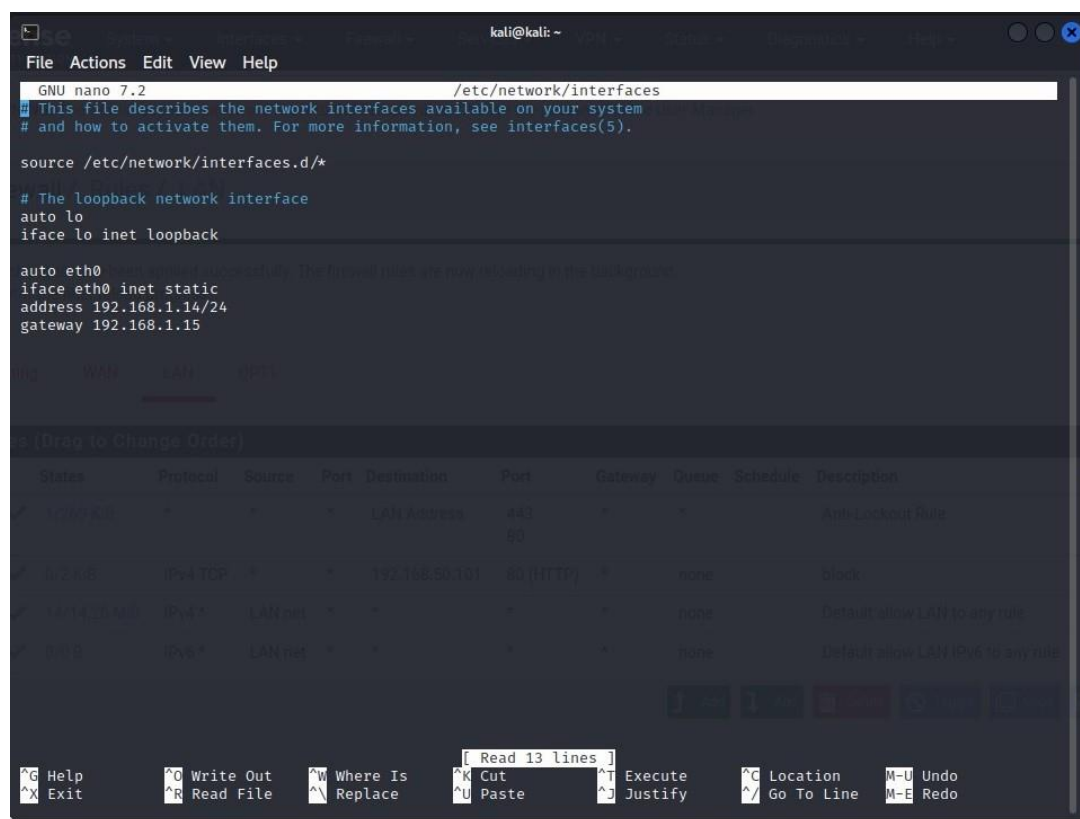


# Esercizio 23/10/2023

Nell'esercizio odierno ci veniva richiesto di creare una regola sul firewall (PfSense) che bloccasse l'accesso alla pagina DVWA di Metasploitable.

Prima di tutto sono andata a cambiare l'indirizzo ip di kali, estrapolando dal prompt dei comandi come base e modificando solo gli ultimi numeri

