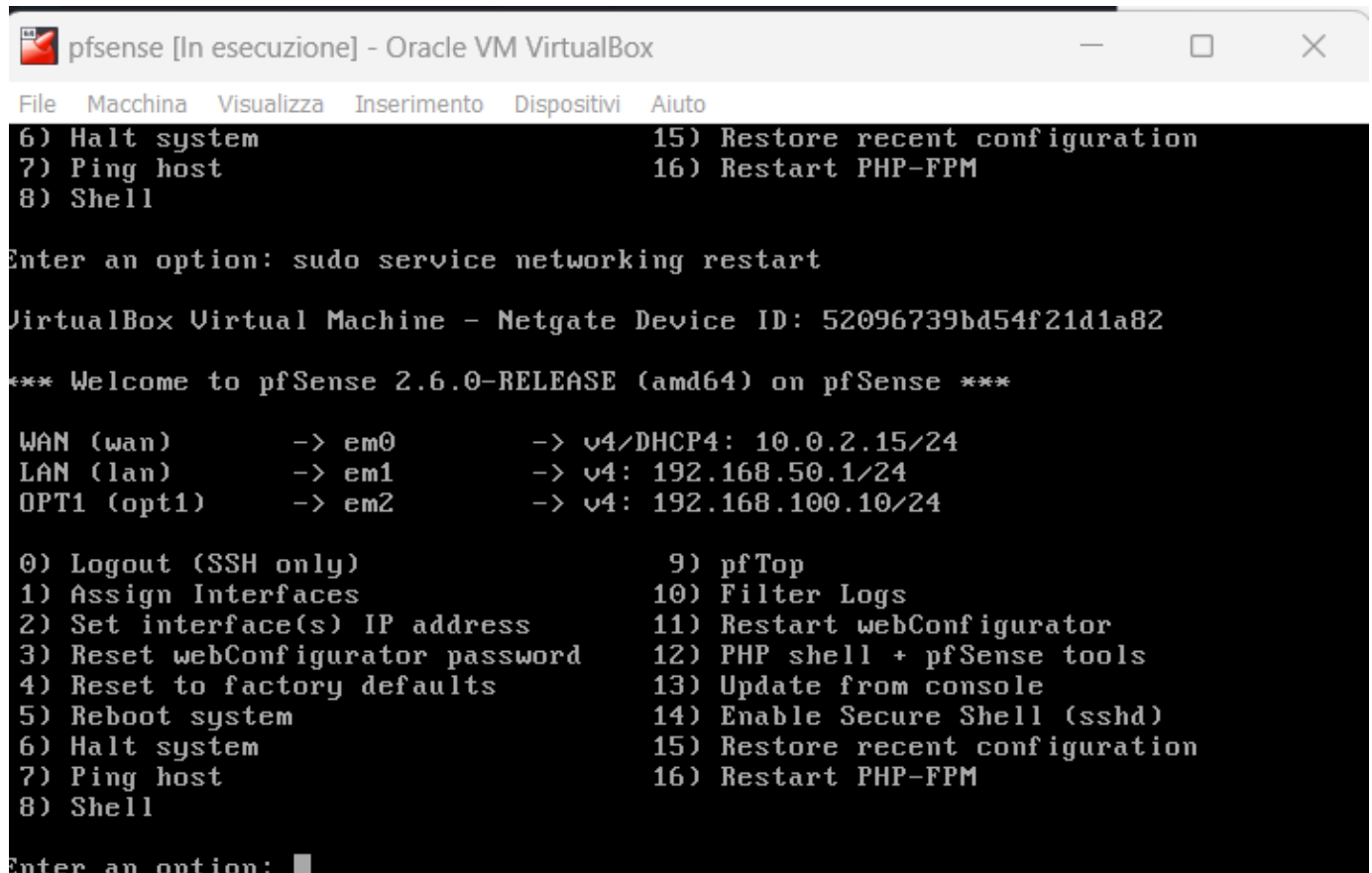


FIREWALL CON PFSENSE

- Ho settato l'ip della lan em1 in 192.168.50.1.
- Ho creato una seconda lan opt1 (em2) a cui ho assegnato IP 192.168.100.10, ergo su rete diversa da Kali.



```
pfsense [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
6) Halt system          15) Restore recent configuration
7) Ping host            16) Restart PHP-FPM
8) Shell

Enter an option: sudo service networking restart

VirtualBox Virtual Machine - Netgate Device ID: 52096739bd54f21d1a82

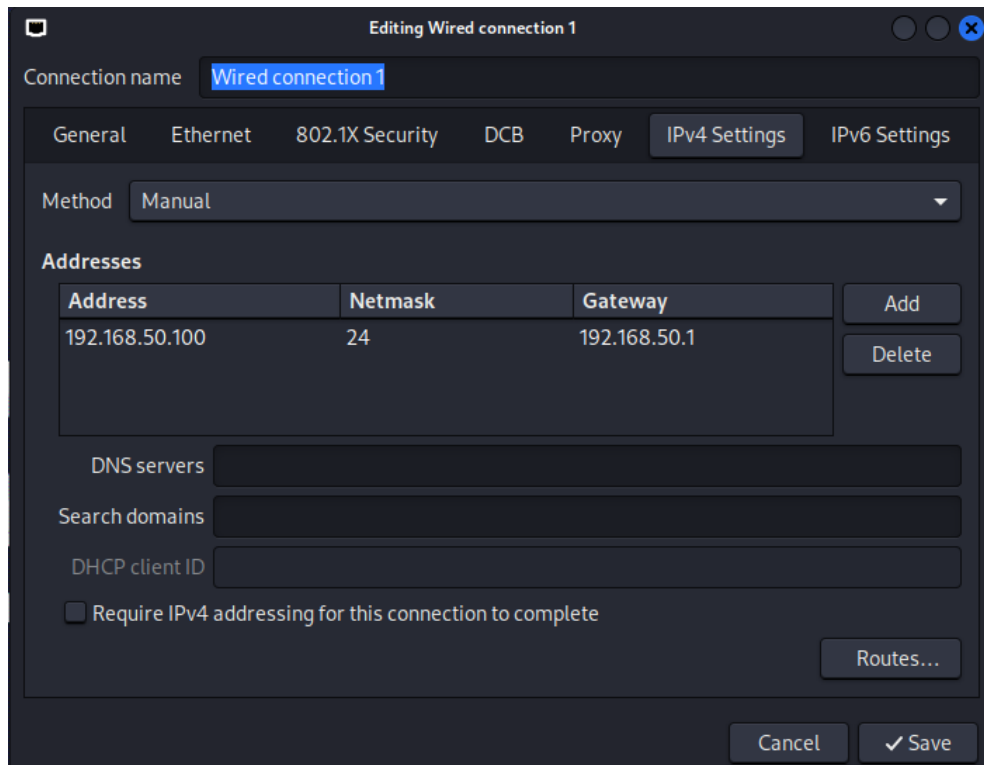
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
LAN (lan)      -> em1      -> v4: 192.168.50.1/24
OPT1 (opt1)    -> em2      -> v4: 192.168.100.10/24

0) Logout (SSH only)    9) pfTop
1) Assign Interfaces    10) Filter Logs
2) Set interface(s) IP address  11) Restart webConfigurator
3) Reset webConfigurator password  12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system        14) Enable Secure Shell (sshd)
