

In questo esercizio si creerà una struttura in cui si avrà Pfsense come tramite tra la macchina host e macchine virtuali.

Prima di tutto si andrà a modificare gli indirizzi delle macchine in questo modo:

Kali: 192.168.50.100

Windows: 192.168.50.102

```
(kali㉿kali)-[~]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.50.100 netmask 255.255.255.0 broadcast 192.168.50.255  
    inet6 fe80::5254:7da8:25f8:fc25 prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:50:14:a1 txqueuelen 1000 (Ethernet)  
    RX packets 495 bytes 55940 (54.6 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 163 bytes 17941 (17.5 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
C:\Users\user>ipconfig  
  
Configurazione IP di Windows  
  
Scheda Ethernet Ethernet:  
  
    Suffisso DNS specifico per connessione:  
    Indirizzo IPv4. . . . . : 192.168.50.102  
    Subnet mask . . . . . : 255.255.255.0  
    Gateway predefinito . . . . . : 192.168.50.1
```

Mentre Meta in un'altra rete: 192.168.51.101

```
msfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet  HWaddr 08:00:27:4e:32:53  
    inet addr:192.168.51.101 Bcast:192.168.51.255 Mask:255.255.255.0  
    inet6 addr: fe80::a00:27ff:fe4e:3253/64 Scope:Link  
    UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
    RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
    TX packets:61 errors:0 dropped:0 overruns:0 carrier:0  
    collisions:0 txqueuelen:1000  
    RX bytes:0 (0.0 B)  TX bytes:4626 (4.5 KB)  
    Base address:0xd020 Memory:f0200000-f0220000
```

Intanto su pfSense impostiamo la lan 1 con indirizzo 192.168.50.1

Invece per le impostazioni delle schede di rete:

Scheda di rete 1: Bridged (collegata con la Wan)

Scheda di rete 2: Interna (192.168.50.1, collegata con Kali e Windows)

