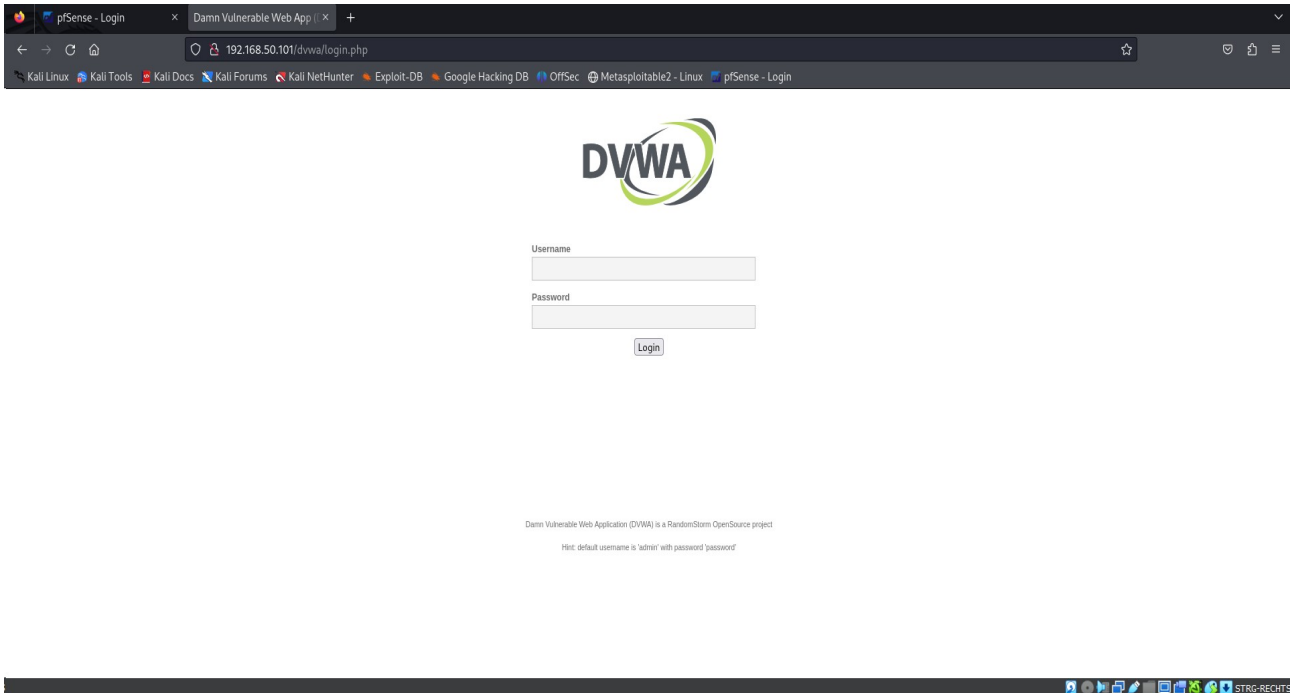
Creazione regola firewall

In questo esercizio siamo andati a creare una regola del firewall che bloccasse l'accesso al sito della DVWA di Metasploitable.

Appena installato e configurato il firewall possiamo notare che l'accesso a DVWA è consentito.



