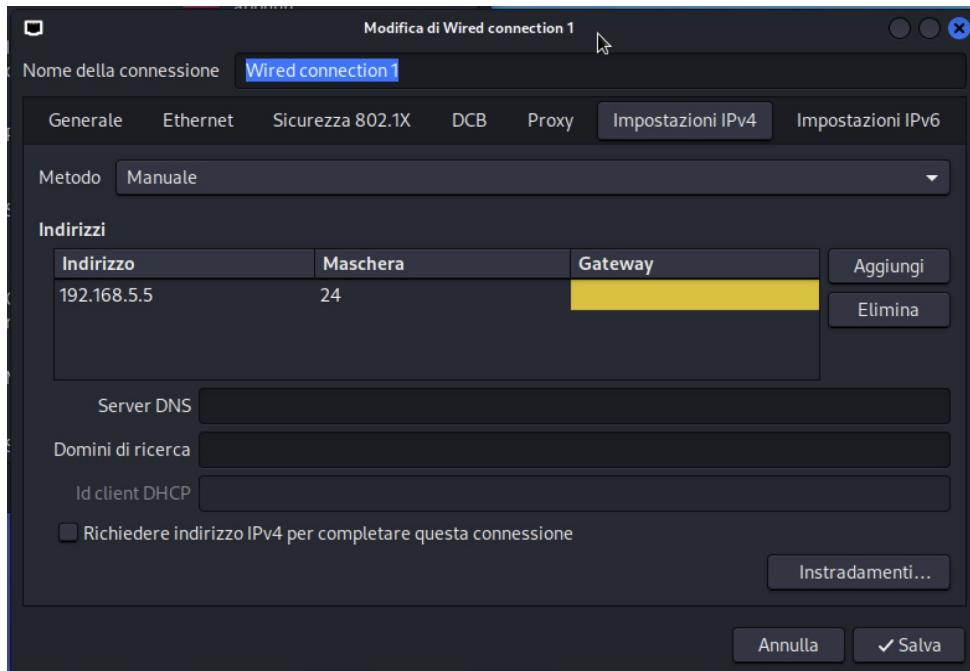


La traccia di oggi verteva sul creare una regola Firewall, tramite Pfsense, per bloccare l'accesso DVWA da Metasploitable2 a Kali Linux, e di conseguenza che ne blocchi anche la scansione. Il tutto lavorando su VM

Un Firewall è un componente hardware e/o software che serve a controllare il traffico di una rete sia in entrata che in uscita, usato principalmente per bloccare eventuali malware sia in entrata, appunto, che in uscita

Come prima cosa impostiamo un indirizzo IPv4 da usare come test, questo lo facciamo su Kali



Utilizziamo il 192.168.5.5

Ora configuriamo questo indirizzo anche su Pfsense in VM, cambiamo l'ultimo ottetto, quindi 192.168.5.6

```

0) Logout (SSH only)
1) Assign Interfaces
2) Set interface(s) IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell

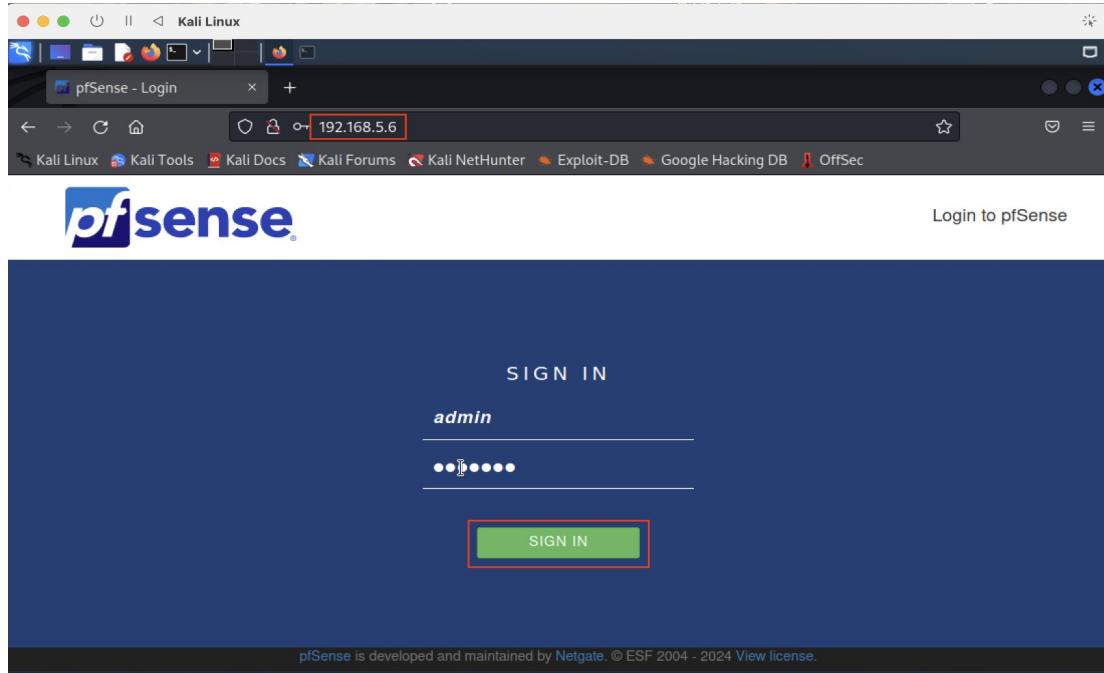
Enter an option: 2

Available interfaces:
1 - WAN (re0 - dhcp)
2 - LAN (em0 - static)

Enter the number of the interface you wish to configure: 2
Configure IPv4 address LAN interface via DHCP? (y/n) n
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.5.6
  