Poi ho modificato i parametri su kali con il comando "sudo nano /etc/network/interfaces"



```
GNU nano 7.2 /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

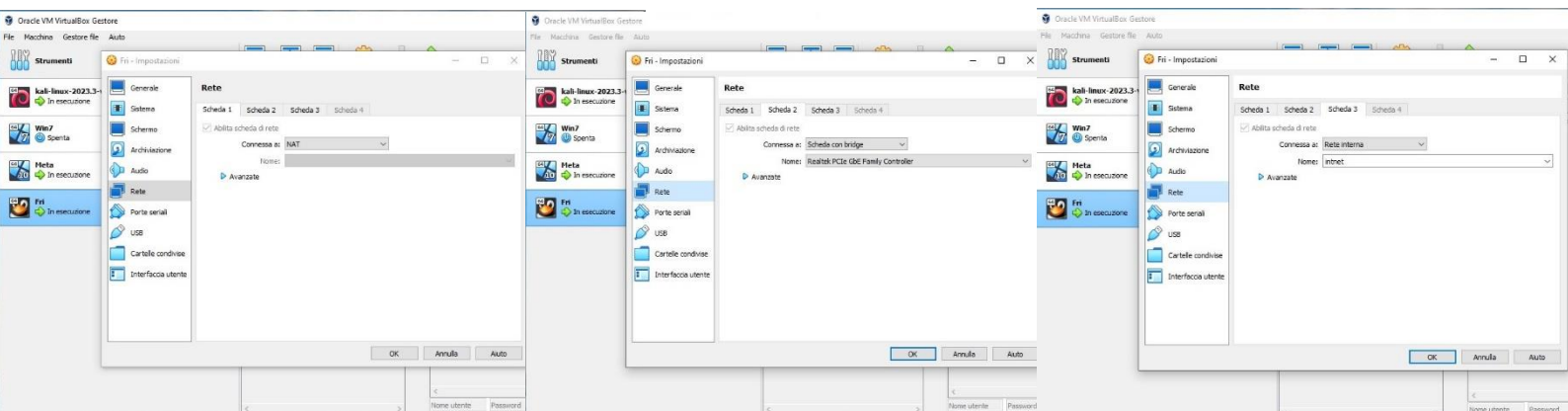
source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

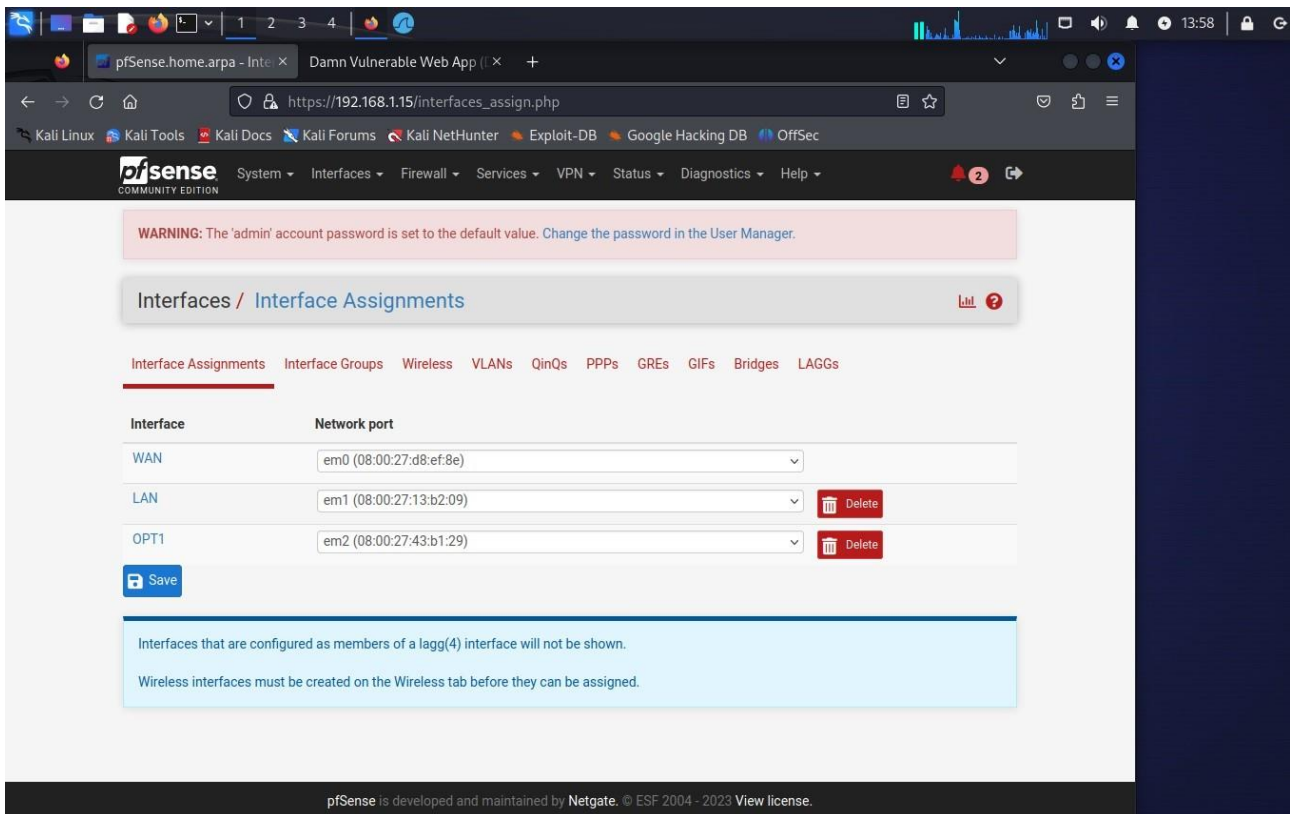
# The ethernet network interface
auto eth0
iface eth0 inet static
address 192.168.1.14/24
gateway 192.168.1.15
```

