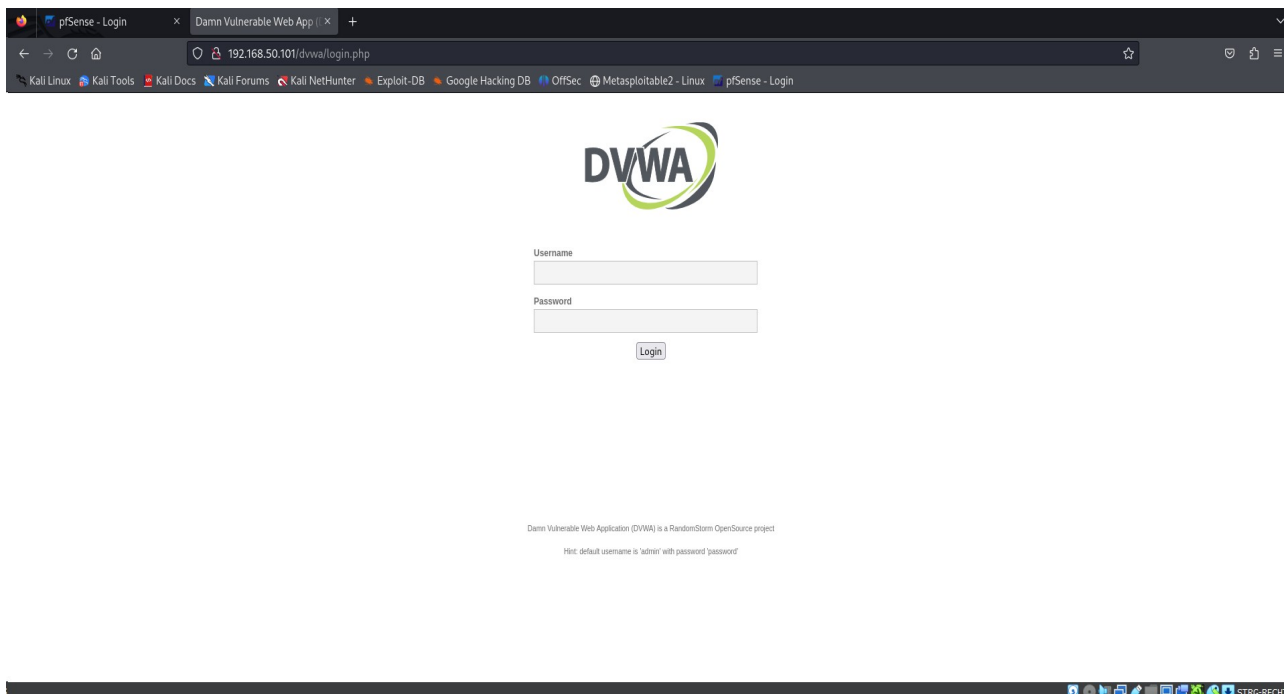


## Creazione regola firewall

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.

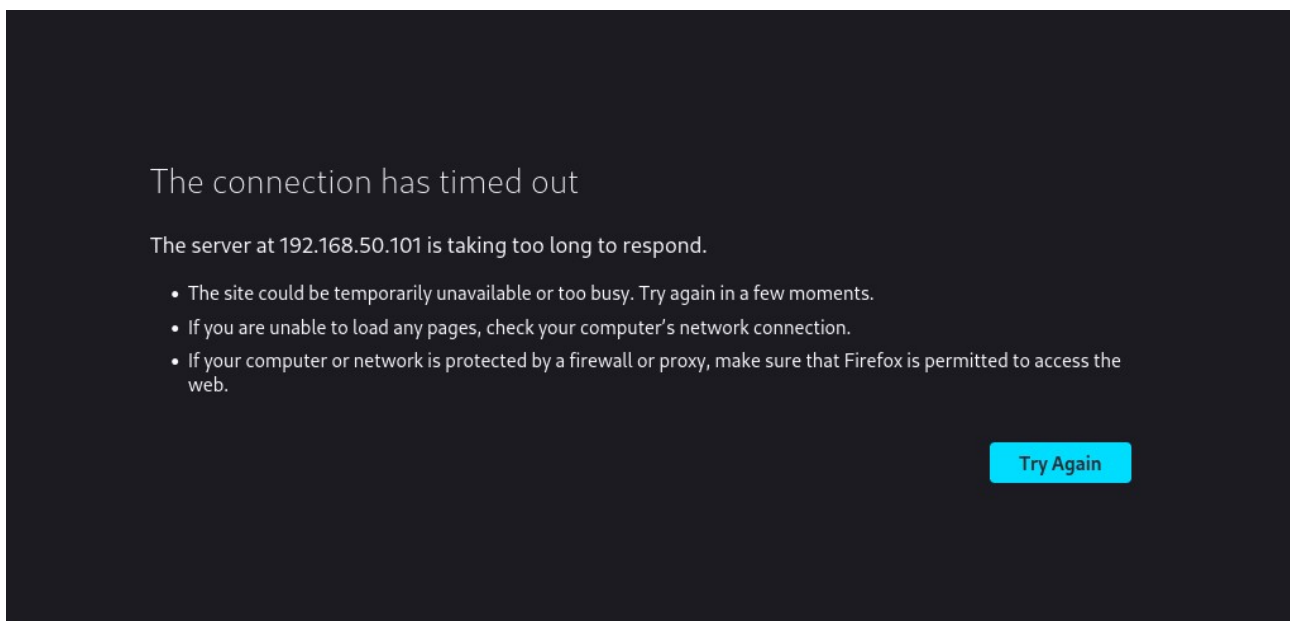
Edit Firewall Rule	
<b>Action</b>	<div>Block</div> <div>Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.</div>
<b>Disabled</b>	<div><input type="checkbox"/> Disable this rule</div> <div>Set this option to disable this rule without removing it from the list.</div>
<b>Interface</b>	<div>LAN</div> <div>Choose the interface from which packets must come to match this rule.</div>
<b>Address Family</b>	<div>IPv4</div> <div>Select the Internet Protocol version this rule applies to.</div>
<b>Protocol</b>	<div>TCP</div> <div>Choose which IP protocol this rule should match.</div>

Source	
<b>Source</b>	<div><input type="checkbox"/> Invert match</div> <div>any</div> <div>Source Address /</div>
<div> Display Advanced</div> <div>The <b>Source Port Range</b> 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, <b>any</b>.</div>	























































Destination	
<b>Destination</b>	<div><input type="checkbox"/> Invert match</div> <div>Single host or alias</div> <div>192.168.50.101 /</div>
<b>Destination Port Range</b>	<div><div>HTTP (80)</div><div>From</div><div>Custom</div><div>HTTP (80)</div><div>To</div><div>Custom</div></div> <div>Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.</div>

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