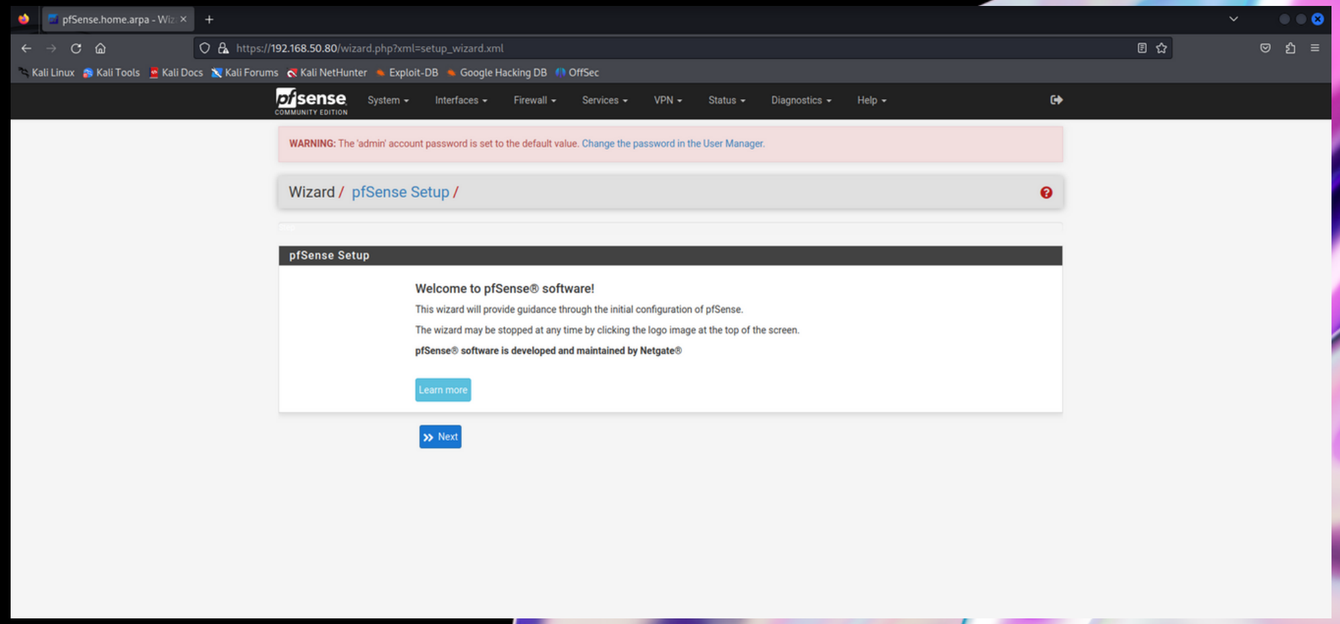
RICCARDO AGOSTINO MONTI

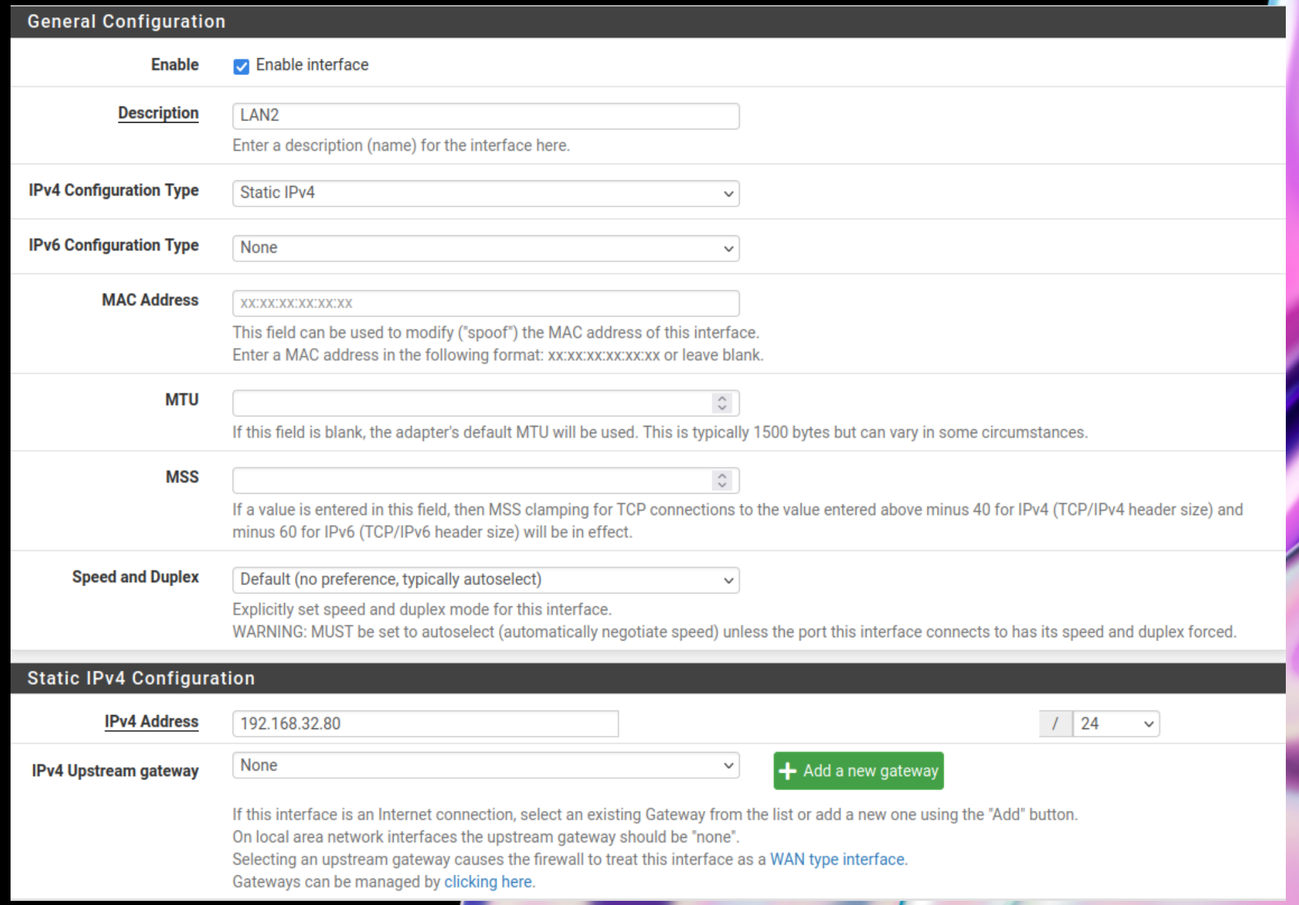
Consegna S5/L1 CyberSecurity

