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

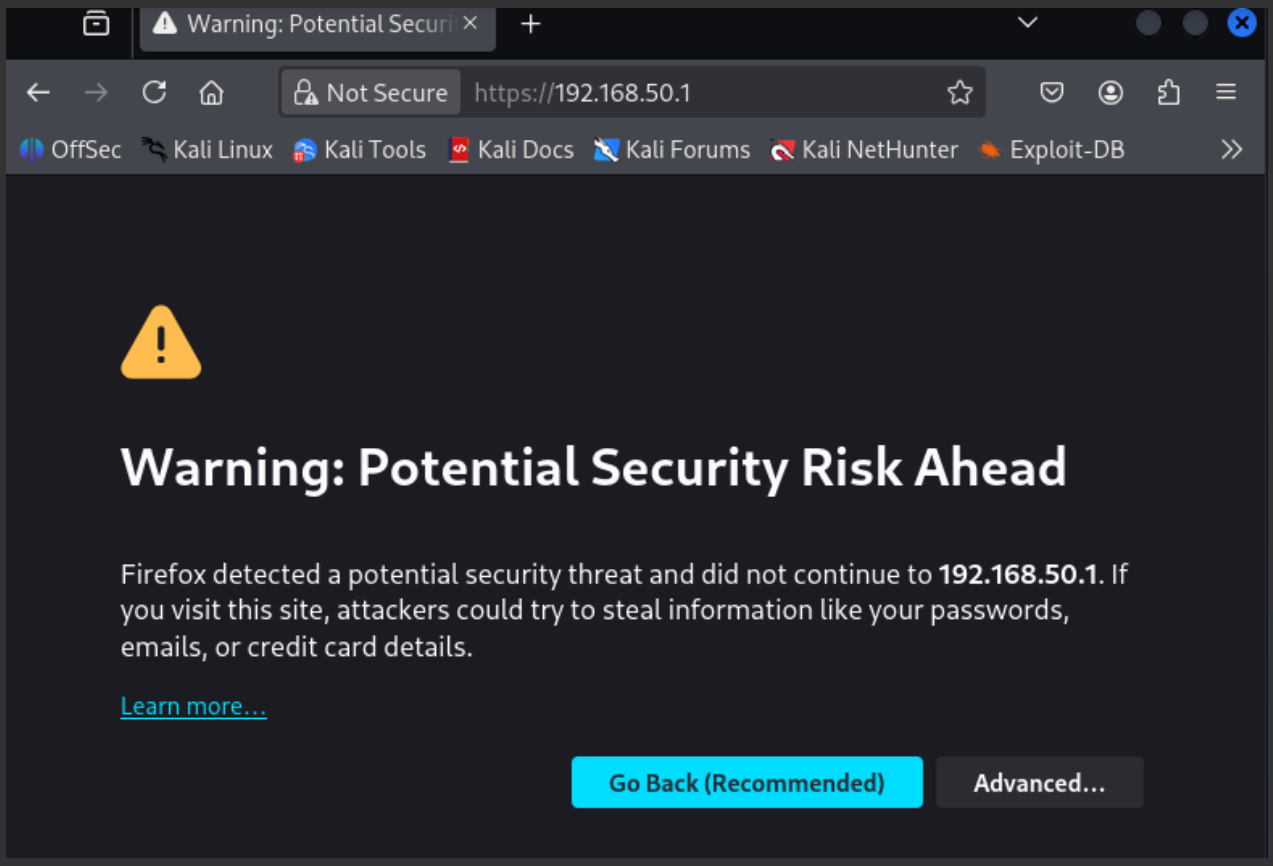
```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:4e:32:53
          inet addr:192.168.51.101  Bcast:192.168.51.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe4e:3253/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          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

