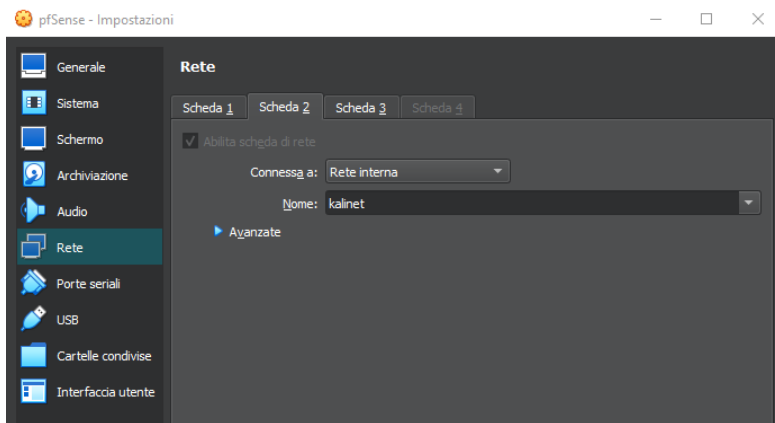


CONFIGURAZIONE DELLE RETI

Configurazione Kali



NIC che gestisce la rete nella quale è presente la macchina Kali

```
GNU nano 7.2
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

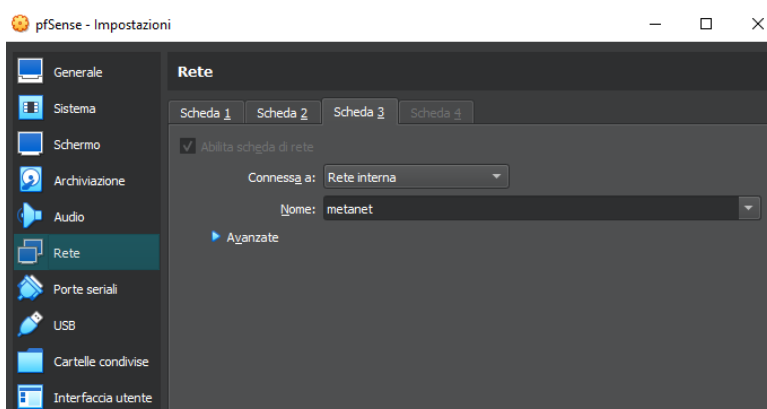
# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
#iface eth0 inet dhcp

iface eth0 inet static
address 192.168.1.100
netmask 255.255.255.0
broadcast 192.168.1.255
gateway 192.168.1.1
```

Configurazione IP della macchina Kali.
Viene assegnato un IP statico:
192.168.1.100

Configurazione Metasploitable 2



NIC che gestisce la rete nella quale è presente la macchina Metasploitable 2

```
# The primary network interface
auto eth0


#iface eth0 inet dhcp

iface eth0 inet static
address 192.168.2.100
netmask 255.255.255.0
network 192.168.2.0
broadcast 192.168.2.255
gateway 192.168.2.1
```



Configurazione IP della macchina Metasploitable 2.



Viene assegnato un IP statico: 192.168.2.100

Configurazione interfaccia di rete aggiuntiva su pfSense per gestire la rete nella quale è presente la macchina Metasploitable 2 in quanto quella che gestisce Kali era già stata configurata in fasi di installazione di pfSense.

Interfaces / Interface Assignments 

Interface Assignments Interface Groups Wireless VLANs QinQs PPPs GREs GIFs Bridges LAGGs

Interface	Network port
WAN	em0 (08:00:27:b4:59:8c)
LAN	em1 (08:00:27:4f:e9:a2) 
LAN1	em2 (08:00:27:9a:e8:7f) 

Interfaces / LAN1 (em2)  

General Configuration

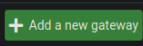
Enable ☒ Enable interface

Description
Enter a description (name) for the interface here.

IPv4 Configuration Type

Static IPv4 Configuration

IPv4 Address /

IPv4 Upstream 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".
Selecting an upstream gateway causes the firewall to treat this interface as a WAN type interface.
Gateways can be managed by [clicking here](#).