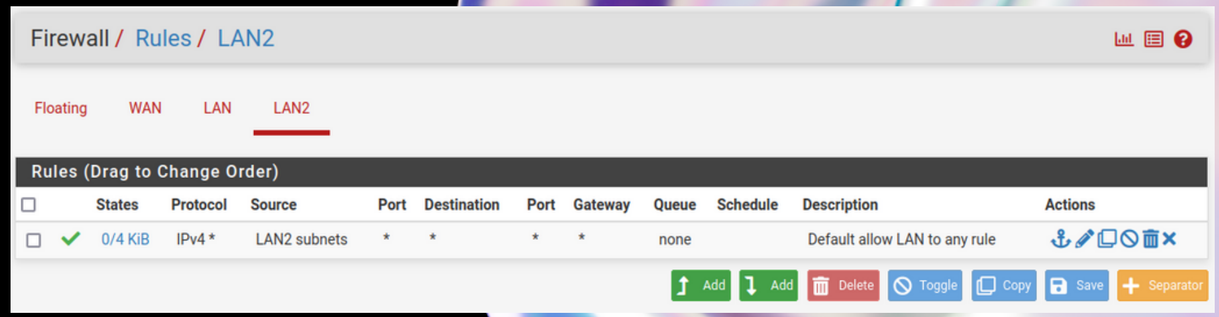
Penetration Testing: Introduzione

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».