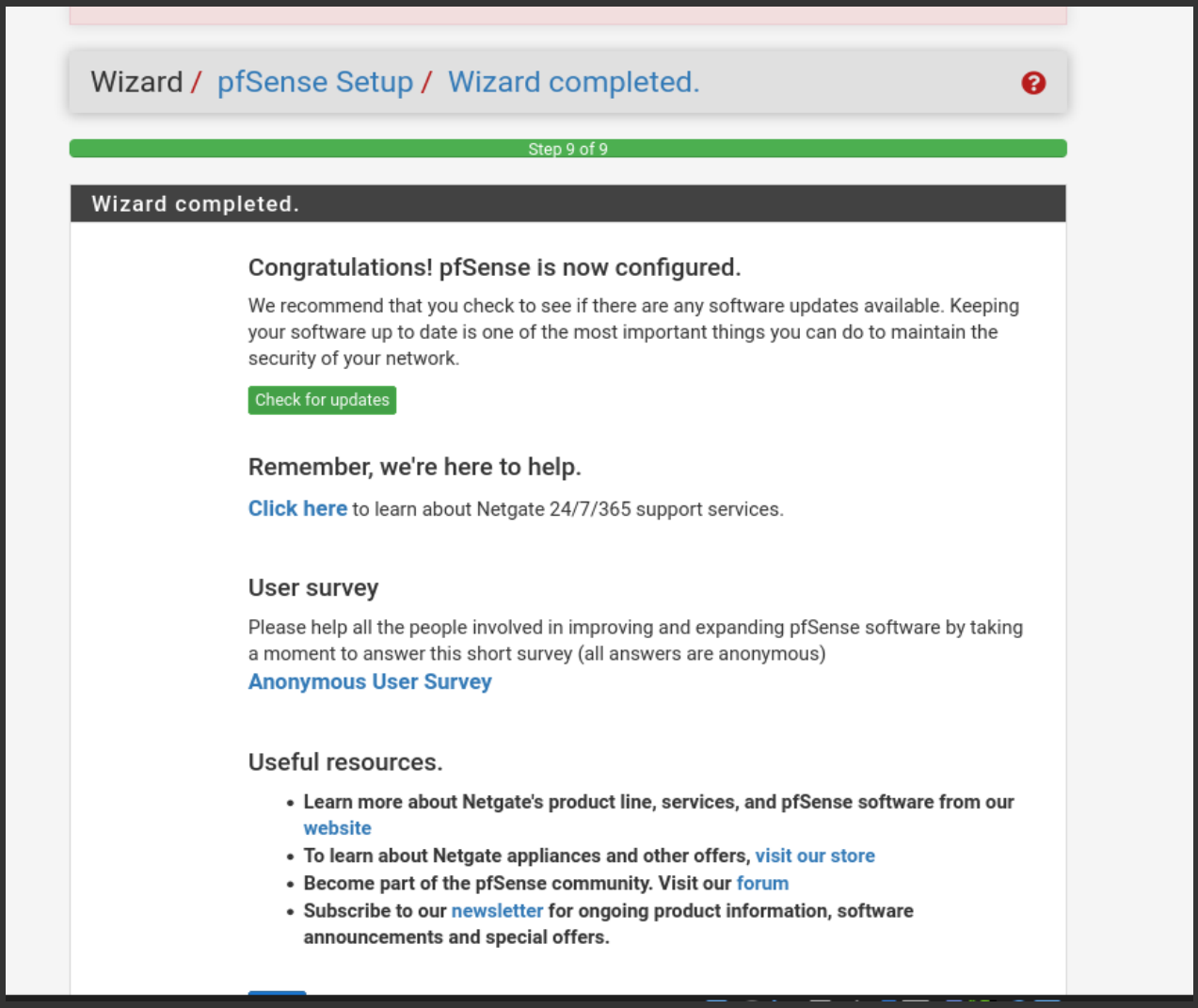
Invece per le impostazioni delle schede di rete:
Scheda di rete 1: Bridged (collegata con la Wan)
Scheda di rete 2: Interna (192.168.50.1, collegata con Kali e Windows)
Scheda di rete 3: Interna (192.168.51.1, collegata con Meta, cambiando il nome della rete sia su pfSense che su meta, inserendo la stessa.)

