

Creazione policy PfSense

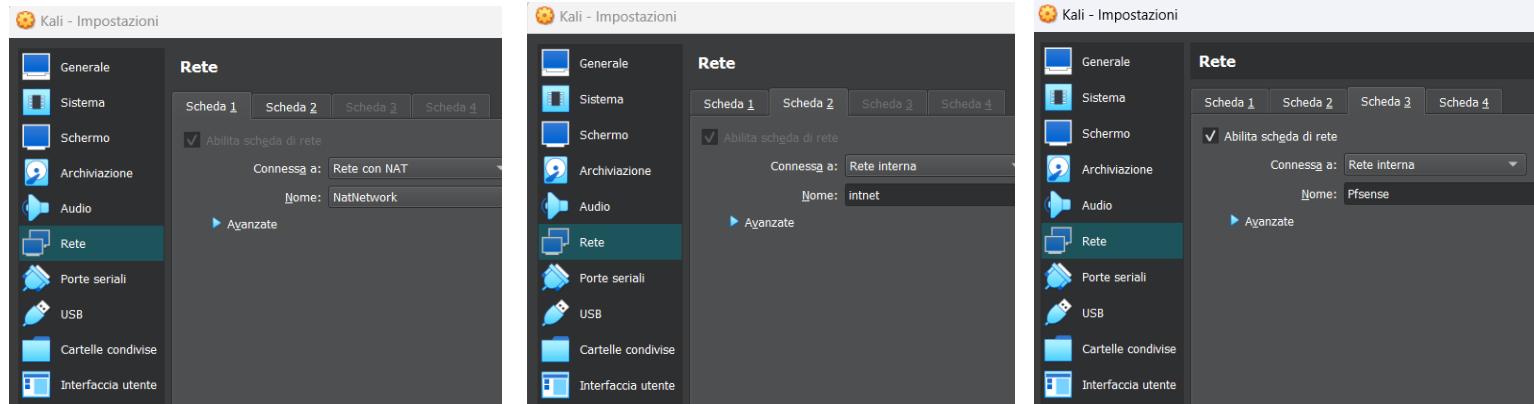
I) Modifico le impostazioni di rete nelle impostazioni di VirtualBox per le seguenti macchine:

Kali Linux:

Scheda 1) Rete con NAT - per navigare su web

Scheda 2) Rete interna (intnet) - per la connettività con Metasploitable

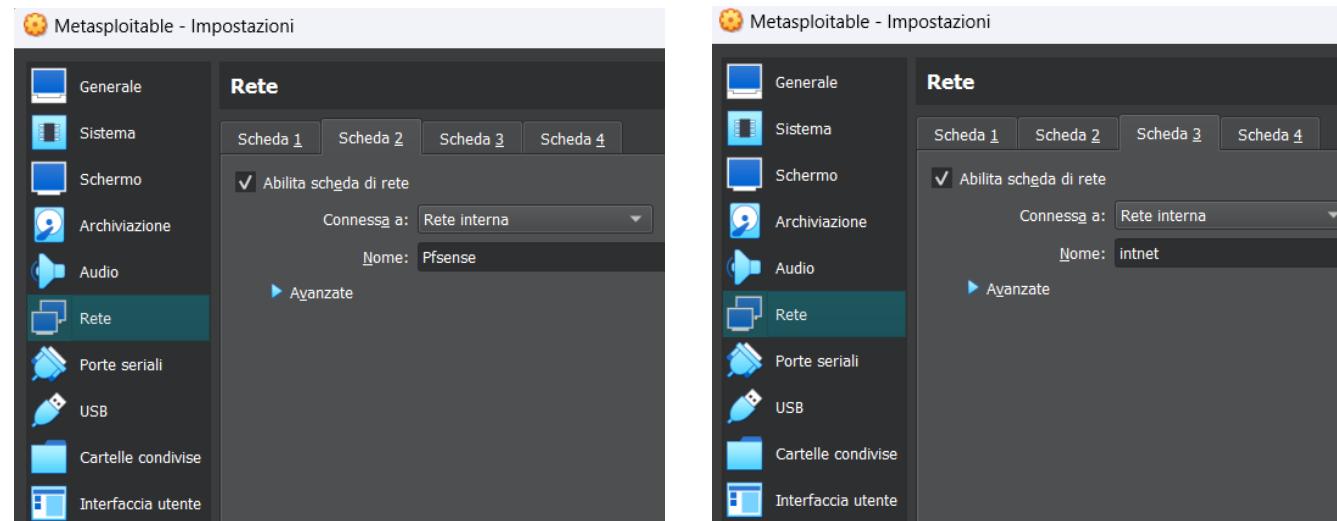
Scheda 3) Rete interna (PfSense) - per la connettività con PfSense



