

Traccia: Dopo aver configurato le macchine di Kali e Metasploitable su 2 reti differenti e aver settato il firewall PFSense, successivamente creare un regola che blocchi l'accesso alla DVWA su Metasploitable.

- Ho configurato le macchine virtuali Kali e Metasploitable su 2 reti differenti e la terza interfaccia su Pfsense;

```
(giorgio@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.100 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::a00:27ff:fe94:f4fb prefixlen 64 scopeid 0x20<link>
    inet6 2001:b07:ad4:a4a7:a00:27ff:fe94:f4fb prefixlen 64 scopeid 0x0<global>
    ether 08:00:27:94:f4:fb txqueuelen 1000 (Ethernet)
    RX packets 415 bytes 30345 (29.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 89 bytes 8511 (8.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

msfadmin@metasploitable:~$ ifconfig
eth0: Link encap:Ethernet HWaddr 08:00:27:6b:1d:4c
    inet addr:192.168.50.101 Bcast:192.168.50.255 Mask:255.255.255.0
    inet6 addr: fe80::a00:27ff:fe6b:1d4c/64 Scope:Link
    UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
    RX packets:0 errors:0 dropped:0 overruns:0 frame:0
    TX packets:64 errors:0 dropped:0 overruns:0 carrier:0
    collisions:0 txqueuelen:1000
    RX bytes:0 (0.0 B) TX bytes:4752 (4.6 KB)
    Base address:0xd010 Memory:f0200000-f0220000

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

WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
LAN (lan)      -> em1      -> v4: 192.168.1.10/24
LAN2 (opt1)    -> em2      -> v4: 192.168.50.1/24
```

- Ho potuto constatare che le macchine potessero comunicare effettivamente tra di loro sia tramite protocollo TCP che ICMP;

```
(giorgio@kali)-[~]
$ ping 192.168.50.101
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data:
64 bytes from 192.168.50.101: icmp_seq=1 ttl=63 time=1.91 ms
64 bytes from 192.168.50.101: icmp_seq=2 ttl=63 time=1.77 ms
64 bytes from 192.168.50.101: icmp_seq=3 ttl=63 time=2.34 ms
64 bytes from 192.168.50.101: icmp_seq=4 ttl=63 time=1.50 ms
64 bytes from 192.168.50.101: icmp_seq=5 ttl=63 time=1.68 ms
^Z
zsh: suspended ping 192.168.50.101
```



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

- Tramite l'utilizzo della Web GUI di PfSense è stata creata una nuova regola che impedisse a Kali di comunicare con la DVWA;

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: Any
Choose which IP protocol this rule should match.

Source

Source: ☐ Invert match | Single host or alias | 192.168.1.100 | / |

Destination

Destination: ☐ Invert match | Single host or alias | 192.168.50.101 | / |

Extra Options

Log: ☒ 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).

- Abbiamo potuto constatare che la nuova regola firewall ha impedito la comunicazione tra le 2 macchine, ciò è confermato sia dai file di log che dal tentativo effettuato con web browser come dimostrato nelle seguenti immagini.

✗	Oct 23 20:47:56	LAN	USER_RULE (1698093425)	192.168.1.100	192.168.50.101	ICMP
✗	Oct 23 20:47:57	LAN	USER_RULE (1698093425)	192.168.1.100	192.168.50.101	ICMP
✗	Oct 23 20:47:58	LAN	USER_RULE (1698093425)	192.168.1.100	192.168.50.101	ICMP
✗	Oct 23 20:47:59	LAN	USER_RULE (1698093425)	192.168.1.100	192.168.50.101	ICMP

