

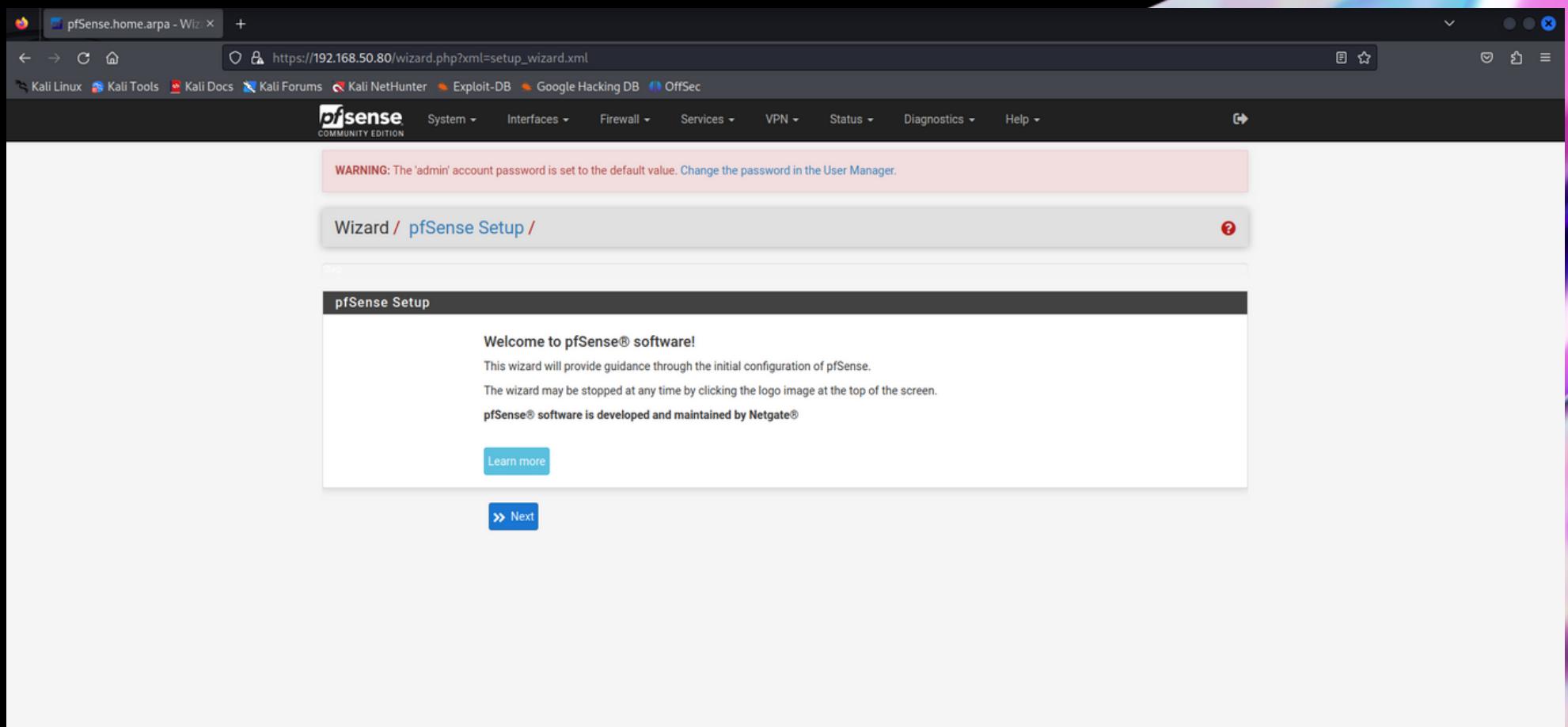


Consegna S5/L1 CyberSecurity

Penetration Testing: Introduzione



Per eseguire l'esercizio di oggi il primo passo è installare una nuova macchina virtuale con OS pfSense, una distribuzione software open source basata su FreeBSD adatta per essere utilizzata come firewall/router. Per eseguire l'accesso l'username e la password di default sono «admin» e «pfSense».





A questo punto possiamo configurare l'interfaccia di rete posta sulla LAN2 e per verificare che tutto sia corretto impostiamo una prima regola che ci permette a connetterci al DVWA di metasploitable2

General Configuration

Enable	<input checked="" type="checkbox"/> Enable interface
Description	LAN2 Enter a description (name) for the interface here.
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	None
MAC Address	XXXX:XX:XX:XX:XX: This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xx:xx:xx:xx:xx or leave blank.
MTU	<input type="text"/> If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS	<input type="text"/> If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.
Speed and Duplex	Default (no preference, typically autoselect) Explicitly set speed and duplex mode for this interface. WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Static IPv4 Configuration

IPv4 Address	192.168.32.80
IPv4 Upstream gateway	None + Add a new 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](#).

Firewall / Rules / LAN2

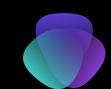
Floating	WAN	LAN	LAN2								
Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/4 KiB	IPv4 *	LAN2 subnets	*	*	*	*	none		Default allow LAN to any rule	
↑ Add ↓ Add Delete Toggle Copy Save + Separator											



Controlliamo la connettività

The screenshot shows a web browser window with the address bar displaying `192.168.32.101/dvwa/login.php`. The DVWA logo is centered above a login form. The form contains fields for 'Username' and 'Password', both currently empty. A 'Login' button is located below the password field. At the bottom of the page, there is a note about the Damn Vulnerable Web Application (DVWA) being a RandomStorm OpenSource project, with a hint that the default username is 'admin' and the password is 'password'.

Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project
Hint: default username is 'admin' with password 'password'

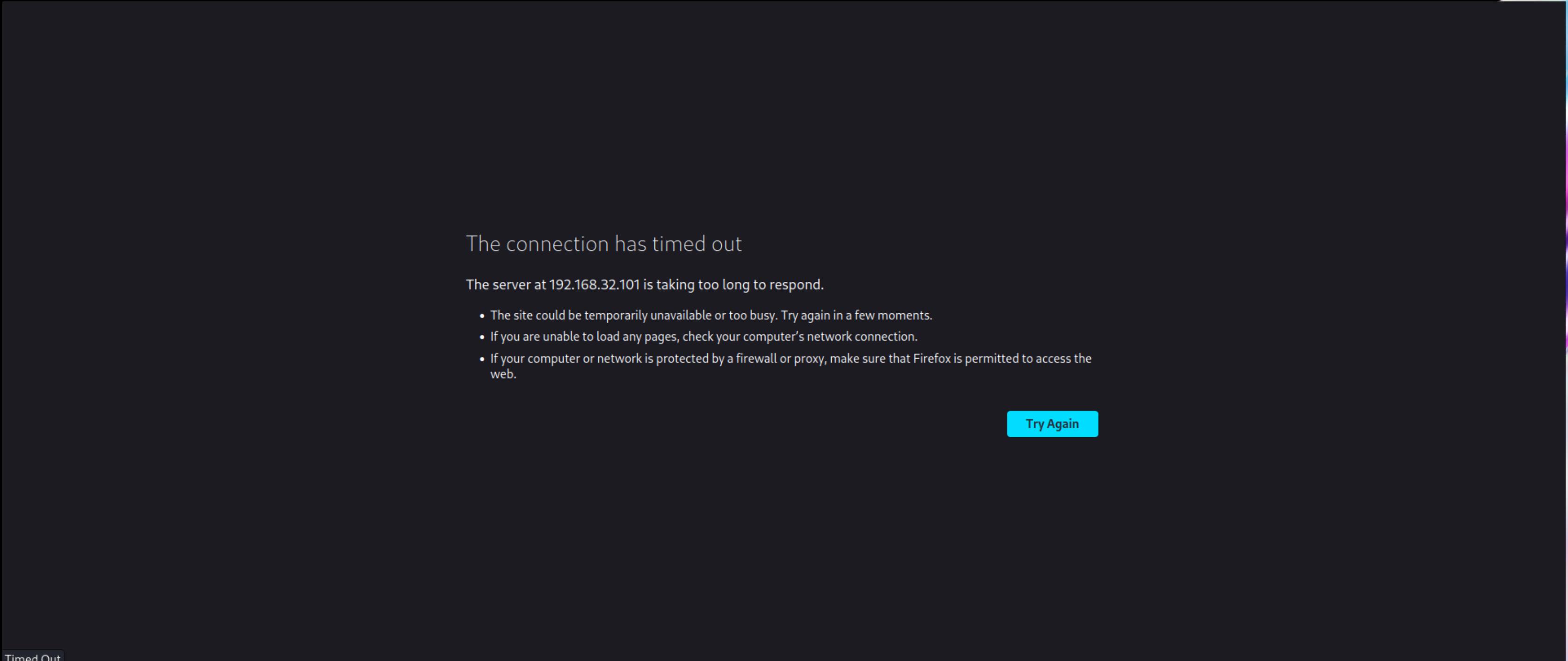


A questo punto aggiungiamo una regola al firewall per impedire l'accesso dalla macchina di kali linux al server di meta:





Verifichiamo che non c'è più possibilità di connessione con il dvwa di meta:





Non ci resta che verificare che le due macchine restano comunque in comunicazione pur non potendo sfruttare i servizi web offerti da metà.

Per fare questo ci facciamo aiutare dallo scan di nmap che ci dice che a quell'ip è presente un host ma non trova nessuna porta aperta. In successione verifichiamo la connettività con un ping.

```
(kali㉿kali) - [~]
└$ sudo nmap 192.168.32.101 -ss
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-18 13:16 CET
Nmap scan report for 192.168.32.101
Host is up (0.0073s latency).
All 1000 scanned ports on 192.168.32.101 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 34.93 seconds
```

```
(kali㉿kali) - [~]
└$ ping 192.168.32.101
PING 192.168.32.101 (192.168.32.101) 56(84) bytes of data.
64 bytes from 192.168.32.101: icmp_seq=1 ttl=63 time=8.43 ms
64 bytes from 192.168.32.101: icmp_seq=2 ttl=63 time=16.6 ms
64 bytes from 192.168.32.101: icmp_seq=3 ttl=63 time=2.00 ms
64 bytes from 192.168.32.101: icmp_seq=4 ttl=63 time=17.0 ms
64 bytes from 192.168.32.101: icmp_seq=5 ttl=63 time=2.17 ms
64 bytes from 192.168.32.101: icmp_seq=6 ttl=63 time=6.36 ms
64 bytes from 192.168.32.101: icmp_seq=7 ttl=63 time=2.37 ms
64 bytes from 192.168.32.101: icmp_seq=8 ttl=63 time=10.2 ms
^C
--- 192.168.32.101 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7013ms
rtt min/avg/max/mdev = 2.004/8.142/17.031/5.746 ms
```

```
(kali㉿kali) - [~]
└$
```