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
ACCEPT	*	*	*	LAN Address	443	*	*	*	Auto-Loopback Rule
REJECT	IPV4 TCP	*	*	192.168.50.101	80 (HTTP)	*	none	*	block
ACCEPT	IPV4 *	LAN ip	*	*	*	*	none	*	Default allow LAN to any rule
ACCEPT	IPV6 *	LAN ip	*	*	*	*	none	*	Default allow LAN IPV6 to any rule

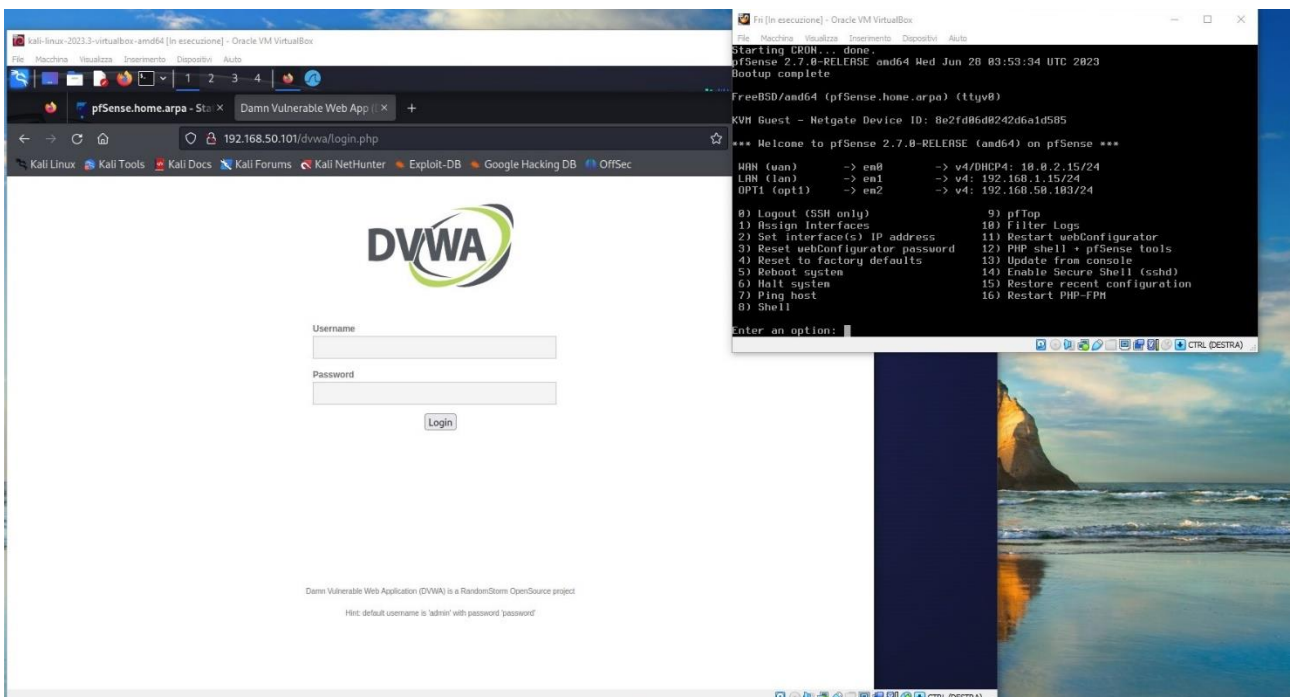
Sono andata a creare la terza rete sul Firewall (la prima NAT, la seconda Bridge e la terza interna)