6) Halt system          15) Restore recent configuration
7) Ping host            16) Restart PHP-FPM
8) Shell

Enter an option: █
```

- Ho impostato come gateway della macchina Kali Linux (IP 192.168.50.100).



Ho assegnato l'IP di tale rete al gateway di Metasploitable.

```

meta [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
GNU nano 2.0.7 File: /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

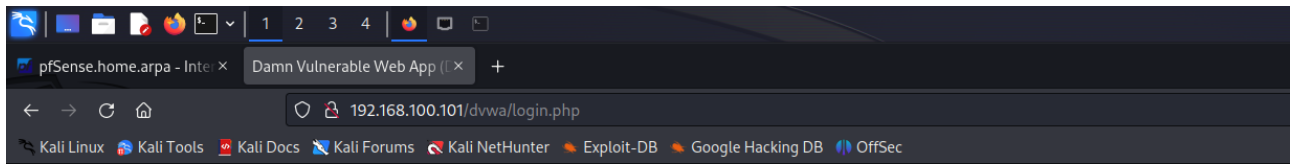
# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.100.101
netmask 255.255.255.0
network 192.168.100.0
broadcast 192.168.100.255
gateway 192.168.100.10

[ Wrote 16 lines ]
msfadmin@metasploitable:~$

```

- In questo modo ho avuto accesso alla pagina DVWA di Metasploitable



Username

Password

Login

Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project

Hint: default username is 'admin' with password 'password'