Scheda di rete 3: Interna (192.168.51.1, collegata con Meta, cambiando il nome della rete sia su pfSense che su meta, inserendo la stessa.)

```
>
Configure IPv6 address LAN interface via DHCP6? (y/n) n

Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 192.168.50.2
Enter the end address of the IPv4 client address range: 192.168.50.254
Disabling IPv6 DHCPD...

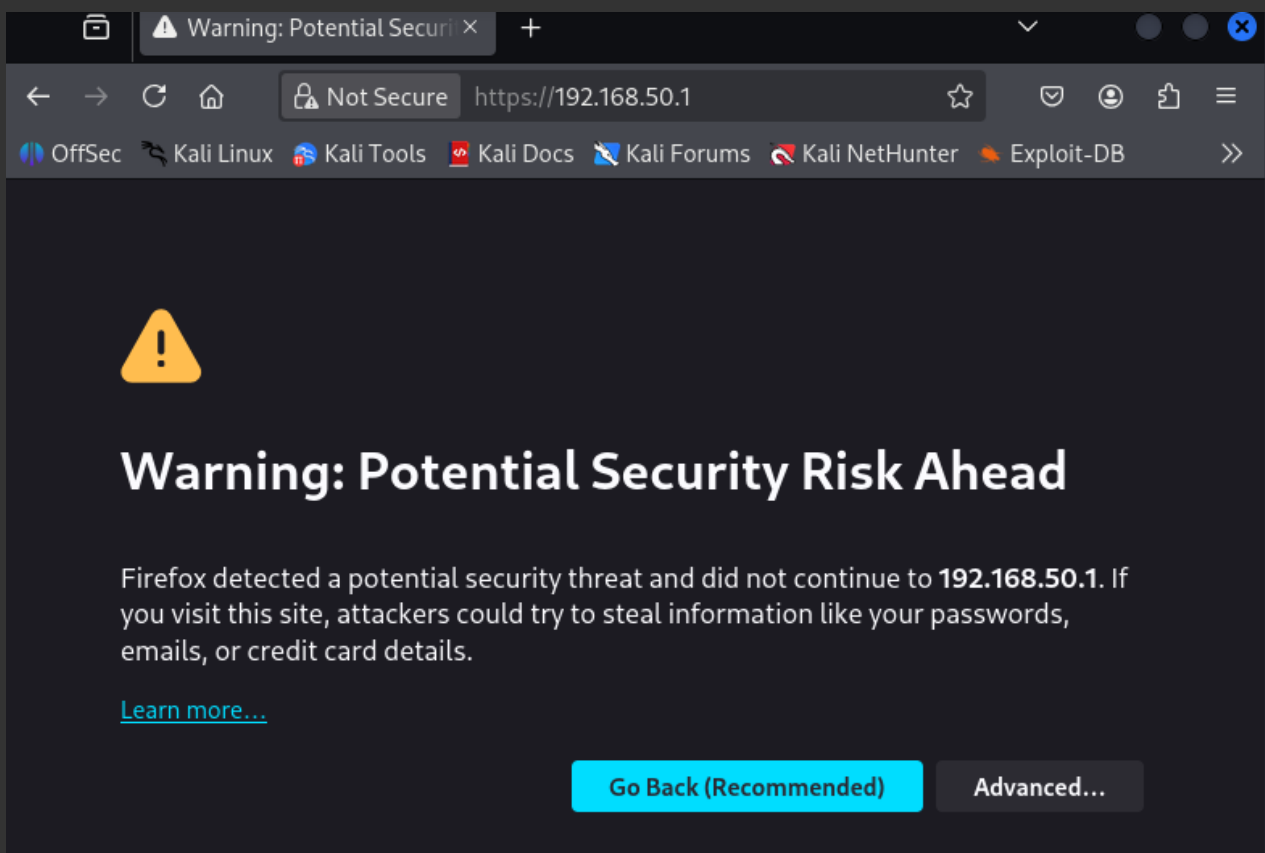
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

Please wait while the changes are saved to LAN...
Reloading filter...
Reloading routing configuration...
DHCPD...

The IPv4 LAN address has been set to 192.168.50.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
        https://192.168.50.1/

Press <ENTER> to continue.█
```

Ora riusciamo ad accedere alla DVWA di Meta da Kali



Andiamo dunque a configurare pfSense dall'interfaccia grafica accedendo da Kali, e impostando le 2 Lan.

[Wizard](#) / [pfSense Setup](#) / [Wizard completed.](#)

Step 9 of 9

Wizard completed.

Congratulations! pfSense is now configured.

We recommend that you check to see if there are any software updates available. Keeping your software up to date is one of the most important things you can do to maintain the security of your network.

[Check for updates](#)

Remember, we're here to help.

[Click here](#) to learn about Netgate 24/7/365 support services.



User survey

Please help all the people involved in improving and expanding pfSense software by taking a moment to answer this short survey (all answers are anonymous)

[Anonymous User Survey](#)

Useful resources.

- Learn more about Netgate's product line, services, and pfSense software from our [website](#)
- To learn about Netgate appliances and other offers, [visit our store](#)
- Become part of the pfSense community. Visit our [forum](#)
- Subscribe to our [newsletter](#) for ongoing product information, software announcements and special offers.



 COMMUNITY EDITION 


WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

[Interfaces](#) / [Interface Assignments](#)

[Interface Assignments](#) [Interface Groups](#) [Wireless](#) [VLANs](#) [QinQs](#) [PPPs](#) [GREs](#) [GIFs](#) [Bridges](#)

LAGGs

Interface	Network port
WAN	<input type="text" value="em0 (08:00:27:19:9d:fc)"/>
LAN	<input type="text" value="em1 (08:00:27:1d:f5:03)"/>  Delete
LAN2	<input type="text" value="em2 (08:00:27:c4:7c:7f)"/>  Delete

