

## Progetto S3/L5

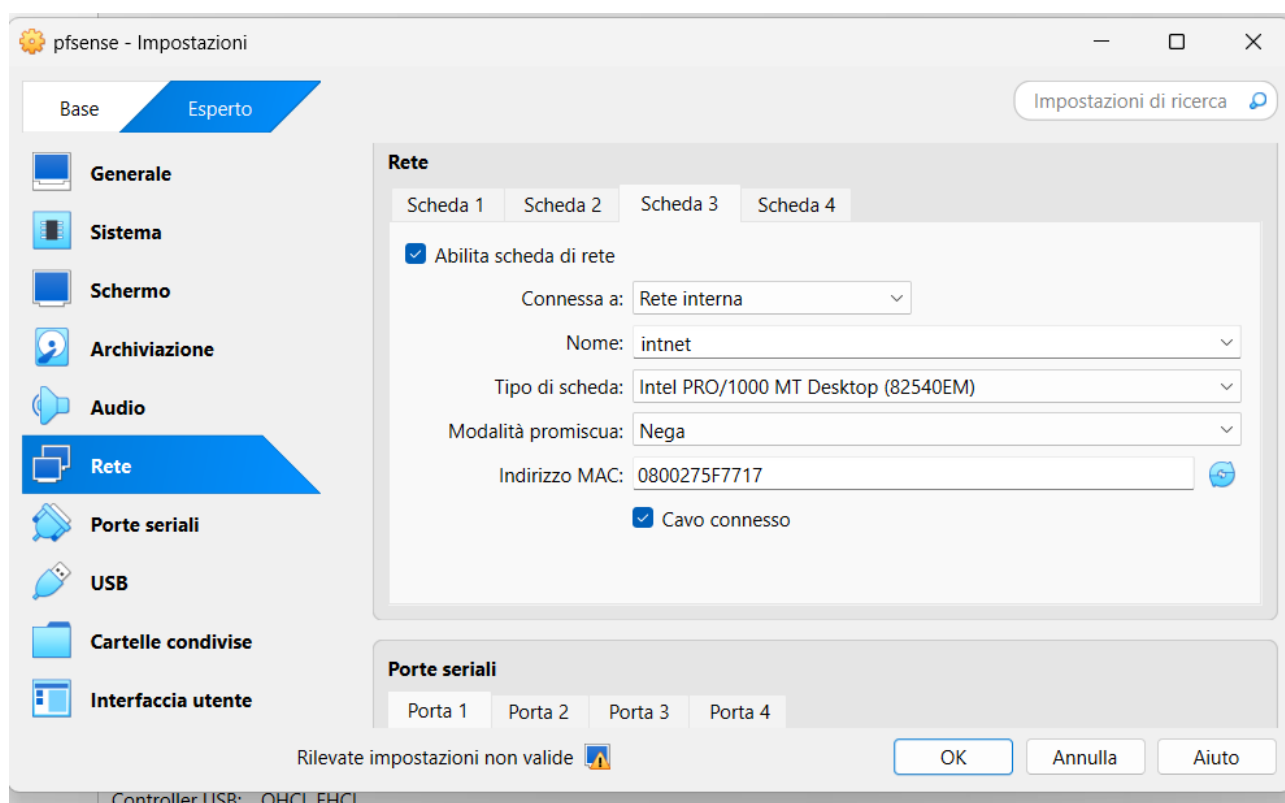
### Creazione policy Pfsense

Sulla base di quanto illustrato, 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.

### Svolgimento:

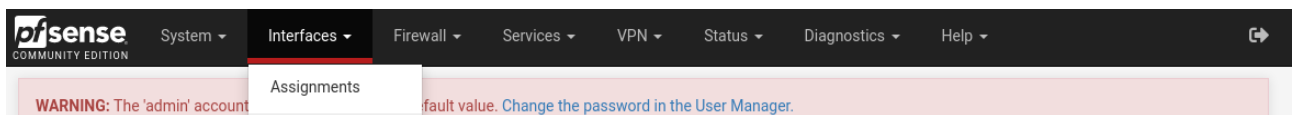
Anzitutto, aggiungo una nuova interfaccia di rete a Pfsense. Dal gestore Oracle VirtualBox modico le impostazioni di rete, aggiungendo la Scheda 3, con connessione alla rete interna, come già preimpostato per la Scheda 2.