Prove di connessione tra host presenti sulle reti

```
(kali㉿kali)-[~]
$ ping 192.168.1.1 -c 4
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=0.391 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=0.295 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=0.338 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=64 time=0.322 ms

— 192.168.1.1 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3068ms
rtt min/avg/max/mdev = 0.295/0.336/0.391/0.035 ms

(kali㉿kali)-[~]
$ ping 192.168.2.1 -c 4
PING 192.168.2.1 (192.168.2.1) 56(84) bytes of data:
64 bytes from 192.168.2.1: icmp_seq=1 ttl=64 time=0.309 ms
64 bytes from 192.168.2.1: icmp_seq=2 ttl=64 time=0.259 ms
64 bytes from 192.168.2.1: icmp_seq=3 ttl=64 time=0.289 ms
64 bytes from 192.168.2.1: icmp_seq=4 ttl=64 time=0.269 ms

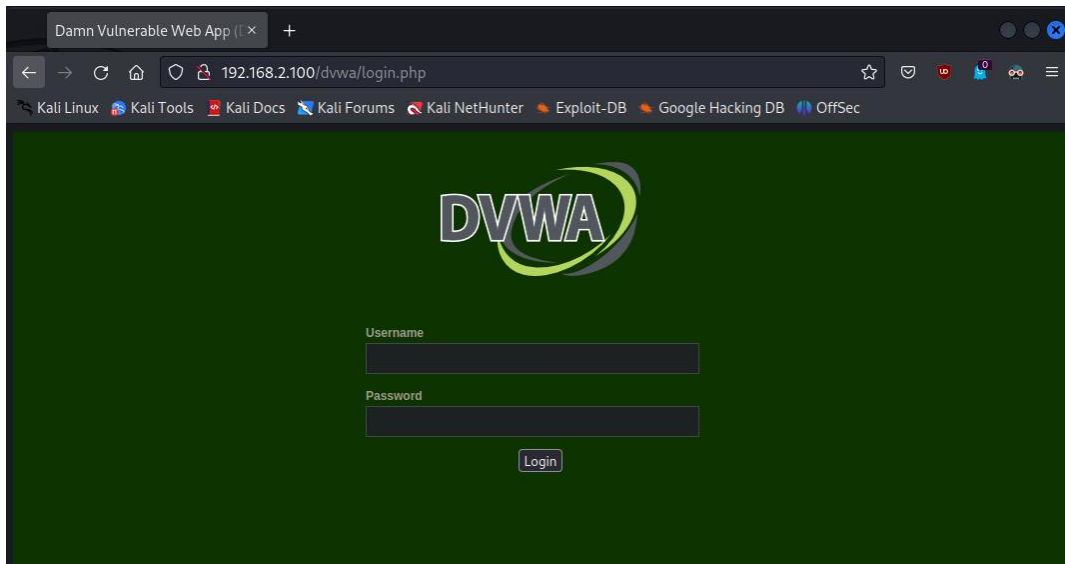
— 192.168.2.1 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3061ms
rtt min/avg/max/mdev = 0.259/0.281/0.309/0.019 ms

(kali㉿kali)-[~]
$ ping 192.168.2.100 -c 4
PING 192.168.2.100 (192.168.2.100) 56(84) bytes of data:
64 bytes from 192.168.2.100: icmp_seq=1 ttl=63 time=0.547 ms
64 bytes from 192.168.2.100: icmp_seq=2 ttl=63 time=0.502 ms
64 bytes from 192.168.2.100: icmp_seq=3 ttl=63 time=0.501 ms
64 bytes from 192.168.2.100: icmp_seq=4 ttl=63 time=0.525 ms

— 192.168.2.100 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3066ms
rtt min/avg/max/mdev = 0.501/0.518/0.547/0.018 ms
```

CREAZIONE REGOLA FIREWALL

Prova di accesso alla DVWA su Metasploitable 2 senza regole di firewall



Cattura dei pacchetti con Wireshark che mostra il corretto scambio di pacchetti con la DVWA