 Save

Si imposteranno le interfacce nel seguente modo:

```
The IPv4 OPT1 address has been set to 192.168.51.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
    https://192.168.51.1/

Press <ENTER> to continue.
VirtualBox Virtual Machine - Netgate Device ID: 4496a2c206b132ccee36

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

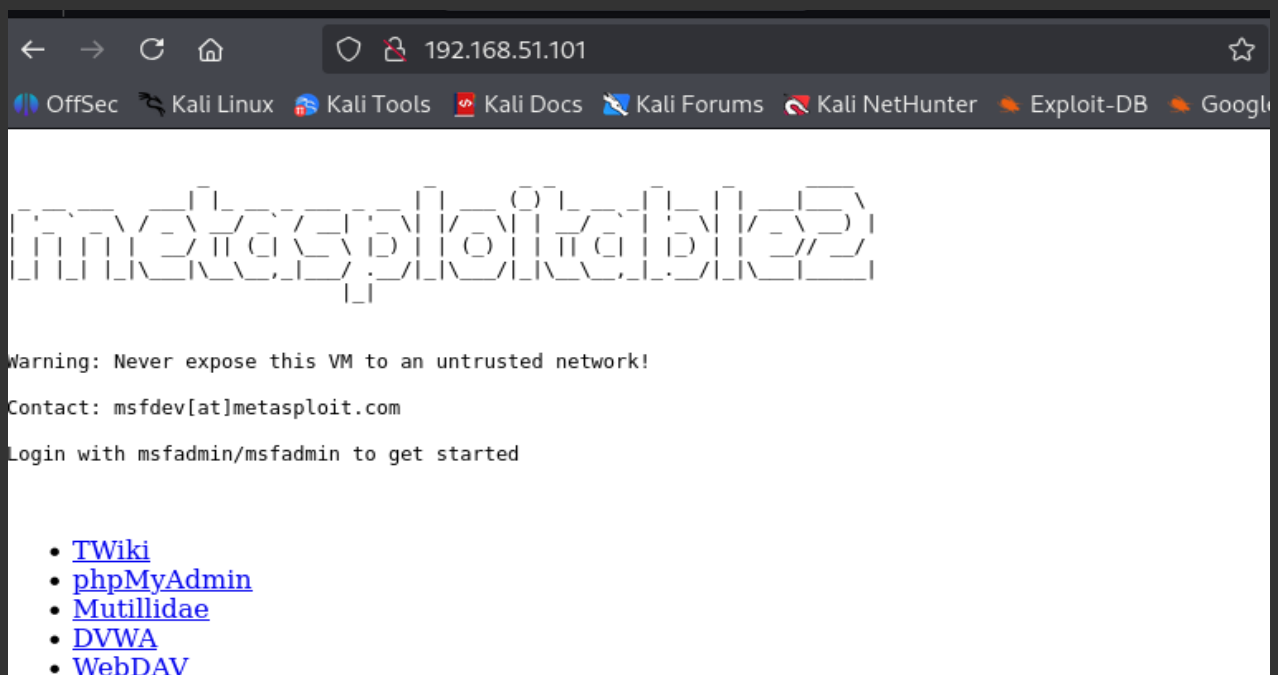
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.13/24
LAN (lan)      -> em1      -> v4: 192.168.50.1/24
LAN2 (opt1)    -> em2      -> v4: 192.168.51.1/24

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: █
```

Ora riusciamo a pingare Meta da Kali, ed anche ad accedere alla DVWA

```
(kali㉿kali)-[~]
$ ping 192.168.51.101
PING 192.168.51.101 (192.168.51.101) 56(84) bytes of data.
64 bytes from 192.168.51.101: icmp_seq=1 ttl=63 time=3.26 ms
64 bytes from 192.168.51.101: icmp_seq=2 ttl=63 time=2.03 ms
64 bytes from 192.168.51.101: icmp_seq=3 ttl=63 time=3.47 ms
64 bytes from 192.168.51.101: icmp_seq=4 ttl=63 time=3.89 ms
^C
— 192.168.51.101 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 2.034/3.162/3.888/0.689 ms
```



← → ↻ 🏠 192.168.51.101 ☆

OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google

DVWA

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](#)

Ora si va a creare una regola nella quale si blocca la porta 80 nella Lan 2, quindi non dovremmo essere più in grado di accedere alla DVWA di Meta da Kali.

