

S5/L1



PfSense

Creazione pratica di una regola Firewall.

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.

1. Settare le interfacce di rete su PfSense (WAN, LAN e OPT1)

```
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***  
  
WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24  
LAN (lan)      -> em1      -> v4: 192.168.49.1/24  
OPT1 (opt1)    -> em2      -> v4: 192.168.50.1/24
```

2. Settiamo gli indirizzi IP di Kali Linux e di Metasploitable2

```
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.49.100 netmask 255.255.255.0 broadcast 192.168.49.255
          inet6 fe80::a00:27ff:fe1e:364a prefixlen 64 scopeid 0x20<link>
            ether 08:00:27:1e:36:4a txqueuelen 1000 (Ethernet)
              RX packets 18 bytes 2014 (1.9 KiB)
              RX errors 0 dropped 0 overruns 0 frame 0
              TX packets 469 bytes 40150 (39.2 KiB)
              TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Kali Linux - 192.168.49.100

```
To access official Ubuntu documentation, please visit:
```

```
http://help.ubuntu.com/
```

```
No mail.
```

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:6d:5f:cb
          inet addr:192.168.50.100 Bcast:192.168.50.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe6d:5fcba/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
            RX packets:10 errors:0 dropped:0 overruns:0 frame:0
            TX packets:70 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:640 (640.0 B) TX bytes:8449 (8.2 KB)
            Base address:0xd020 Memory:f0200000-f0220000
```

Metasploitable2 - 192.168.50.100

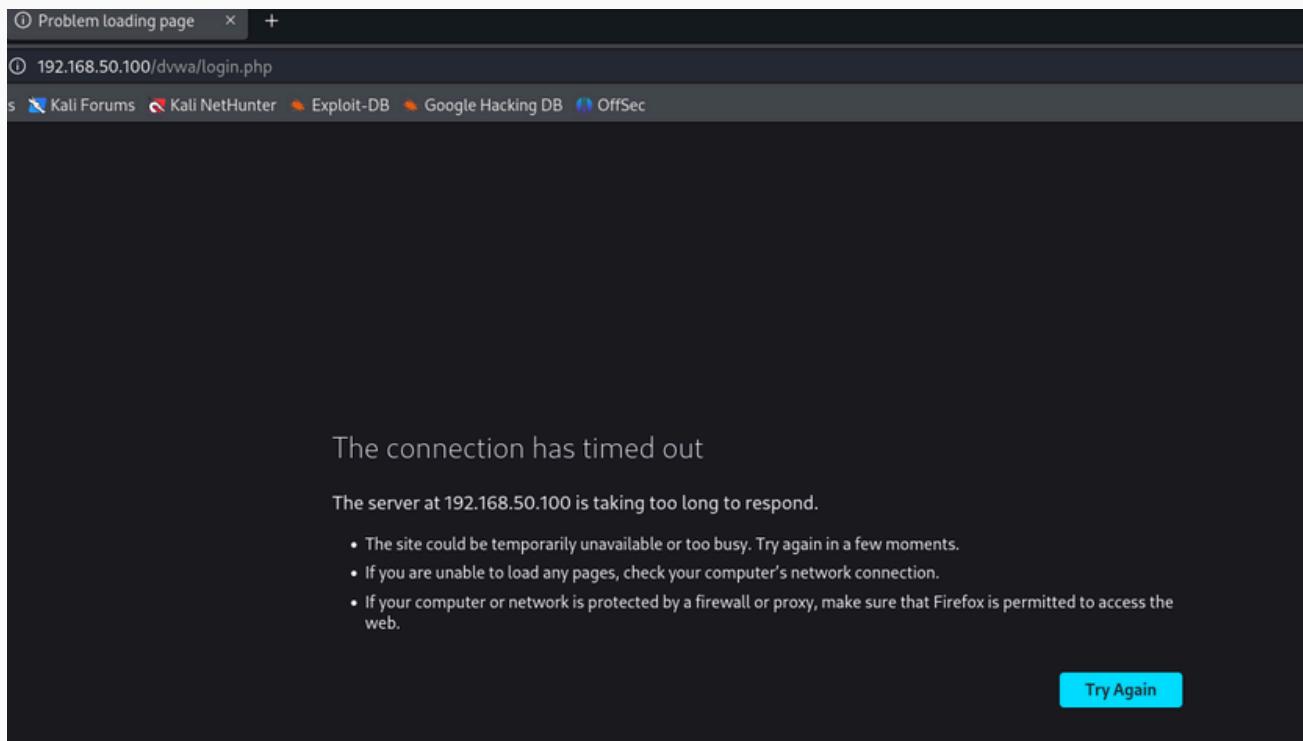
3. Una volta configurate le due reti, entriamo nella GUI Web di PfSense per impostare una nuova regola per bloccare lo scan delle porte e la connettività alla DVWA da parte di Kali Linux