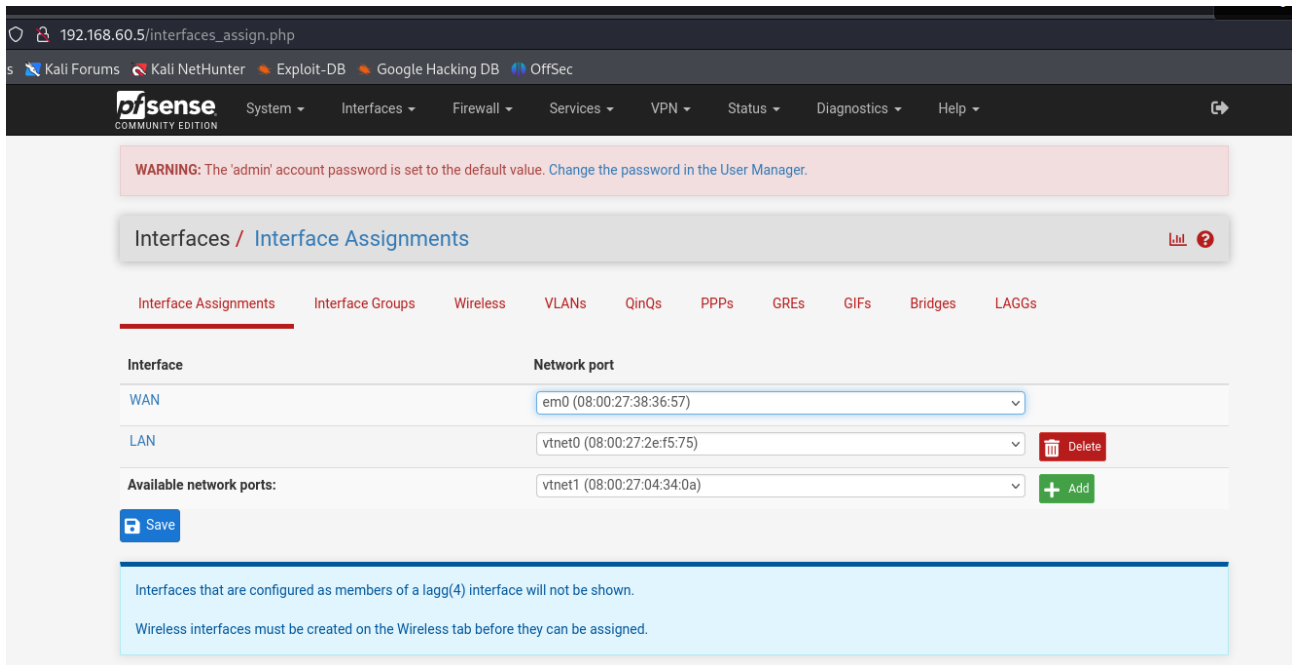
L'impostazione complessiva quindi è:

Rete
Scheda 1: Intel PRO/1000 T Server (NAT)
Scheda 2: Rete paravirtualizzata (Rete interna, 'intnet')
Scheda 3: Rete paravirtualizzata (Rete interna, 'intnet')

Poi, mi connetto in web GUI, accedendo a Pfsense. Tramite “Interfaces”, poi “Assignments” :



Ora aggiungo una nuova interfaccia, cliccando su “+ Add”:



Chiamo l’interfaccia LAN2 e imposto l’IPv4 statico 192.168.50.5.

