

Progetto S3/L5

In questo laboratorio l'obiettivo è stato configurare una regola **firewall** su **pfSense** per impedire a una macchina attaccante (**Kali Linux**) di effettuare scansioni o accedere alle applicazioni web (nello specifico è stato utilizzato **DVWA**) ospitata su una macchina target (**Metasploitable**). Un requisito fondamentale è stato garantire la segmentazione della rete, posizionando le due **macchine** su sottoreti distinte.

Come prima cosa dobbiamo configurare le "schede di rete virtuali" su VirtualBox. Dobbiamo simulare che **Kali** e **Metasploitable** siano in due stanze diverse, collegate solo da **pfSense**.

1. Configurazione pfSense (router centrale)

Andando sulle impostazioni di rete impostiamo le 3 schede di rete di cui abbiamo bisogno.

- **Scheda 1 (WAN)**: "Scheda con bridge" (dà accesso ad internet).
- **Scheda 2 (LAN)**: Impostata su **Rete Interna** (chiamala **kalinet**).
- **Scheda 3 (OPT1)**: Abilitiamo la scheda e la impostiamo su **Rete Interna** (chiamala **metaspInet**).

Si imposta in questo modo perchè pfSense deve avere un piede in ogni rete per poterle collegare e filtrare.

2. Configurazione Kali (macchina attaccante)

- Andiamo sulle impostazioni di rete della **Kali Linux** e impostiamo come la scheda di rete su “ **Rete Interna** ” selezionando “**kalinet**”.

3. Configurazione Metasploitable (macchina attaccata)

- Andiamo sulle impostazioni di rete della **Metasploitable** e impostiamo come la scheda di rete su “ **Rete Interna** ” selezionando “**metaspInet**”.

Successivamente ci colleghiamo dal browser della **Kali** all'interfaccia web della pfSense per impostare una nuova interfaccia di rete, in questo caso sarà **OPT1**, che corrisponderà alla rete “**metaspInet**”.

Configurazione delle schede di rete su pfSense

```
Pfsense [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

Press ENTER to continue.
VirtualBox Virtual Machine - Netgate Device ID: 060e7382738a522b9431

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> vtnet0      -> v4/DHCP4: 192.168.0.73/24
LAN (lan)      -> vtnet1      -> v4: 192.168.50.1/24
OPT1 (opt1)    -> em0        -> v4: 192.168.60.1/24

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:

FreeBSD/amd64 (pfSense.home.arp) (ttyv2)

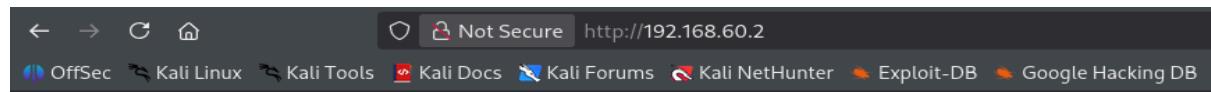
login: ■
```

Da questa schermata si può osservare la configurazione delle 3 schede di rete:

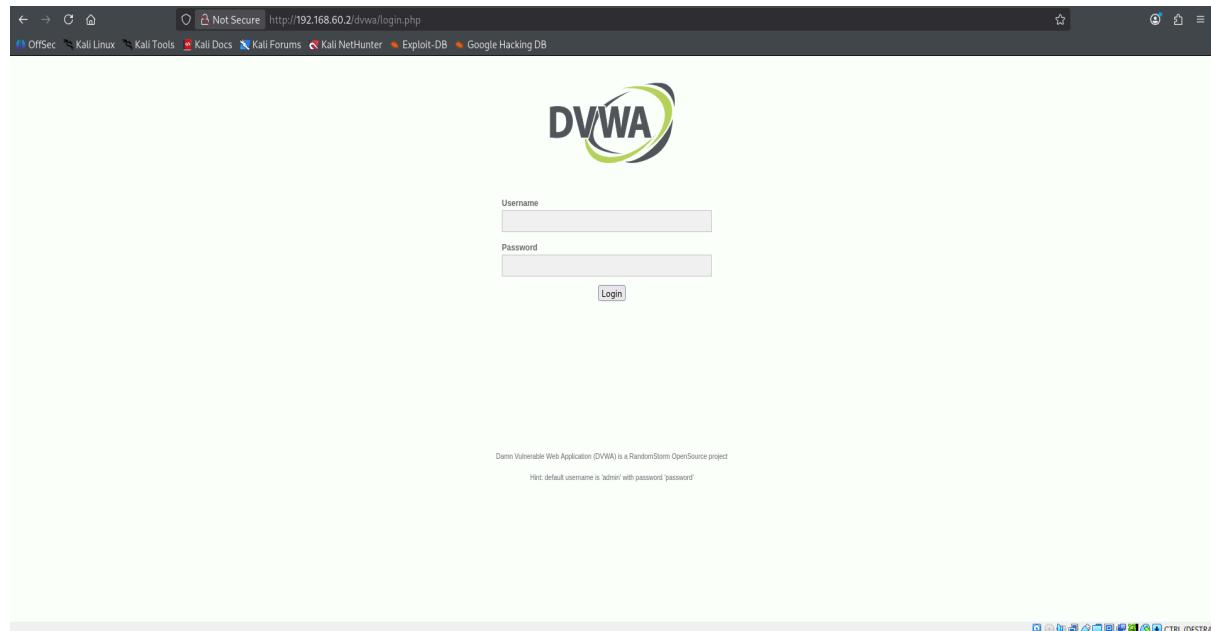
1. **WAN** (dà accesso ad internet)
2. **LAN** (rete relativa alla Kali)
3. **OPT1** (rete relativa alla Metasploitable)