The screenshot shows the 'Edit Firewall Rule' interface in the PfSense web UI. The rule is set to 'Block' action, disabled, and applies to LAN interface, IPv4 address family, and TCP protocol. The source is 192.168.49.100 and the destination is 192.168.50.100. The rule is for SSH (22) and HTTP (80) ports. Advanced options like logging and a description are present, and the rule information shows it was created and updated by admin.

Edit Firewall Rule	
Action	<input type="button" value="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	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
Interface	<input type="button" value="LAN"/>
Choose the interface from which packets must come to match this rule.	
Address Family	<input type="button" value="IPv4"/>
Select the Internet Protocol version this rule applies to.	
Protocol	<input type="button" value="TCP"/>
Choose which IP protocol this rule should match.	
Source	
Source	<input type="checkbox"/> Invert match <input type="text" value="Address or Alias"/> <input type="text" value="192.168.49.100"/> / <input type="button" value="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	<input type="checkbox"/> Invert match <input type="text" value="Address or Alias"/> <input type="text" value="192.168.50.100"/> / <input type="button" value="Display Advanced"/>
Destination Port Range	<input type="button" value="SSH (22)"/> From <input type="text" value="Custom"/> To <input type="button" value="HTTP (80)"/> To <input type="text" value="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	<input type="checkbox"/> Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).
Description	<input type="text"/> A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.
Advanced Options	<input type="button" value="Display Advanced"/>
Rule Information	
Tracking ID	1719247165
Created	6/24/24 16:39:25 by admin@192.168.49.100 (Local Database)
Updated	6/24/24 16:43:23 by admin@192.168.49.100 (Local Database)

4. Impostando l' interfaccia LAN (che corrisponde alla subnet di Kali), il protocollo TCP, il source IP di Kali, il destination IP di Meta e poi il range delle porte da SSH(22) a HTTP(80), il collegamento tra le due sarà interrotto.

Provando a connettersi tramite Firefox a 192.168.50.1 la connessione non viene stabilita



5. Attraverso i log dei file di sistema del firewall, possiamo vedere come la nuova regola sia efficace.

✗	Jun 24 16:25:05	OPT1	Default deny rule IPv4 (1000000103)	✗ 192.168.50.100:52687	✗ 192.168.50.1:53	UDP
✗	Jun 24 16:25:05	OPT1	Default deny rule IPv4 (1000000103)	✗ 192.168.50.100:52687	✗ 192.168.50.1:53	UDP
✗	Jun 24 16:25:05	OPT1	Default deny rule IPv4 (1000000103)	✗ 192.168.50.100:52689	✗ 192.168.50.1:53	UDP
✗	Jun 24 16:25:05	OPT1	Default deny rule IPv4 (1000000103)	✗ 192.168.50.100:52689	✗ 192.168.50.1:53	UDP
✗	Jun 24 16:25:05	OPT1	Default deny rule IPv4 (1000000103)	✗ 192.168.50.100:37326	✗ 192.168.50.1:53	UDP
✗	Jun 24 16:25:05	OPT1	Default deny rule IPv4 (1000000103)	✗ 192.168.50.100:37326	✗ 192.168.50.1:53	UDP
✗	Jun 24 16:25:05	OPT1	Default deny rule IPv4 (1000000103)	✗ 192.168.50.100:33391	✗ 192.168.50.1:53	UDP
✗	Jun 24 16:25:05	OPT1	Default deny rule IPv4 (1000000103)	✗ 192.168.50.100:33391	✗ 192.168.50.1:53	UDP
✗	Jun 24 16:25:06	OPT1	Default deny rule IPv4 (1000000103)	✗ 192.168.50.100:46904	✗ 192.168.50.1:53	UDP
✗	Jun 24 16:25:06	OPT1	Default deny rule IPv4 (1000000103)	✗ 192.168.50.100:46904	✗ 192.168.50.1:53	UDP