Source

Source

☐ Invert match

Address or Alias

192.168.50.100

/

⚙ 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

☐ Invert match

Address or Alias

192.168.51.101

/

Destination Port Range

HTTP (80)

From

Custom

To

HTTP (80)

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

☒ 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

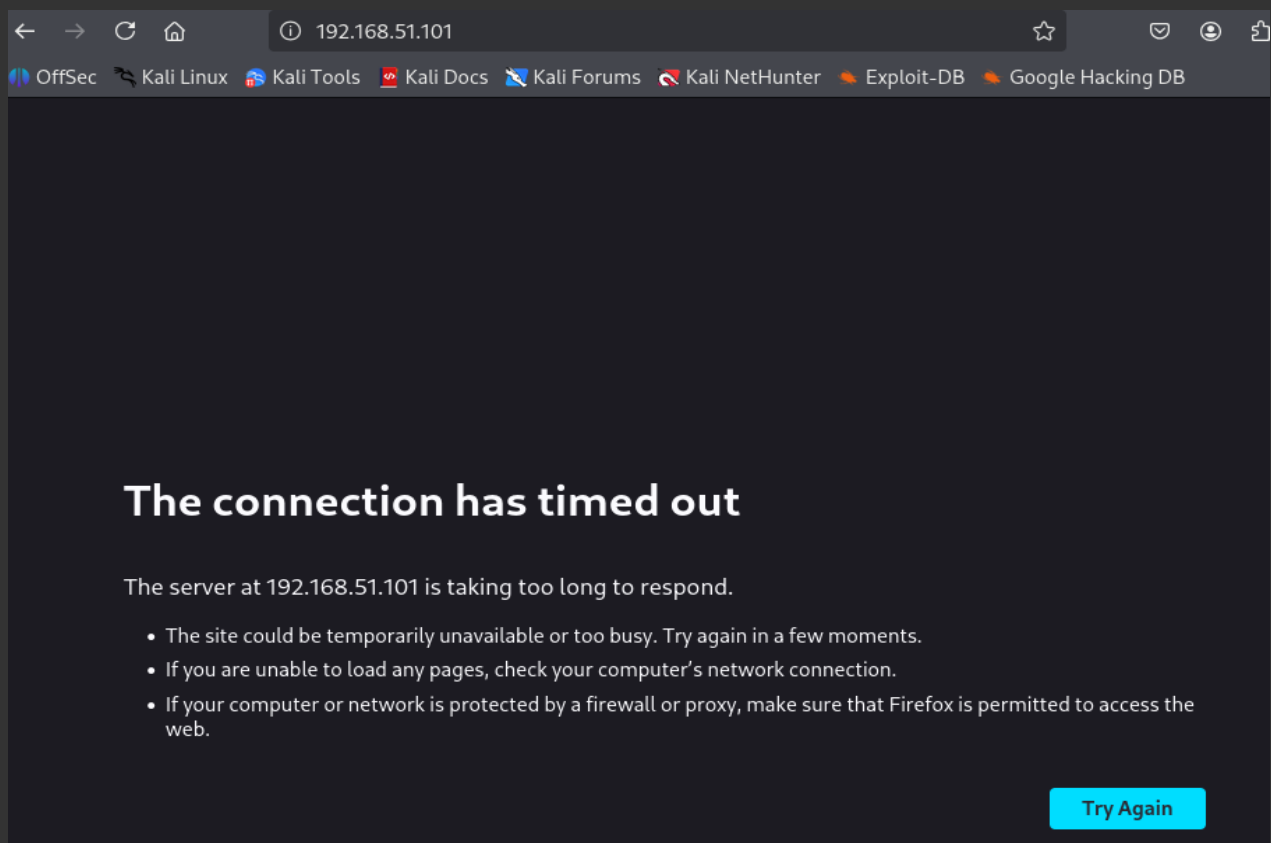
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options

⚙ Display Advanced

Rule Information

Adesso riprovando ad accedere alla DVWA dà errore.