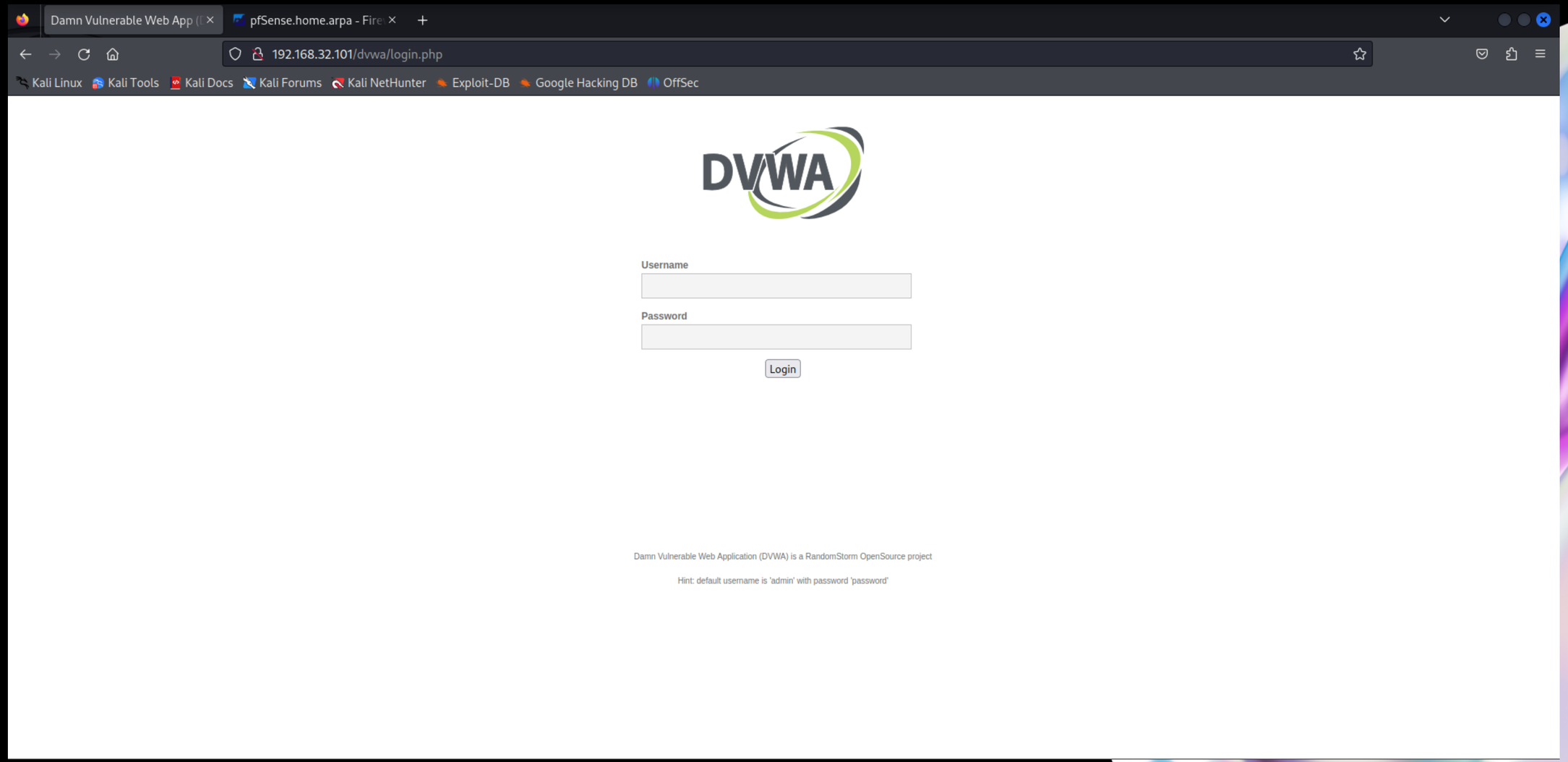


A questo punto possiamo configurare l’interfaccia di rete posta sulla LAN2 e per verificare che tutto sia corretto impostiamo una prima regola che ci permette a connetterci al DVWA di metasploitable2