Metasploitable:

Scheda 1) Rete interna (intnet) - per la connettività con Kali Linux

Scheda 2) Rete interna (PfSense) - per la connettività con PfSense

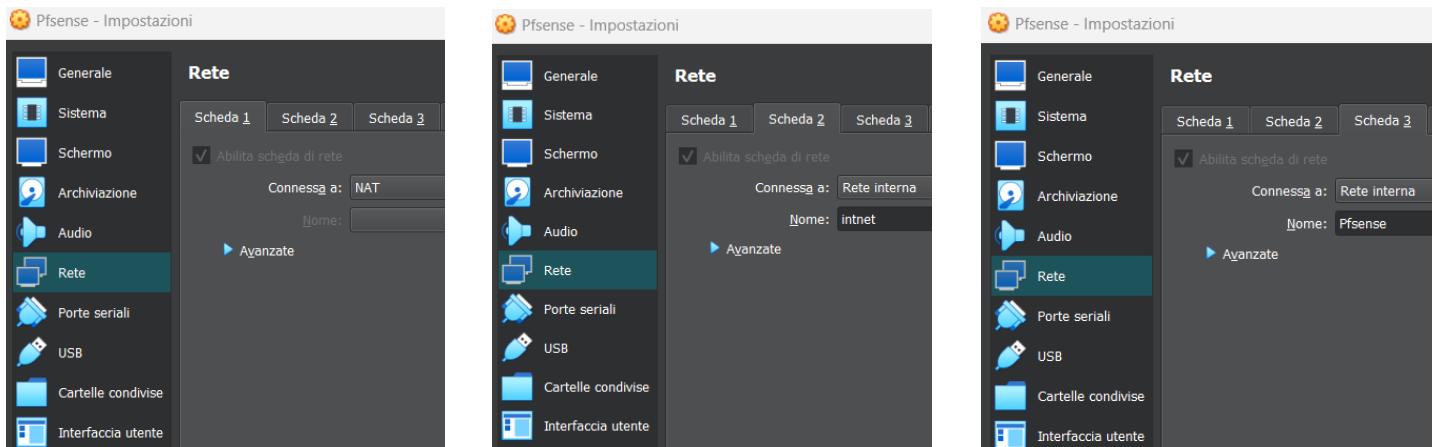


PfSense:

Scheda 1) Rete con NAT

Scheda 2) Rete interna(intnet) - per la connettività con Kali Linux

Scheda 3) Rete interna (PfSense) - per la connettività con Metasploitable

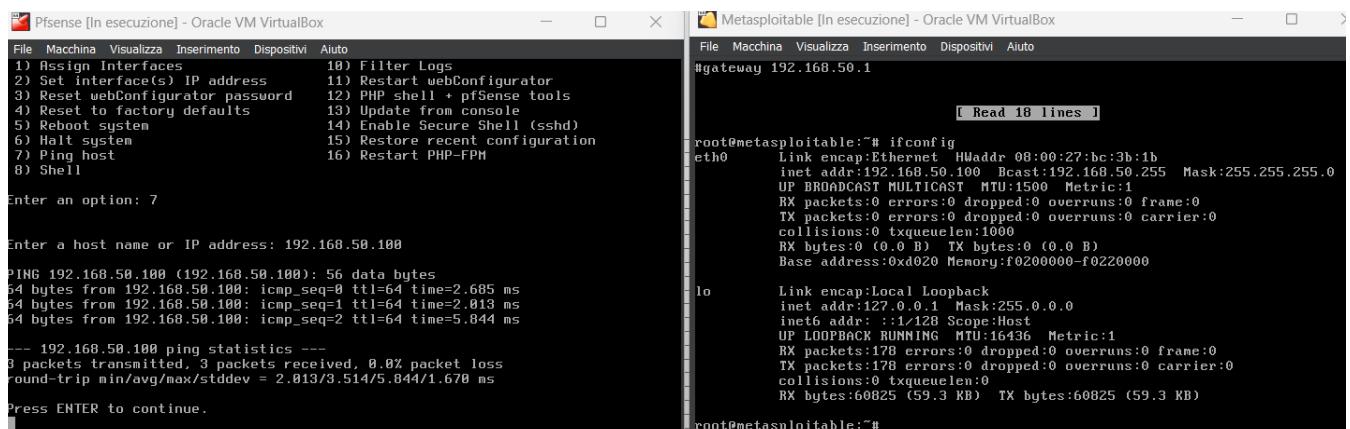


II) Verifico la connettività tra Pfsense(192.168.1.1) e Kali (192.168.1.100) eseguendo un ping tra le due macchine:

```
(kali㉿kali)-[~]
$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=2.35 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=1.50 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=9.86 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=6.50 ms
64 bytes from 192.168.1.1: icmp_seq=5 ttl=64 time=6.59 ms
64 bytes from 192.168.1.1: icmp_seq=6 ttl=64 time=2.35 ms
64 bytes from 192.168.1.1: icmp_seq=7 ttl=64 time=2.11 ms
64 bytes from 192.168.1.1: icmp_seq=8 ttl=64 time=2.41 ms
64 bytes from 192.168.1.1: icmp_seq=9 ttl=64 time=2.83 ms
64 bytes from 192.168.1.1: icmp_seq=10 ttl=64 time=5.76 ms
64 bytes from 192.168.1.1: icmp_seq=11 ttl=64 time=9.62 ms
^C
--- 192.168.1.1 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10809ms
rtt min/avg/max/mdev = 1.495/4.716/9.861/2.947 ms
```

```
Enter a host name or IP address: 192.168.1.100
PING 192.168.1.100 (192.168.1.100): 56 data bytes
64 bytes from 192.168.1.100: icmp_seq=0 ttl=64 time=1.249 ms
64 bytes from 192.168.1.100: icmp_seq=1 ttl=64 time=9.288 ms
64 bytes from 192.168.1.100: icmp_seq=2 ttl=64 time=4.997 ms
--- 192.168.1.100 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.249/5.151/9.208/3.251 ms
```

III) Verifico la connettività tra Pfsense (192.168.1.1) e Metasploitable (192.168.50.100)



```
Pfsense [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
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: 7

Enter a host name or IP address: 192.168.50.100
PING 192.168.50.100 (192.168.50.100): 56 data bytes
64 bytes from 192.168.50.100: icmp_seq=0 ttl=64 time=2.685 ms
64 bytes from 192.168.50.100: icmp_seq=1 ttl=64 time=2.013 ms
64 bytes from 192.168.50.100: icmp_seq=2 ttl=64 time=5.844 ms
--- 192.168.50.100 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 2.013/3.514/5.844/1.678 ms
Press ENTER to continue.

Metasploitable [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
#gateway 192.168.50.1

[ Read 18 lines ]

root@metasploitable:~# ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:bc:3b:1b
          inet addr: 192.168.50.100 Bcast:192.168.50.255 Mask:255.255.255.0
          UP BROADCAST MULTICAST MTU:1500 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)
          Base address:0xd020 Memory:f0200000-f0220000

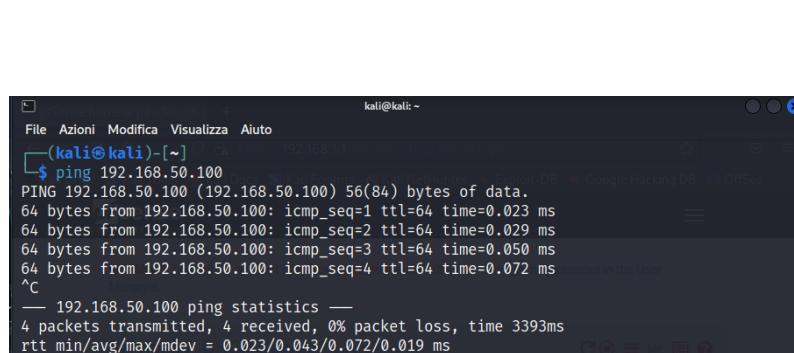
lo       Link encap:Local Loopback
          inet addr: 127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:178 errors:0 dropped:0 overruns:0 frame:0
          TX packets:178 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:60825 (59.3 KB) TX bytes:60825 (59.3 KB)

root@metasploitable:~#
```