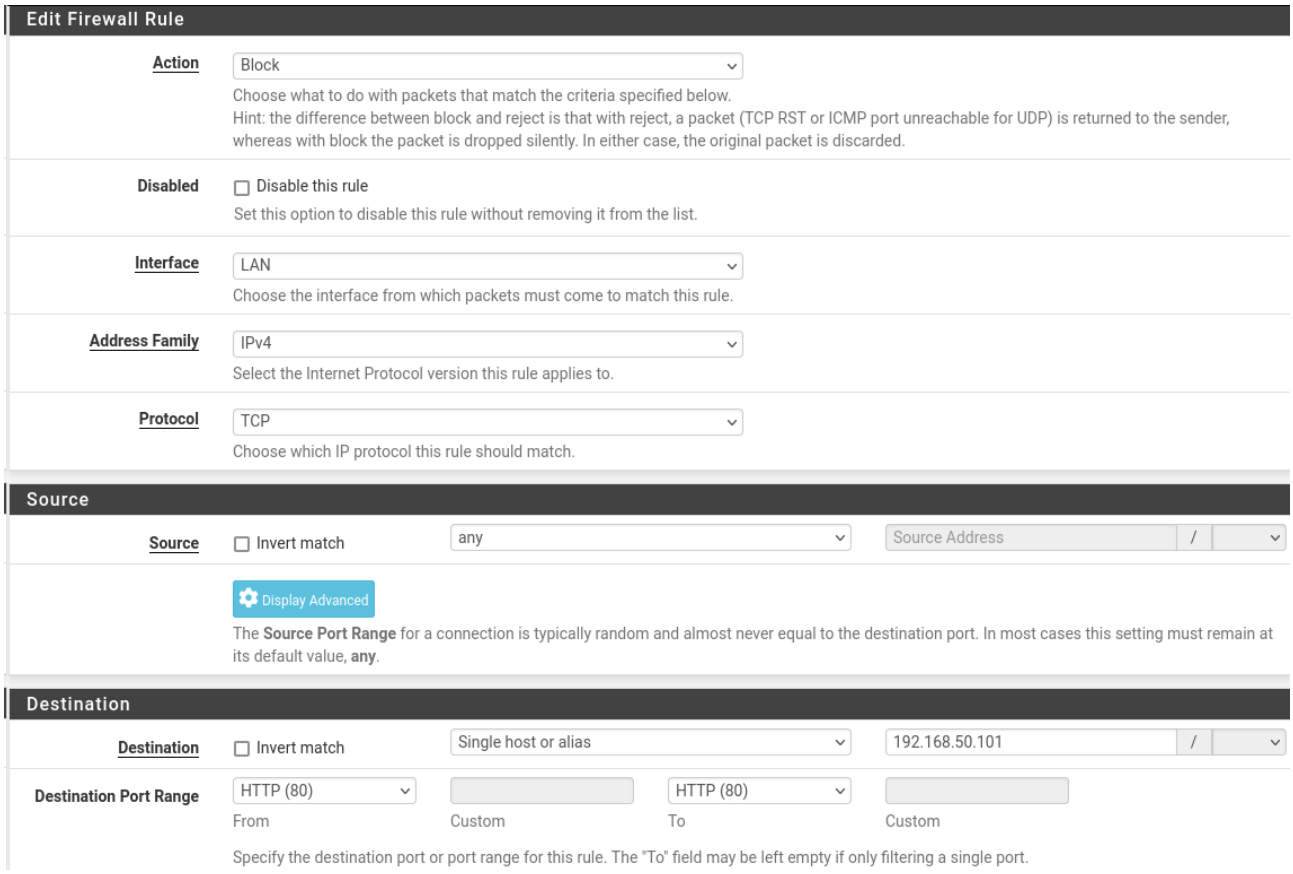
Andiamo quindi a settare la regola.

Controlliamo intanto che le macchine Kali e Metasploitable pingano tra loro.