Enable	<input checked="" type="checkbox"/> Enable interface
Description	<input type="text" value="LAN2"/> Enter a description (name) for the interface here.
IPv4 Configuration Type	<input type="text" value="Static IPv4"/>
IPv6 Configuration Type	<input type="text" value="None"/>
MAC Address	<input type="text" value="xx:xx:xx:xx:xx:xx"/> This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.
MTU	<input type="text" value=""/> 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	<input type="text" value=""/> 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	<input type="text" value="Default (no preference, typically autoselect)"/> Explicitly set speed and duplex mode for this interface. WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

### Static IPv4 Configuration

IPv4 Address	<input type="text" value="192.168.50.5"/>	/ 24
IPv4 Upstream gateway	<input type="text" value="None"/>	<input type="button" value="+ 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".

Controllo la configurazione dell'IP della macchina Metasploitable e inserisco l'IPv4 192.168.50.2, con subnet 255.255.255.0; e imposto come IP gateway 192.168.50.5 (lo stesso dell'interfaccia LAN2 di Pfsense).

```
RX bytes:112293 (109.6 KB) TX bytes:112293 (109.6 KB)
msfadmin@metasploitable:~$ sudo ifconfig eth0 192.168.50.2 netmask 255.255.255.0
msfadmin@metasploitable:~$ sudo route add default gw 192.168.50.5
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:c6:83:bc
          inet addr:192.168.50.2  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fec6:83bc/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:240  errors:0  dropped:0  overruns:0  frame:0
          TX packets:76  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:15360 (15.0 KB)  TX bytes:18128 (17.7 KB)
          Base address:0xd020 Memory:f0200000-f0220000
```

```
RX bytes:112293 (109.6 KB) TX bytes:112293 (109.6 KB)
msfadmin@metasploitable:~$ sudo ifconfig eth0 192.168.50.2 netmask 255.255.255.0
msfadmin@metasploitable:~$ sudo route add default gw 192.168.50.5
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:c6:83:bc
          inet addr:192.168.50.2  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fec6:83bc/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:240  errors:0  dropped:0  overruns:0  frame:0
          TX packets:76  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:15360 (15.0 KB)  TX bytes:18128 (17.7 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:286  errors:0  dropped:0  overruns:0  frame:0
          TX packets:286  errors:0  dropped:0  overruns:0  carrier:0
          collisions:0 txqueuelen:0
          RX bytes:114337 (111.6 KB)  TX bytes:114337 (111.6 KB)

msfadmin@metasploitable:~$ _
```

L'IP della macchina Kali è invece 192.168.60.10

```
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.60.10 netmask 255.255.255.0 broadcast 192.168.60.255
    inet6 fe80::e604:c17b:5e82:2ef4 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:ad:25:87 txqueuelen 1000 (Ethernet)
    RX packets 1462 bytes 1130770 (1.0 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 847 bytes 180426 (176.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 10 bytes 580 (580.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 10 bytes 580 (580.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Configuro l'IP gateway della macchina Kali impostando come IP 192.168.60.5, ossia l'IP dell'interfaccia LAN di Pfsense collegata a Kali:

```
(kali㉿kali)-[~]
$ sudo route add default gw 192.168.60.5
Home 512secondo
(kali㉿kali)-[~]
$ ip route show
default via 192.168.60.5 dev eth0
192.168.60.0/24 dev eth0 proto kernel scope link src 192.168.60.10 metric 100
(kali㉿kali)-[~]
$
```

L'interfaccia LAN di Pfsense è sulla stessa rete di Kali, mentre l'interfaccia LAN2 è sulla rete di Metasploitable:

```
Enter an option: 0

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)
VirtualBox Virtual Machine - Netgate Device ID: c63cd10cc33a9cdb0670
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

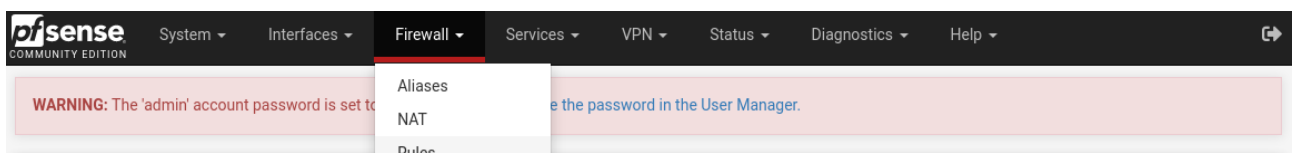
WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
LAN (lan)      -> vtnet0    -> v4: 192.168.60.5/24
LAN2 (opt1)    -> vtnet1    -> v4: 192.168.50.5/24