- Ho effettuato uno scan nmap -sS su IP di Metasploitable, riuscito tranquillamente.

```
(kali@kali)-[~]
$ sudo nmap -sS 192.168.100.101
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-29 10:18 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid serv
Nmap scan report for 192.168.100.101
Host is up (0.013s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.81 seconds
```

- Ho impostato un firewall per bloccare l'accesso di Kali Linux sul DVWA di Metasploitable

https://192.168.50.1/firewall_rules.php?if=opt1

Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

pfSense COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

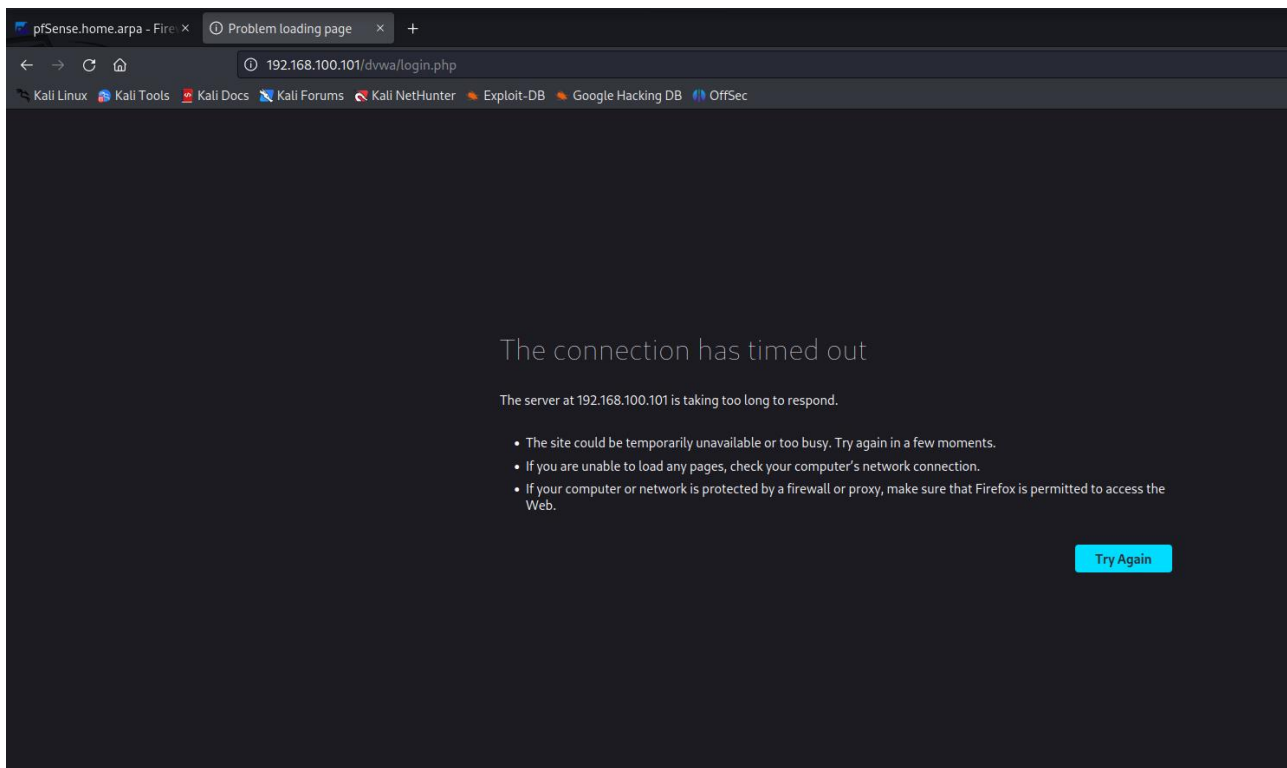
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Firewall / Rules / OPT1

Floating WAN LAN OPT1

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/>	0/0 B	IPv4 TCP	192.168.50.100	*	192.168.100.101	*	*	none		Add Edit Delete Save Separator

- Dopo aver impostato il firewall, da Kali non riuscivo a connettermi sulla DVWA di Metasploitable



- Dopo aver impostato il firewall ho provato a rifare lo scan nmap -sS sull'indirizzo IP di Metasploitable, senza risultato.

```
(kali㉿kali)-[~]
$ sudo nmap -sS 192.168.100.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-29 10:36 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify
Stats: 0:00:18 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 83.65% done; ETC: 10:36 (0:00:04 remaining)
Nmap scan report for 192.168.100.101
Host is up (0.015s latency).
All 1000 scanned ports on 192.168.100.101 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 21.39 seconds

(kali㉿kali)-[~]
$
```