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.50.101
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data.
64 bytes from 192.168.50.101: icmp_seq=1 ttl=63 time=1.92 ms
64 bytes from 192.168.50.101: icmp_seq=2 ttl=63 time=2.23 ms
64 bytes from 192.168.50.101: icmp_seq=3 ttl=63 time=2.34 ms
64 bytes from 192.168.50.101: icmp_seq=4 ttl=63 time=2.28 ms
64 bytes from 192.168.50.101: icmp_seq=5 ttl=63 time=2.08 ms
64 bytes from 192.168.50.101: icmp_seq=6 ttl=63 time=2.03 ms
64 bytes from 192.168.50.101: icmp_seq=7 ttl=63 time=1.93 ms
^C64 bytes from 192.168.50.101: icmp_seq=8 ttl=63 time=2.03 ms
```

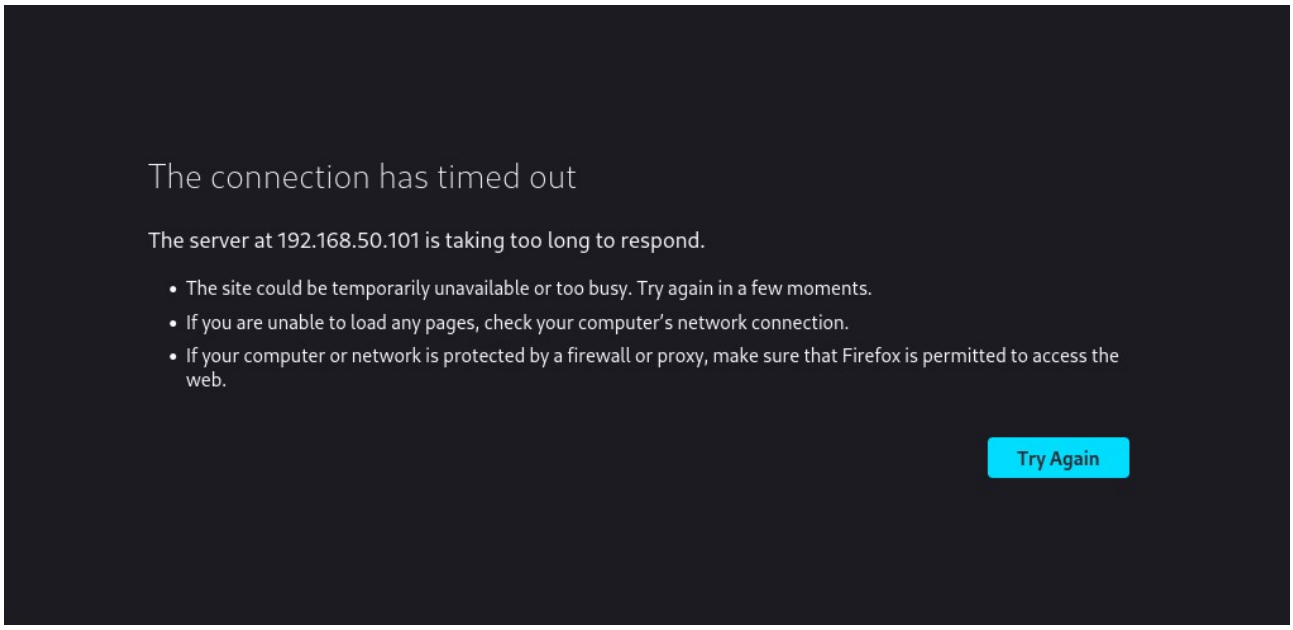
Una volta verificato che le macchine sono collegate. facciamo il login nel firewall, ci spostiamo sul menu firewall, nella cartella “rules”.

Qui possiamo impostare la nuova regola.



Abbiamo bloccato le richieste in uscita dalla nostra LAN con protocollo TCP e dirette verso l'indirizzo 192.168.50.101, che appartiene a Metasploitable, sulla porta 80, dedicata alle richieste HTTP.

Ora non abbiamo più l'accesso alla DVWA di Metasploitable:



Possiamo vedere anche dai log di sistema che viene applicata la regola del blocco dell'IP di Metasploitable:

✕	Oct 23 19:55:43	LAN	Block DVWA (1698089817)	192.168.1.100:42780	192.168.50.101:80	TCP:S
✕	Oct 23 19:55:43	LAN	Block DVWA (1698089817)	192.168.1.100:42784	192.168.50.101:80	TCP:S
✕	Oct 23 19:55:44	LAN	Block DVWA (1698089817)	192.168.1.100:42780	192.168.50.101:80	TCP:S
✕	Oct 23 19:55:44	LAN	Block DVWA (1698089817)	192.168.1.100:42784	192.168.50.101:80	TCP:S
✕	Oct 23 19:55:45	LAN	Block DVWA (1698089817)	192.168.1.100:42780	192.168.50.101:80	TCP:S
✕	Oct 23 19:55:45	LAN	Block DVWA (1698089817)	192.168.1.100:42784	192.168.50.101:80	TCP:S
✕	Oct 23 19:55:46	LAN	Block DVWA (1698089817)	192.168.1.100:42780	192.168.50.101:80	TCP:S
✕	Oct 23 19:55:46	LAN	Block DVWA (1698089817)	192.168.1.100:42784	192.168.50.101:80	TCP:S
✕	Oct 23 19:55:48	LAN	Block DVWA (1698089817)	192.168.1.100:42780	192.168.50.101:80	TCP:S
✕	Oct 23 19:55:48	LAN	Block DVWA (1698089817)	192.168.1.100:42784	192.168.50.101:80	TCP:S
✕	Oct 23 19:55:52	LAN	Block DVWA (1698089817)	192.168.1.100:42780	192.168.50.101:80	TCP:S
✕	Oct 23 19:55:52	LAN	Block DVWA (1698089817)	192.168.1.100:42784	192.168.50.101:80	TCP:S
✕	Oct 23 19:56:01	LAN	Block DVWA (1698089817)	192.168.1.100:42780	192.168.50.101:80	TCP:S
✕	Oct 23 19:56:01	LAN	Block DVWA (1698089817)	192.168.1.100:42784	192.168.50.101:80	TCP:S
✕	Oct 23 19:56:17	LAN	Block DVWA (1698089817)	192.168.1.100:42780	192.168.50.101:80	TCP:S
✕	Oct 23 19:56:17	LAN	Block DVWA (1698089817)	192.168.1.100:42784	192.168.50.101:80	TCP:S
✕	Oct 23 19:56:50	LAN	Block DVWA (1698089817)	192.168.1.100:42784	192.168.50.101:80	TCP:S
✕	Oct 23 19:56:50	LAN	Block DVWA (1698089817)	192.168.1.100:42780	192.168.50.101:80	TCP:S