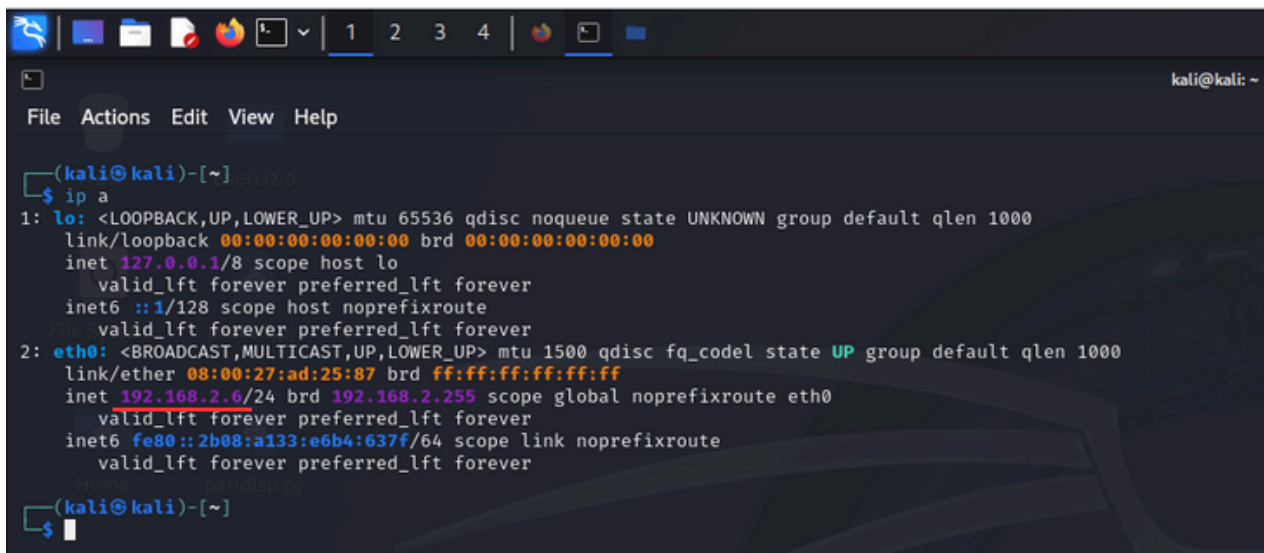


Progetto S3/L5

Il progetto di oggi richiede la creazione di una regola firewall che blocchi l'accesso alla DVWA (su metasploitable) dalla macchina Kali Linux e ne impedisca di conseguenza lo scan. Kali e Metasploitable devono essere su reti diverse. Innanzitutto l'interfaccia generale di pfsense si presenta così



Per proseguire con la creazione della regola bisogna tenere a mente i 2 indirizzi IP delle macchine, per esempio Kali ha come IP **192.168.2.6**



```
(kali@kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:ad:25:87 brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.6/24 brd 192.168.2.255 scope global noprefixroute eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::2b08:a133:e6b4:637f/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Metasploitable invece ha come IP **192.168.1.62**, dunque i 2 IP sono su 2 reti diverse

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:d5:a5:c9
          inet addr:192.168.1.62  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: 2001:b07:6473:e463:a00:27ff:fed5:a5c9/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fed5:a5c9/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:47 errors:0 dropped:0 overruns:0 frame:0
          TX packets:65 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5080 (4.9 KB)  TX bytes:6898 (6.7 KB)
          Base address:0xd020  Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:91 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$
```

A questo punto, andando su Firewall/Rules/Edit bisogna inserire i dati di connessione di che il firewall ha bisogno di conoscere per bloccare la comunicazione. Quindi come azione si inserisce “**Blocca**”, e poi gli IP di sorgente e di destinazione, assieme agli altri settaggi

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

Firewall / Rules / Edit

Edit Firewall Rule

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	LAN 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	<input type="checkbox"/> Invert match Address or Alias 192.168.2.6 / ▼

Destination	
Destination	<input type="checkbox"/> Invert match Address or Alias 192.168.1.62 / ▼

Infine, bisogna salvare le impostazioni e cliccare sul pulsante Apply Changes, così facendo bloccheremo le comunicazioni da Kali a Metasploitable, e di conseguenza Kali non potrà eseguire lo scan sulla DVWA.

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**

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 1/726 KiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	⚙️
<input type="checkbox"/>	✗ 0/0 B	IPv4 *	192.168.2.6	*	192.168.1.62	*	*	none			📌 ⚙️ 🗑️ ⏏️
<input type="checkbox"/>	✓ 0/1 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

Bonus:

L'esercizio bonus, richiedeva invece la creazione di una regola che bloccasse il Telnet da Kali a Metasploitable, siccome Telnet utilizza il protocollo TCP sulla porta 23, occorreva impostarlo come si vede in figura

Edit Firewall Rule

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

Interface LAN
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
Choose which IP protocol this rule should match.

Source

Source ☐ Invert match Address or Alias 192.168.2.6 /

⚙️ 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 ☐ Invert match Address or Alias 192.168.1.62 /

Destination Port Range Telnet (23) 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.