Collegamento interfaccia web della Metasploitable da browser della Kali.

Prima di andare ad impostare le regole del **Firewall** verifichiamo l'effettiva possibilità di poterci connettere all'interfaccia web della **Metasploitable** dal browser della **Kali**



- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)



Creazione della Regola Firewall

Creazione delle regole firewall che bloccano l'accesso alla **DVWA** (su **Metasploitable**) dalla macchina **Kali** e ne impedisca lo scan.

Regole Firewall per WAN

The screenshot shows the 'WAN' tab selected under 'Rules'. There are two entries in the table:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/3 KIB	*	RFC 1918 networks	*	*	*	*	*		Block private networks	
0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	

A message at the bottom states: "No rules are currently defined for this interface. All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule."

Regole Firewall per LAN

The screenshot shows the 'LAN' tab selected under 'Rules'. There are four entries in the table:

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
2/200 Kib	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
0/0 B	IPv4 TCP	192.168.50.10	*	192.168.60.2	*	*	none			
13/2.63 MiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

At the bottom are buttons for Add, Delete, Toggle, Copy, Save, and Separator.

Regola impostata sul protocollo **TCP** per permettere il ping con la Metasploitable che è possibile grazie al protocollo **ICMP**.

Regole Firewall per OPT1

The screenshot shows the 'OPT1' tab selected under 'Rules'. A message at the top states: "No rules are currently defined for this interface. All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule."

At the bottom are buttons for Add, Delete, Toggle, Copy, Save, and Separator.

Per questo specifico esercizio non è necessario configurare la tabella **OPT1**.

PING dalla Kali Linux alla Metasploitable prima dell'attivazione della regola di Firewall.

Ping funziona

```
kali@kali: ~
Session Actions Edit View Help
└─(kali㉿kali)-[~]
$ ping -c 10 192.168.60.2
PING 192.168.60.2 (192.168.60.2) 56(84) bytes of data.
64 bytes from 192.168.60.2: icmp_seq=1 ttl=63 time=8.83 ms
64 bytes from 192.168.60.2: icmp_seq=2 ttl=63 time=8.61 ms
64 bytes from 192.168.60.2: icmp_seq=3 ttl=63 time=8.50 ms
64 bytes from 192.168.60.2: icmp_seq=4 ttl=63 time=9.59 ms
64 bytes from 192.168.60.2: icmp_seq=5 ttl=63 time=8.36 ms
64 bytes from 192.168.60.2: icmp_seq=6 ttl=63 time=8.76 ms
64 bytes from 192.168.60.2: icmp_seq=7 ttl=63 time=9.01 ms
64 bytes from 192.168.60.2: icmp_seq=8 ttl=63 time=8.84 ms
64 bytes from 192.168.60.2: icmp_seq=9 ttl=63 time=9.22 ms
64 bytes from 192.168.60.2: icmp_seq=10 ttl=63 time=8.68 ms

--- 192.168.60.2 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9029ms
rtt min/avg/max/mdev = 8.359/8.839/9.593/0.342 ms
```