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: █
```

Ora passo alla configurazione di una regola firewall che blocchi l'accesso da Kali alla DVWA situata su Metasploitable.

Tramite la web GUI di Pfsense, seleziono "Firewall", poi "Rules"



e poi l'interfaccia "LAN", a cui è collegata la macchina Kali, e infine "Add" per aggiungere una nuova regola.

192.168.60.5/firewall\_rules.php?if=lan

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 / LAN

Floating WAN LAN LAN2

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓ 1/574 KiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✓ 0/18 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

Nella configurazione della nuova regola, come **action** seleziono “Block” per bloccare il traffico. L’**interfaccia** è “LAN”, da cui provengono i pacchetti della macchina Kali Linux, a cui voglio impedire l’accesso.

Come **protocollo** seleziono TCP, in modo da bloccare l’accesso tramite HTTP/HTTPS.

Alla voce **source** inserisco un indirizzo IP preciso, della sorgente a cui voglio impedire l’accesso, ossia quello della macchina Kali: 192.168.60.10.

Alla voce **destination**, invece, inserisco l’IP della destinazione, che è quello della macchina Metasploitable: 192.168.50.2

Infine, come **Destination Port Range** seleziono sia HTTP (80) sia HTTPS (443), per impedire l’accesso su entrambe le porte, a entrambi i protocolli.

<b>Action</b>	<div>Block</div>		
	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.		
<b>Disabled</b>	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.		
<b>Interface</b>	<div>LAN</div>		
	Choose the interface from which packets must come to match this rule.		
<b>Address Family</b>	<div>IPv4</div>		
	Select the Internet Protocol version this rule applies to.		
<b>Protocol</b>	<div>TCP</div>		
	Choose which IP protocol this rule should match.		

---

**Source**

Source

☐ Invert match

Address or Alias

192.168.60.10

/

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

192.168.50.2

/

Destination Port Range

HTTP (80)

From

Custom

To

HTTPS (443)

Custom

Per applicare la nuova regola clicco su “Apply Changes”

The firewall rule configuration has been changed.  
The changes must be applied for them to take effect.

Apply Changes

Floating
WAN
LAN
LAN2

Rules (Drag to Change Order)

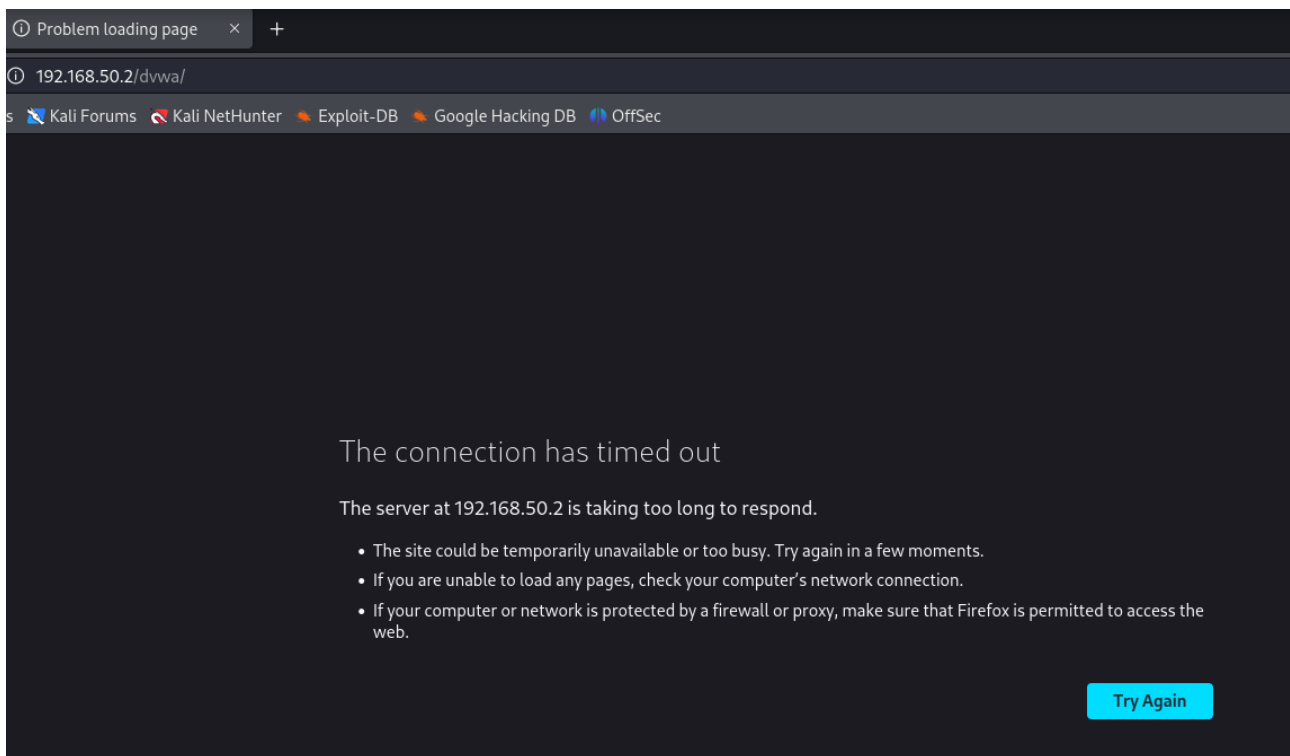