```

Quindi apriamo Pfsense su VM, e gli diamo il comando 2 per configurare l'IP

Una volta configurato, inseriamo questo indirizzo sul browser di Firefox da Kali, per accedere alla configura PfSense



Clicchiamo su “Signi In” per eseguire il log-in

Una volta entrati dobbiamo andare sulla scheda dedita alla creazione delle regole per i Firewall

A screenshot of the pfSense web interface. The top navigation bar includes links for System, Interfaces, Firewall (which is currently selected and highlighted in red), Services, VPN, Status, Diagnostics, and Help. Below the navigation bar, there's a warning message: "WARNING: The 'admin' account password is...". A sidebar on the left contains links for Status / Dashboard and System Information. The main content area shows a "Firewall / Rules / WAN" header. A dropdown menu for the Firewall tab is open, listing options: Aliases, NAT, Rules (which is highlighted with a red box), Schedules, Traffic Shaper, and Virtual IPs. To the right of the dropdown, a note says "Change the password in the User Manager." At the bottom of the screen, there's a "Netgate Services And Support" link.

Andiamo alla voce del menù in alto “Firewall” e clicchiamo su “Rules”

Ora clicchiamo alla voce “Lan”



Ora clicchiamo sul pulsante in verde “Add” per iniziare a creare una regola Firewall da utilizzare

The screenshot shows the pfSense Firewall Rules LAN page. At the top, there's a warning message: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below the header, the URL is "Firewall / Rules / LAN". Underneath, there are tabs for "Floating", "WAN", and "LAN", with "LAN" being the active tab. The main area is titled "Rules (Drag to Change Order)" and contains a table with three existing rules. At the bottom of the table is a toolbar with several buttons: "Add" (highlighted with a red box), "Delete", "Toggle", "Copy", "Save", and "Separator".

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 6/1.83 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
□ ✓ 0/468 B	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
□ ✓ 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Bene ora possiamo impostare i vari parametri per creare la regola

La voce “Action” la impostiamo su “block”, perché il nostro obiettivo è appunto quello di bloccare l’accesso da Metasploitable2 su Kali

Interface mettiamo “Lan”, address family mettiamo “IPv4” e su protocol mettiamo “Any”

The screenshot shows the "Edit Firewall Rule" configuration page. At the top, it says "Edit Firewall Rule". Below that, there's a section for "Action" with a dropdown menu set to "Block". A note below explains the difference between "block" and "reject": "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." Further down, there are sections for "Interface" (set to "LAN"), "Address Family" (set to "IPv4"), and "Protocol" (set to "Any"). Each section has a descriptive note below it.

Ora proseguiamo con le altre impostazioni

Bisogna inserire gli IP di “Source” e “Destination”. Nel primo inseriamo l’IP di Metasploitable2 e nel secondo quello di Kali che abbiamo creato noi all’inizio dell’esercizio, ovvero 192.168.5.5

Source

<u>Source</u>	<input type="checkbox"/> Invert match	Address or Alias	192.168.1.39	/	▼
---------------	---------------------------------------	------------------	--------------	---	---

Destination

<u>Destination</u>	<input type="checkbox"/> Invert match	Address or Alias	192.168.5.5	/	▼
--------------------	---------------------------------------	------------------	-------------	---	---

Bene ora clicchiamo su “Save” e applichiamo le modifiche



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

Ora verifichiamo che il ping non arrivi a destinazione, ovvero che il Firewall non permetta la comunicazione tra Kali e Metasploitable2

```
(kali㉿kali)-[~]
$ ping 192.168.1.39
PING 192.168.1.39 (192.168.1.39) 56(84) bytes of data.
64 bytes from 192.168.1.39: icmp_seq=1 ttl=63 time=1.51 ms
64 bytes from 192.168.1.39: icmp_seq=2 ttl=63 time=1.81 ms
```

Purtroppo, come possiamo vedere, dopo aver impostato tutte le configurazioni non sono riuscito a bloccare il traffico tra le due macchine virtuali