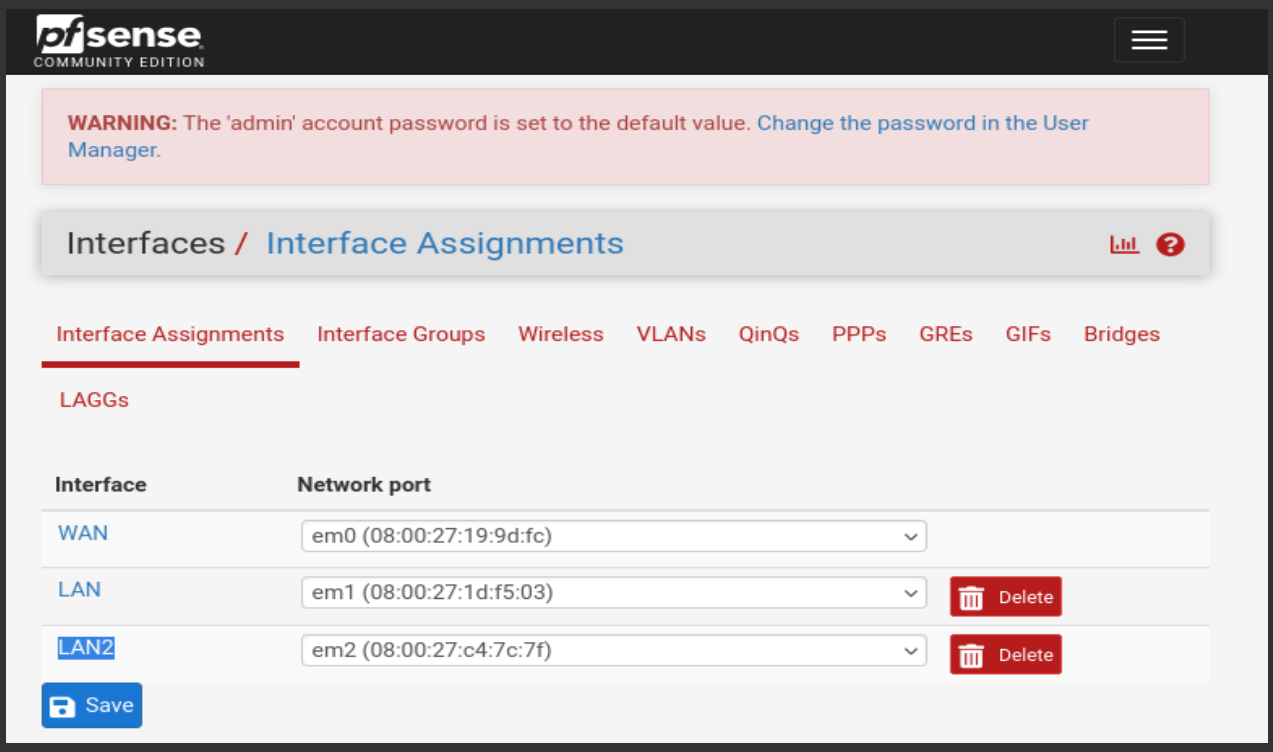
```
>

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.



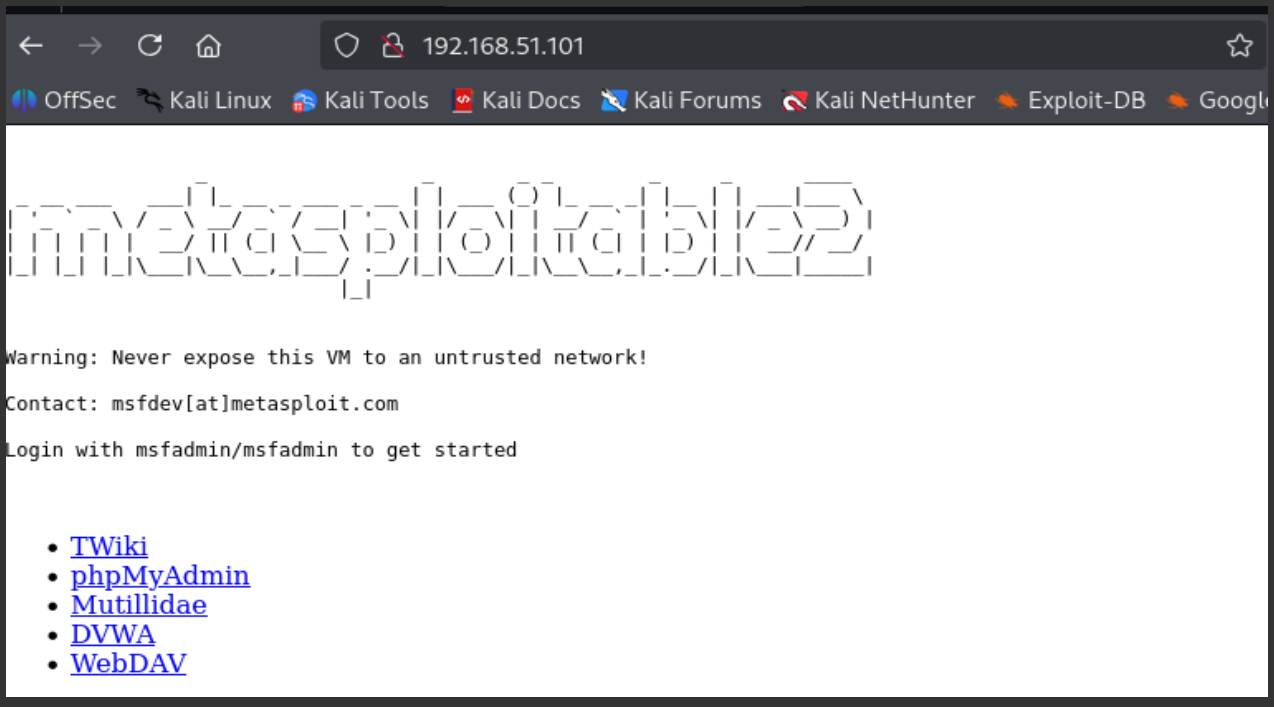


Si imposteranno le interfacce nel seguente modo:

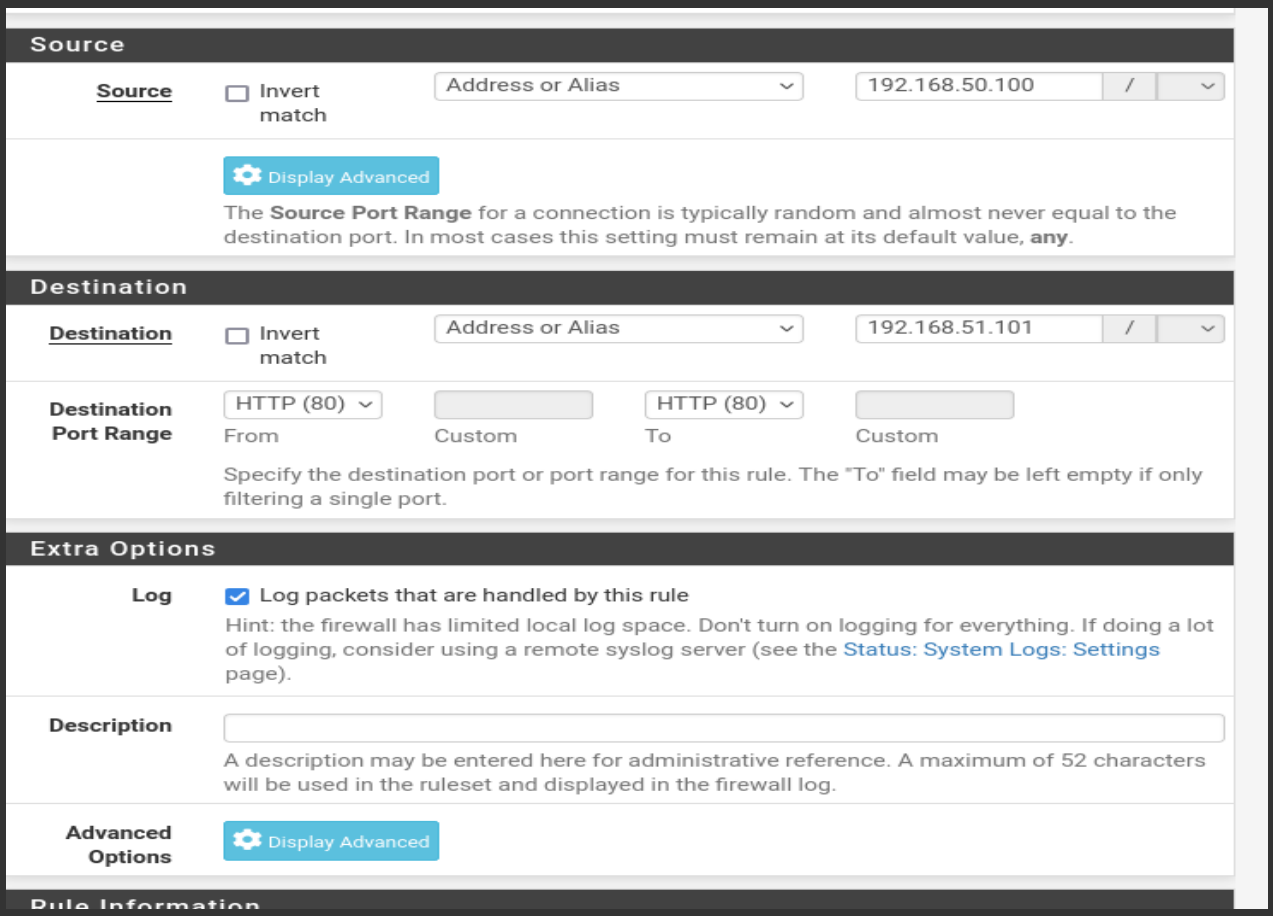
```
The IPv4 OPT1 address has been set to 192.168.51.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                https://192.168.51.1/