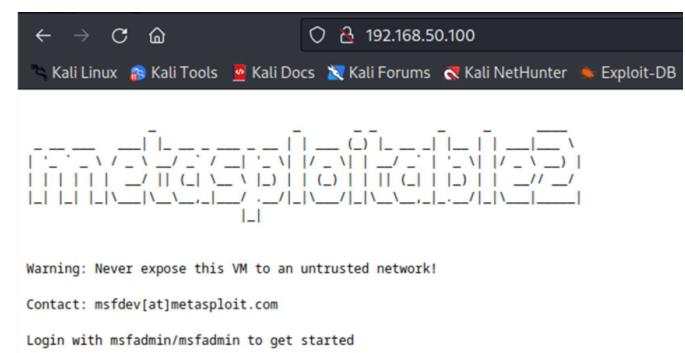
*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense ***

```
WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24
LAN2 (opt1)    -> em2      -> v4: 192.168.50.1/24
```

IV) Verifico la connettività tra Kali (192.168.1.100) e Metasploitable (192.168.50.100) eseguendo un ping tra le due macchine anche verso la DVWA:



```
kali㉿kali)-[~]
$ ping 192.168.50.100
PING 192.168.50.100 (192.168.50.100) 56(84) bytes of data.
64 bytes from 192.168.50.100: icmp_seq=1 ttl=64 time=0.023 ms
64 bytes from 192.168.50.100: icmp_seq=2 ttl=64 time=0.029 ms
64 bytes from 192.168.50.100: icmp_seq=3 ttl=64 time=0.050 ms
64 bytes from 192.168.50.100: icmp_seq=4 ttl=64 time=0.072 ms
^C
--- 192.168.50.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3393ms
rtt min/avg/max/mdev = 0.023/0.043/0.072/0.019 ms
```



192.168.50.100
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

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

V) Creo la regola su Pfsense in modo tale da bloccare il traffico sulla porta 80 da Kali (192.168.1.100) a Metasploitable (192.168.50.100) rendendo la DVWA inaccessibile a Kali

The screenshot shows the 'Edit Firewall Rule' screen. The 'Action' dropdown is set to 'Block'. The 'Disabled' section has a checkbox for 'Disable this rule' which is unchecked. The 'Interface' is set to 'LAN'. The 'Address Family' is 'IPv4'. The 'Protocol' is 'TCP'. In the 'Source' section, the 'Source' dropdown is set to 'Single host or alias' with '192.168.1.100' selected. A note says '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.' In the 'Destination' section, the 'Destination' dropdown is set to 'Single host or alias' with '192.168.50.100' selected. The 'Destination Port Range' dropdown is set to 'HTTP (80)'. At the bottom, there is a summary table:

<input type="checkbox"/>	<input checked="" type="checkbox"/>	0/0 B	IPv4 TCP	192.168.1.100	*	192.168.50.100	80 (HTTP)	*	none	Default allow LAN to any rule
--------------------------	-------------------------------------	-------	----------	---------------	---	----------------	-----------	---	------	-------------------------------

VI) Dai log di Firewall verifico che la regola stia effettivamente bloccano il traffico da Kali verso la DVWA

The screenshot shows the 'Status / System Logs / Firewall / Normal View' screen. The 'Firewall' tab is selected. Below it are three tabs: 'Normal View' (selected), 'Dynamic View', and 'Summary View'. The main area displays a table titled 'Last 318 Firewall Log Entries. (Maximum 500)'. The columns are: Action, Time, Interface, Rule, Source, Destination, and Protocol. The log entries show multiple entries with an 'X' icon in the Action column, indicating they were blocked by the rule. The entries are as follows:

Action	Time	Interface	Rule	Source	Destination	Protocol
✗	Jul 25 22:10:40	LAN	Default deny rule IPv6 (1000000105)	i 192.168.1.10:48392	i 192.168.50.100:80	TCP:S
✗	Jul 25 22:10:40	LAN	Default deny rule IPv6 (1000000105)	i 192.168.1.10:48406	i 192.168.50.100:80	TCP:S
✗	Jul 25 22:10:41	LAN	Default deny rule IPv6 (1000000105)	i 192.168.1.10:48406	i 192.168.50.100:80	TCP:S
✗	Jul 25 22:10:41	LAN	Default deny rule IPv6 (1000000105)	i 192.168.1.10:48380	i 192.168.50.100:80	TCP:S
✗	Jul 25 22:10:43	LAN	Default deny rule IPv6 (1000000105)	i 192.168.1.10:48406	i 192.168.50.100:80	TCP:S
✗	Jul 25 22:10:43	LAN	Default deny rule IPv6 (1000000105)	i 192.168.1.10:48406	i 192.168.50.100:80	TCP:S