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	<span style="color: green;">✔</span> 0/933 KiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	<span style="color: red;">✘</span> 0/3 KiB	IPv4 TCP	192.168.60.10	*	192.168.50.2	80 - 443	*	none		RegolabloccoS3L5	
<input type="checkbox"/>	<span style="color: green;">✔</span> 0/140 KiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	<span style="color: green;">✔</span> 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Nella schermata si vede la regola che ho chiamato “RegolabloccoS3L5”, con le informazioni essenziali. Sono riportati la validità relativa a indirizzo IPv4 e al protocollo TCP, la sorgente (IP di Kali), la destinazione (IP di Metasploitable), le porte di riferimento (80 e 443).

Il posizionamento della regola più in alto assicura priorità alla stessa regola rispetto a quelle riportate di seguito.

Ora verifico se sia possibile effettuare l'accesso da Kali alla DVWA su Metasploitable. Tramite il browser inserisco l'indirizzo <https://192.168.50.2/dvwa>

Dopo un po' di attesa il risultato è:



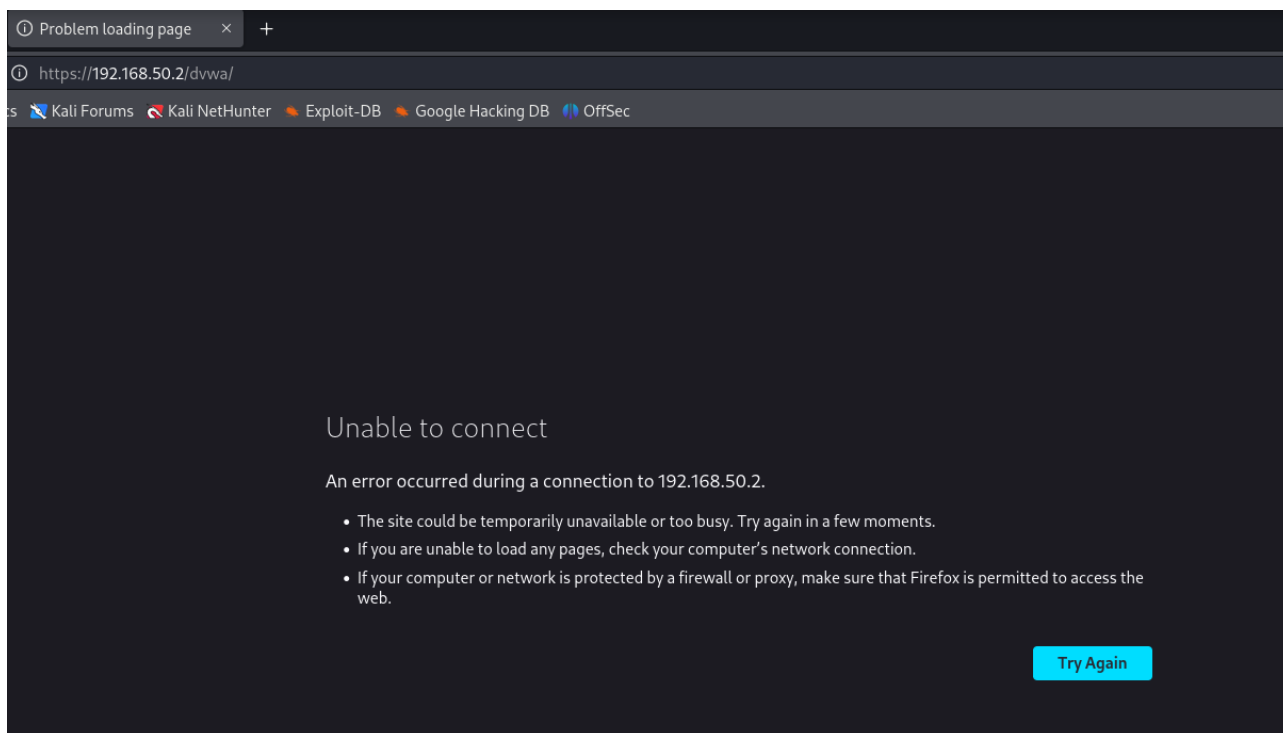
La ragione del “time out” è nella scelta che ho adottato nel configurare la regola di blocco. Alla voce “action” avevo selezionato “Block”, che scarta il pacchetto inviato dalla sorgente senza comunicare alcunché alla stessa sorgente.