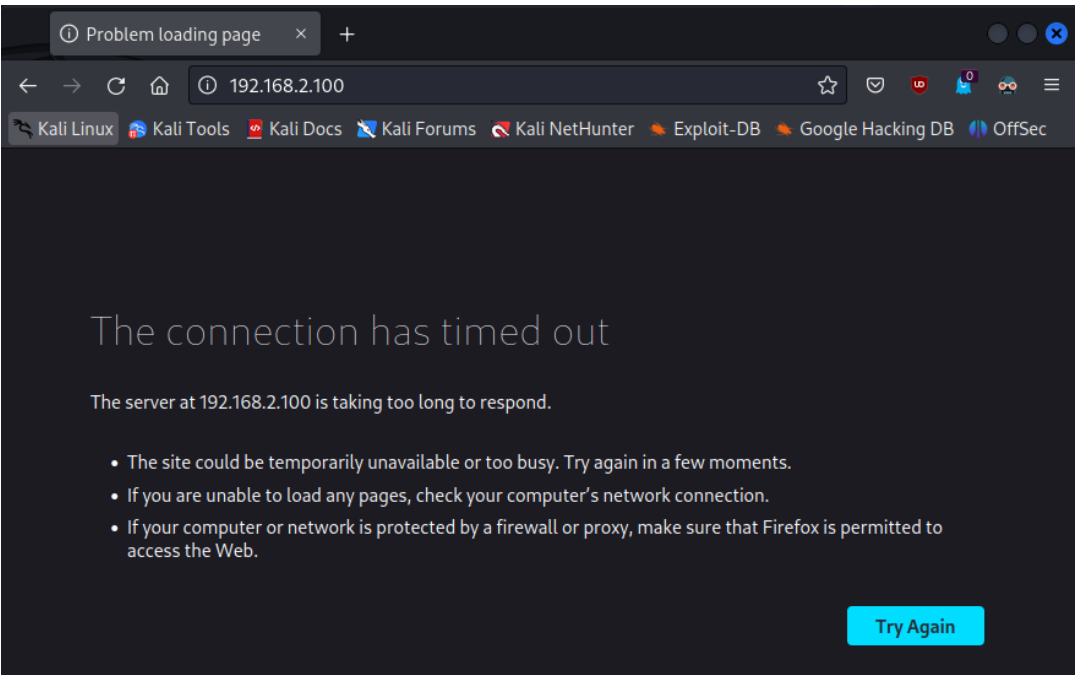
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.1.100	192.168.2.100	HTTP	463	GET / HTTP/1.1
2	0.008735871	192.168.2.100	192.168.1.100	HTTP	1189	HTTP/1.1 200 OK (text/html)
3	0.008767355	192.168.1.100	192.168.2.100	TCP	66	56542 → 80 [ACK] Seq=398 Ack=1124 Win=501 Len=0

Prova di scansione con l'utility nmap sulla porta 80

```
(kali@kali)-[~]
└─$ nmap -A 192.168.2.100 -p 80
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-23 15:29 EDT
Nmap scan report for 192.168.2.100
Host is up (0.00062s latency).
Not shown: 65534 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.67 seconds
```

Prova di accesso alla DVWA su Metasploitable 2 con regola di blocco sul firewall



Cattura dei pacchetti con Wireshark che mostra il mancato scambio di pacchetti con la DVWA

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.1.100	192.168.2.100	TCP	74	55134 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1
2	0.250362735	192.168.1.100	192.168.2.100	TCP	74	51992 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1
3	1.031027323	192.168.1.100	192.168.2.100	TCP	74	[TCP Retransmission] 55134 → 80 [SYN] Seq=0
4	1.259024616	192.168.1.100	192.168.2.100	TCP	74	[TCP Retransmission] 51992 → 80 [SYN] Seq=0
5	3.047311681	192.168.1.100	192.168.2.100	TCP	74	[TCP Retransmission] 55134 → 80 [SYN] Seq=0
6	3.271112890	192.168.1.100	192.168.2.100	TCP	74	[TCP Retransmission] 51992 → 80 [SYN] Seq=0
7	7.207100018	192.168.1.100	192.168.2.100	TCP	74	[TCP Retransmission] 55134 → 80 [SYN] Seq=0
8	7.467145304	192.168.1.100	192.168.2.100	TCP	74	[TCP Retransmission] 51992 → 80 [SYN] Seq=0

Prova di scansione con l'utility nmap sulla porta 80

```
(kali@kali)-[~]
$ nmap -A 192.168.2.100 -p 80
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-23 15:59 EDT
Nmap scan report for 192.168.2.100
Host is up (0.00084s latency).

PORT      STATE      SERVICE VERSION
80/tcp    filtered  http

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.45 seconds
```

Log del firewall dal quale si nota l'effettivo blocco delle richieste da Kali (192.168.1.100) verso la DVWA di Metasploitable (192.168.2.100:80)

✗	Jul 23 22:08:59	LAN	no kali to metasploitable DVWA (1690147184)	192.168.1.100:55134	192.168.2.100:80	TCP:SYN
✗	Jul 23 22:08:59	LAN	no kali to metasploitable DVWA (1690147184)	192.168.1.100:51992	192.168.2.100:80	TCP:SYN
✗	Jul 23 22:09:31	LAN	no kali to metasploitable DVWA (1690147184)	192.168.1.100:55134	192.168.2.100:80	TCP:SYN
✗	Jul 23 22:09:33	LAN	no kali to metasploitable DVWA (1690147184)	192.168.1.100:51992	192.168.2.100:80	TCP:SYN