Sono andata sul programma PfSense per attivare la terza rete



Quindi ho configurato la rete sulla macchina virtuale e ho provato l'accesso a DVWA (inserendo i parametri del Gateway)



A questo punto sono tornata su PfSense e ho creato la regola di blocco per Metasploitable e l'ho inserita nella prima riga disponibile salvando le impostazioni

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

any

Source Address

/

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

Single host or alias

192.168.50.101

/

Destination Port Range

HTTP (80)

From

Custom

HTTP (80)

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

Log

☐ Log packets that are handled by this rule

pfSense

COMMUNITY EDITION

System

Interfaces

Firewall

Services

VPN

Status

Diagnostics

Help

2

WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

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"/>	✓ 1/108 KiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✗ 0/0 B	IPv4 TCP	*	*	192.168.50.101	80 (HTTP)	*	none		block	
<input type="checkbox"/>	✓ 19/4.48 MiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	✓ 0/0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

↑ Add

↓ Add

🗑 Delete

🔄 Toggle

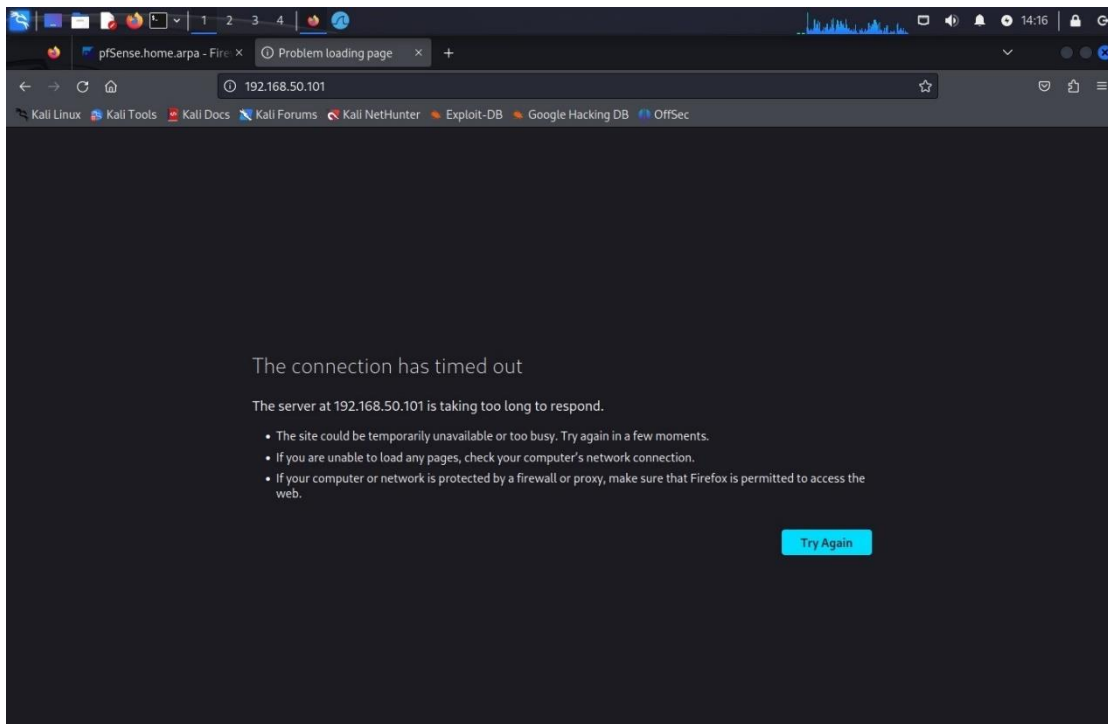
📄 Copy

💾 Save

⚡ Separator

i

Quindi sono andata a fare la prova sul web per controllare che il sito fosse davvero bloccato



Ho fatto la contro prova con il l'action "Pass"