**Action**

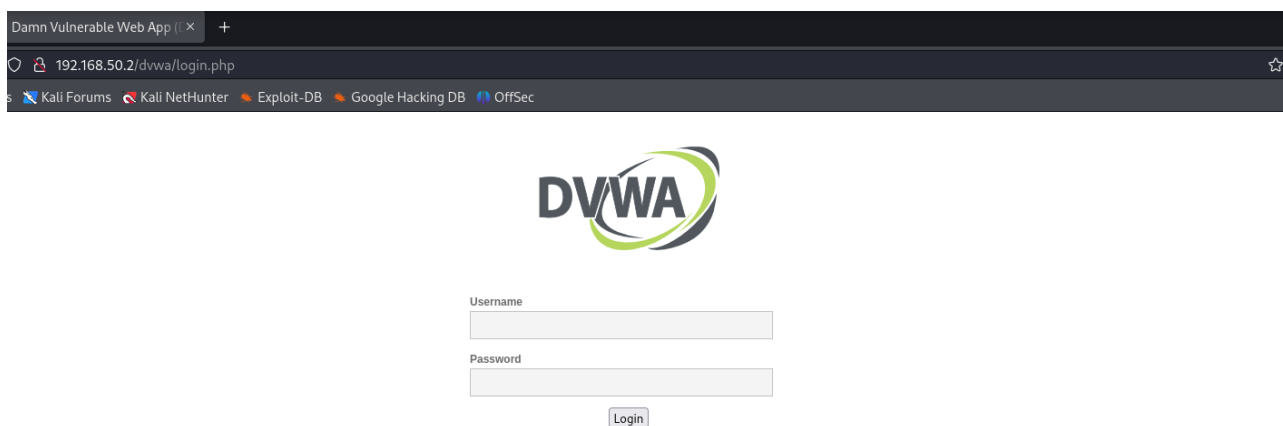
Choose what to do with packets that match the criteria specified below.

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.

Altrimenti, selezionando “Reject”, la sorgente ottiene una risposta, che riporta l'impossibilità di connettersi:



Infine, come ulteriore prova verifico se eliminando la regola dal firewall si possa invece accedere alla DVWA su Metasploitable da Kali:



L'accesso avviene regolarmente in tal caso (senza la regola).

---



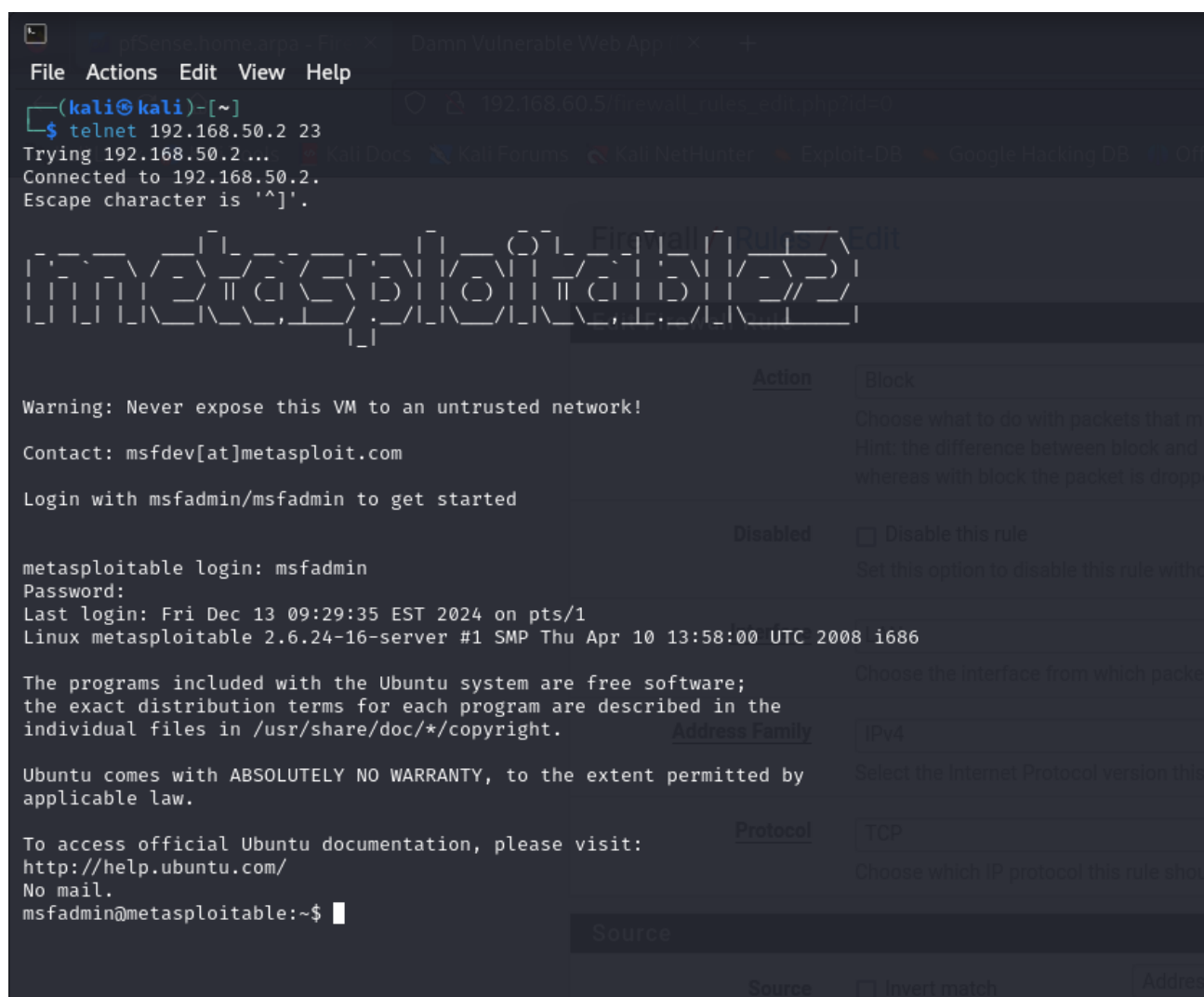
## Esercizio Bonus:

impostare una regola su Pfsense per bloccare da Kali il telnet verso Metasploitable.

## Svolgimento:

Telnet è un protocollo che fornisce una comunicazione bidirezionale tra due macchine, su una rete TCP/IP. Per connettersi, Telnet utilizza la porta 23. Perciò, devo impostare una nuova regola nel firewall, che blocchi il trasferimento di pacchetti sulla porta 23.

Prima di procedere, verifico se al momento sia possibile collegarsi dalla macchina Kali alla macchina Metasploitable tramite Telnet, sulla porta 23:



```
(kali@kali)-[~]
$ telnet 192.168.50.2 23
Trying 192.168.50.2...
Connected to 192.168.50.2.
Escape character is '^]'.

metasploit>

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Fri Dec 13 09:29:35 EST 2024 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
```

Sono riuscito ad accedere. Ora vado a impostare la regola per impedire che ciò accada.

Ripeto le procedure illustrate in precedenza, aprendo la web GUI di Pfsense, andando poi su “Firewall”, poi “Rules”, selezionando quindi LAN e poi “Add” per aggiungere una nuova regola.

**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

192.168.60.10

/

⚙ 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

192.168.50.2

/

**Destination Port Range**

Telnet (23)

From

Custom

To

Telnet (23)

Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Come si osserva nell'immagine, la configurazione di questa nuova regola riprende ampiamente quanto fatto in precedenza. Voglio che la regola blocchi, pertanto come **action** seleziono "block".

L'**interface** da cui provengono i pacchetti che voglio bloccare è "LAN", ossia quella collegata alla macchina Kali.

Il **protocol** è "TCP", su cui opera Telnet come scritto in precedenza.

Alla voce **source**, ossia la sorgente del pacchetto, indico l'IP specifico della macchina Kali: 192.168.60.10

Alla voce **destination**, destinatario del pacchetto, indico l'IP specifico della macchina Metasploitable: 192.168.50.2

La differenza è nella scelta del **destination port range**, che in questo caso si limita a "23", porta utilizzata da Telnet.

Salvo la nuova regola e la applico con "Apply Changes".

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 LAN2

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 1/1.78 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	⚙️
<input type="checkbox"/>	✗ 0/0 B	IPv4 TCP	192.168.60.10	*	192.168.50.2	23 (Telnet)	*	none		BloccaTelnetS3L5bonus	⚓ ⚙️ 📄 🗑️
<input type="checkbox"/>	✗ 0/0 B	IPv4 TCP	192.168.60.10	*	192.168.50.2	80 - 443	*	none		RegolabloccoS3L5	⚓ ⚙️ 📄 🗑️
<input type="checkbox"/>	✓ 1/208 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

La regola compare ora nelle regole, con il nome che ho inserito: BloccaTelnetS3L5bonus.

Infine, verifico se sia possibile effettuare di nuovo la comunicazione, come fatto in precedenza:

```

kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ telnet 192.168.50.2 23
Trying 192.168.50.2 ...
telnet: Unable to connect to remote host: Connection timed out

(kali@kali)-[~]
$

```

Poiché la regola nel Firewall stabilisce il blocco, il pacchetto viene scartato senza comunicare nulla alla sorgente. Quindi, la sorgente vede solamente “Connection timed out”.

Modificando invece la configurazione della regola, alla prima voce, **action**, e selezionando “Reject”, la sorgente ottiene una risposta che comunica il rifiuto della connessione: “Connection refused”.

```

kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ telnet 192.168.50.2 23
Trying 192.168.50.2 ...
telnet: Unable to connect to remote host: Connection refused

(kali@kali)-[~]
$

```