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

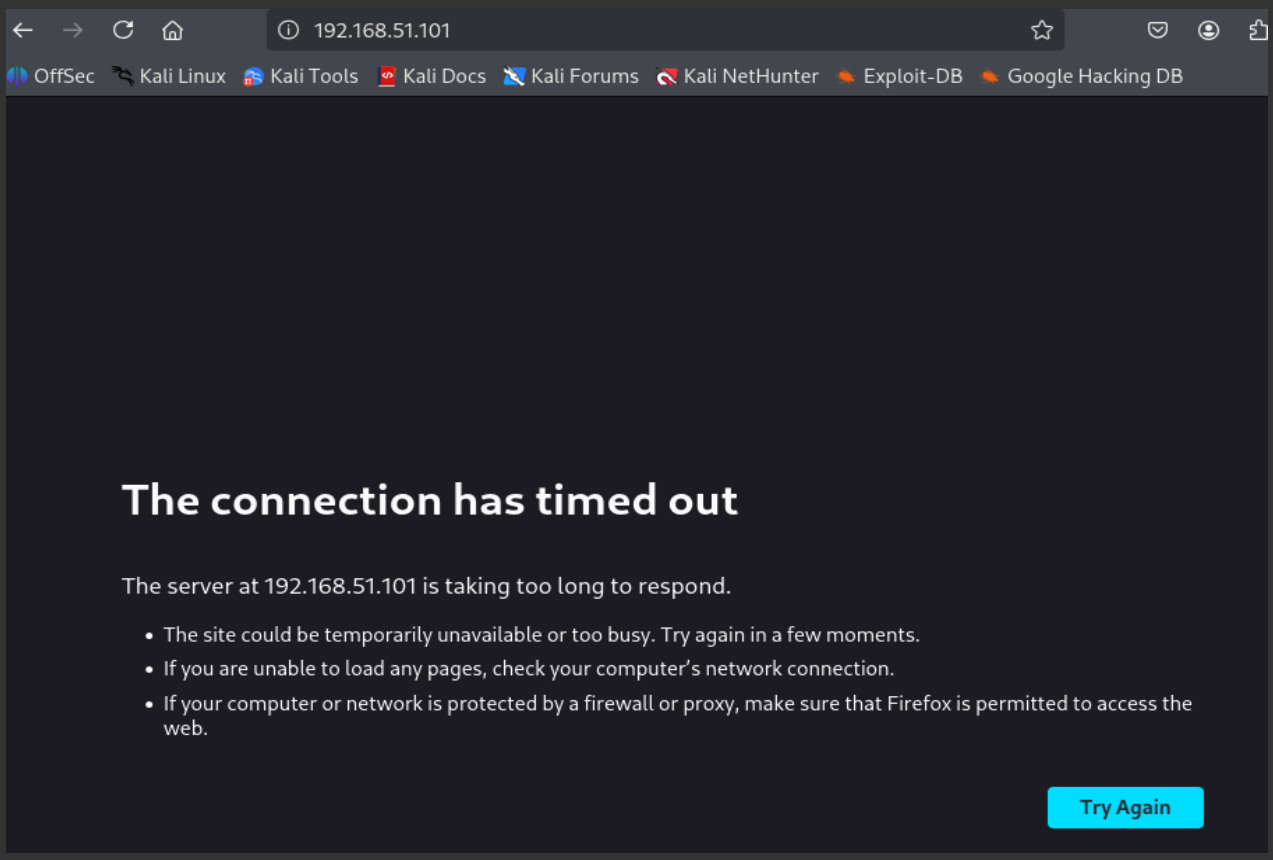
```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.51.101
PING 192.168.51.101 (192.168.51.101) 56(84) bytes of data.
64 bytes from 192.168.51.101: icmp_seq=1 ttl=63 time=3.26 ms
64 bytes from 192.168.51.101: icmp_seq=2 ttl=63 time=2.03 ms
64 bytes from 192.168.51.101: icmp_seq=3 ttl=63 time=3.47 ms
64 bytes from 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
```



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.



Adesso riprovando ad accedere alla DVWA dà errore.



Anche su Wireshark possiamo vedere come il traffico viene bloccato