PING dalla Kali Linux alla Metasploitable dopo aver attivato la regola di Firewall

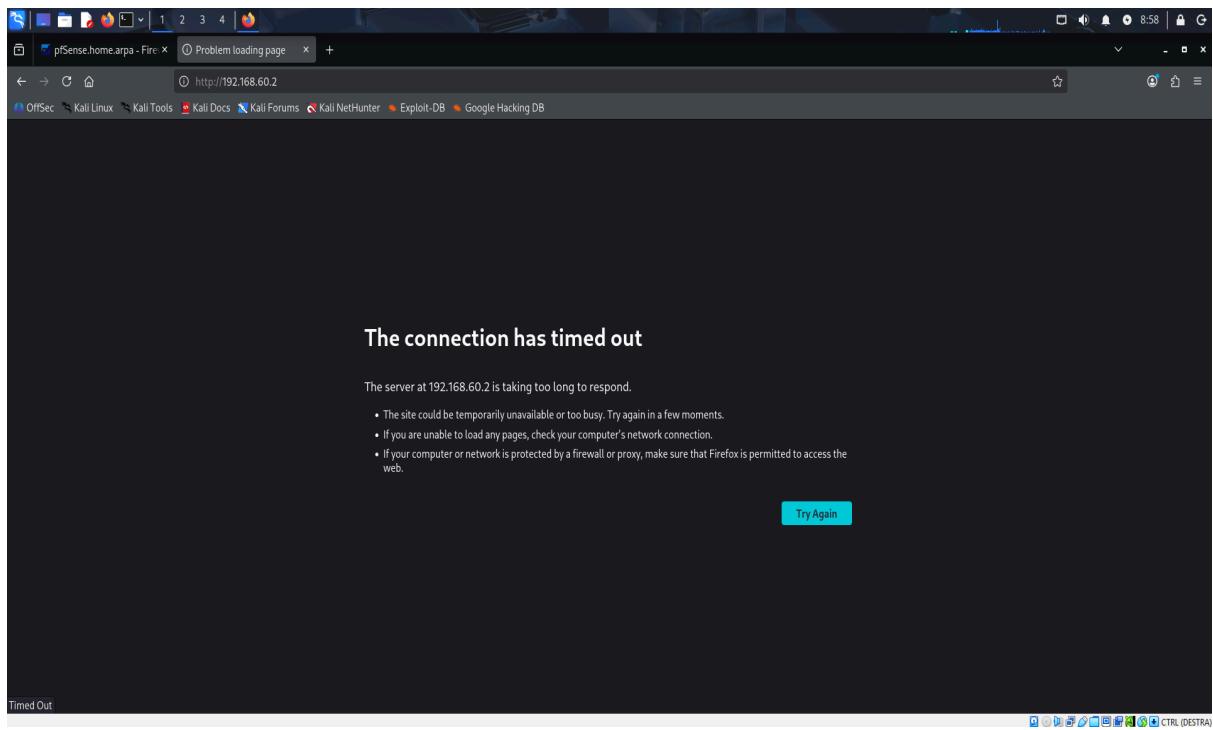
Ping funziona

```
kali@kali: ~
Session Actions Edit View Help
└─(kali㉿kali)-[~]
$ ping -c 5 192.168.60.2
PING 192.168.60.2 (192.168.60.2) 56(84) bytes of data.
64 bytes from 192.168.60.2: icmp_seq=1 ttl=63 time=7.81 ms
64 bytes from 192.168.60.2: icmp_seq=2 ttl=63 time=9.82 ms
64 bytes from 192.168.60.2: icmp_seq=3 ttl=63 time=8.72 ms
64 bytes from 192.168.60.2: icmp_seq=4 ttl=63 time=7.98 ms
64 bytes from 192.168.60.2: icmp_seq=5 ttl=63 time=8.99 ms

--- 192.168.60.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4013ms
rtt min/avg/max/mdev = 7.813/8.664/9.821/0.727 ms
```

Il **ping** continua a funzionare perchè abbiamo configurato la regola del **Firewall** specificatamente per il protocollo **TCP**. Quindi la **Kali** potrà effettuare il **ping** sia prima che dopo l'applicazione della regola.

Collegamento interfaccia web della Metasploitable da browser della Kali dopo aver inserito la regola di Firewall



In questo caso la connessione all'interfaccia web della Metasploitable fallisce.