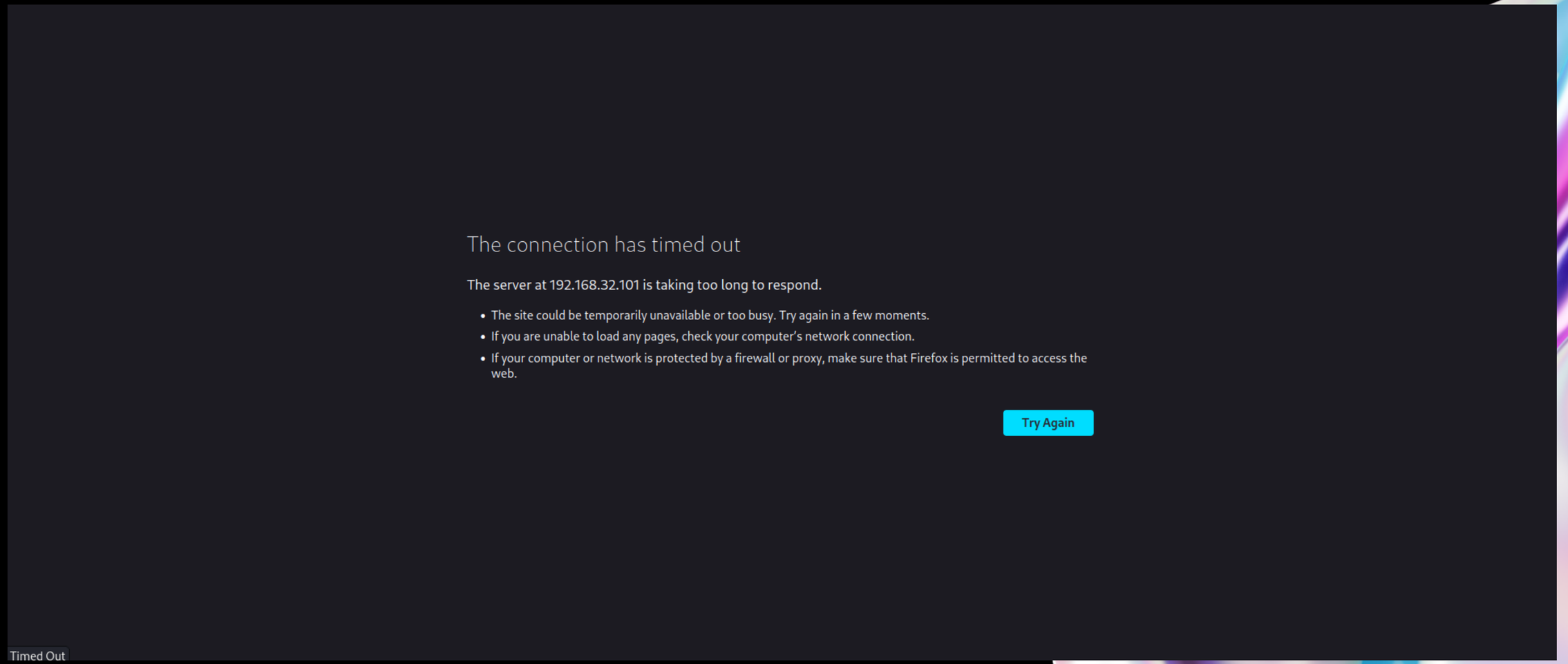


Controlliamo la connettività



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 meta.
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)-[~]
└─$
```