Anche su Wireshark possiamo vedere come il traffico viene bloccato

The image shows a Wireshark packet capture window titled "Capturing from eth0". The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help) and a toolbar. A display filter is applied: "Apply a display filter ... <Ctrl-/>".

The packet list pane shows the following packets:

No.	Time	Source	Destination	Protocol	Length	Info
4	0.047483956	192.168.50.100	192.168.50.1	TCP	66	43510 → 443 [ACK] Seq=40 Ack=40 Win=1562 Len=0 TS=...
5	6.264303397	192.168.50.100	192.168.51.101	TCP	74	35790 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S...
6	6.514359214	192.168.50.100	192.168.51.101	TCP	74	35792 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S...
7	7.275946734	192.168.50.100	192.168.51.101	TCP	74	[TCP Retransmission] 35790 → 80 [SYN] Seq=0 Win=6...
8	7.531184594	192.168.50.100	192.168.51.101	TCP	74	[TCP Retransmission] 35792 → 80 [SYN] Seq=0 Win=6...
9	8.301363900	192.168.50.100	192.168.51.101	TCP	74	[TCP Retransmission] 35790 → 80 [SYN] Seq=0 Win=6...
10	8.555478741	192.168.50.100	192.168.51.101	TCP	74	[TCP Retransmission] 35792 → 80 [SYN] Seq=0 Win=6...
11	9.323314726	192.168.50.100	192.168.51.101	TCP	74	[TCP Retransmission] 35790 → 80 [SYN] Seq=0 Win=6...
12	9.579419181	192.168.50.100	192.168.51.101	TCP	74	[TCP Retransmission] 35792 → 80 [SYN] Seq=0 Win=6...
13	10.347891680	192.168.50.100	192.168.51.101	TCP	74	[TCP Retransmission] 35790 → 80 [SYN] Seq=0 Win=6...
14	10.603556573	192.168.50.100	192.168.51.101	TCP	74	[TCP Retransmission] 35792 → 80 [SYN] Seq=0 Win=6...
15	11.245959492	192.168.50.1	192.168.50.100	TLSv1.2	105	Application Data
16	11.246021562	192.168.50.100	192.168.50.1	TCP	66	43510 → 443 [ACK] Seq=40 Ack=79 Win=1562 Len=0 TS=...
17	11.246296465	192.168.50.1	192.168.50.100	TLSv1.2	90	Application Data
18	11.246302519	192.168.50.100	192.168.50.1	TCP	66	43510 → 443 [ACK] Seq=40 Ack=103 Win=1562 Len=0 T...
19	11.246706360	192.168.50.100	192.168.50.1	TLSv1.2	105	Application Data
20	11.247274614	192.168.50.100	192.168.50.1	TLSv1.2	90	Application Data

The packet details pane for Frame 9 shows the following structure:

- Frame 9: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0
- Ethernet II, Src: PCSSystemtec_50:14:a1 (08:00:27:50:14:a1), Dst: 192.168.51.101
- Internet Protocol Version 4, Src: 192.168.50.100, Dst: 192.168.51.101
- Transmission Control Protocol, Src Port: 35790, Dst Port: 80

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 08 00 27 1d f5 03 08 00 27 50 14 a1 08 00 45 00  ...'....
0010 00 3c ab 47 40 00 40 06 a8 5a c0 a8 32 64 c0 a8  <.G@.
0020 33 65 8b ce 00 50 44 3c f3 af 00 00 00 00 a0 02  3e...PD
0030 fa f0 e7 48 00 00 02 04 05 04 04 02 08 0a 95 83  ...H...
0040 b5 7c 00 00 00 00 01 03 03 07                    -|....
```