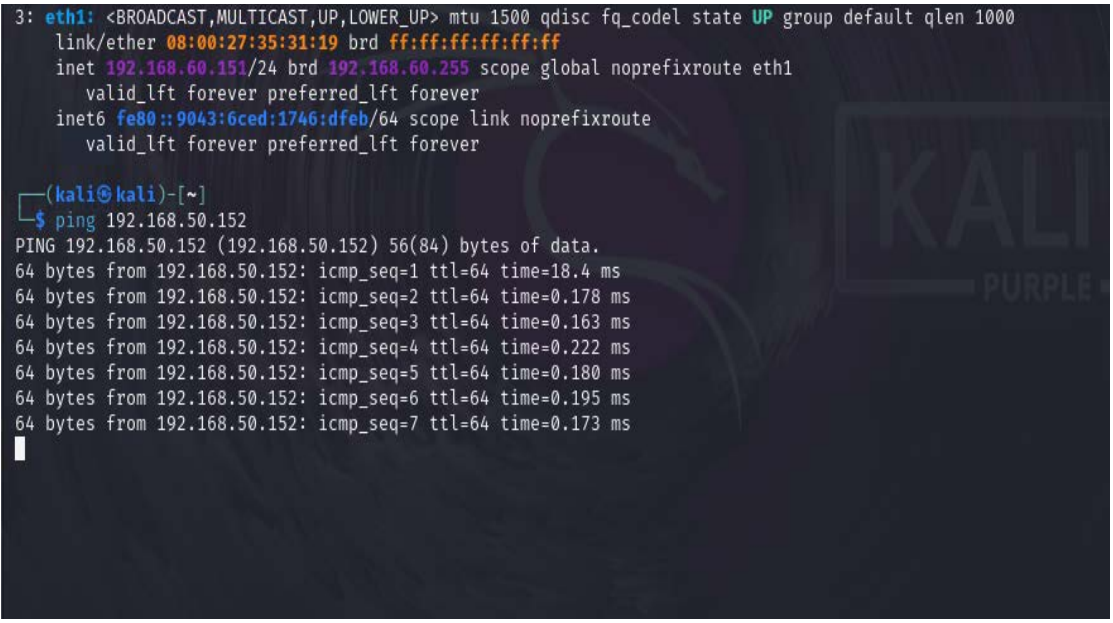
Progetto S3L5

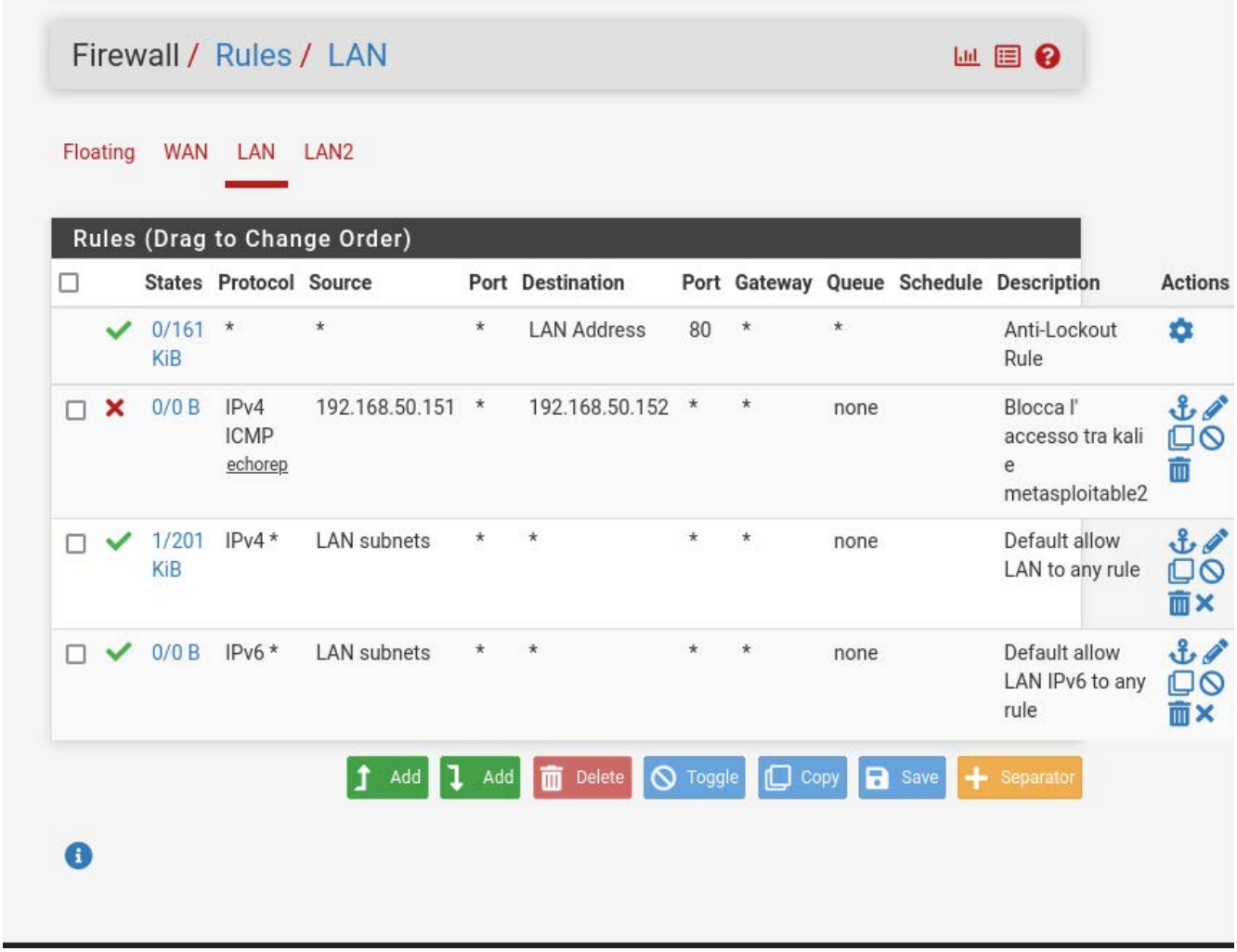
creare una regola firewall che blocchi l'accesso alla DVWA (su metasploitable) dalla macchina Kali Linux e ne impedisca di conseguenza lo scan. Un requisito fondamentale dell'esercizio è che le macchine Kali e Metasploitable siano su reti diverse, potete aggiungere una nuova interfaccia di rete a Pfsense in modo tale da gestire una ulteriore rete.

- Per separare le due macchine Kali e Metasploitable in due reti diverse, è stato necessario configurare pfSense con due interfacce di rete: LAN (dove si trova Metasploitable) e LAN2 (dove si trova Kali).
La prima rete (quella di metasploitable2) ha come indirizzo di gateway 192.168.50.1, mentre l'indirizzo Ip della macchina è 192.168.50.152.
La seconda rete (quella di kali) ha come indirizzo gateway 192.168.60.1, mentre l'indirizzo della macchina è 192.168.60.151.
Un passo fondamentale per il raggiungimento dell`obbiettivo è far si che le macchine riescano a comunicare tra loro anche essendo in due reti diverse, possiamo vereificarlo attraverso il comando Ping.



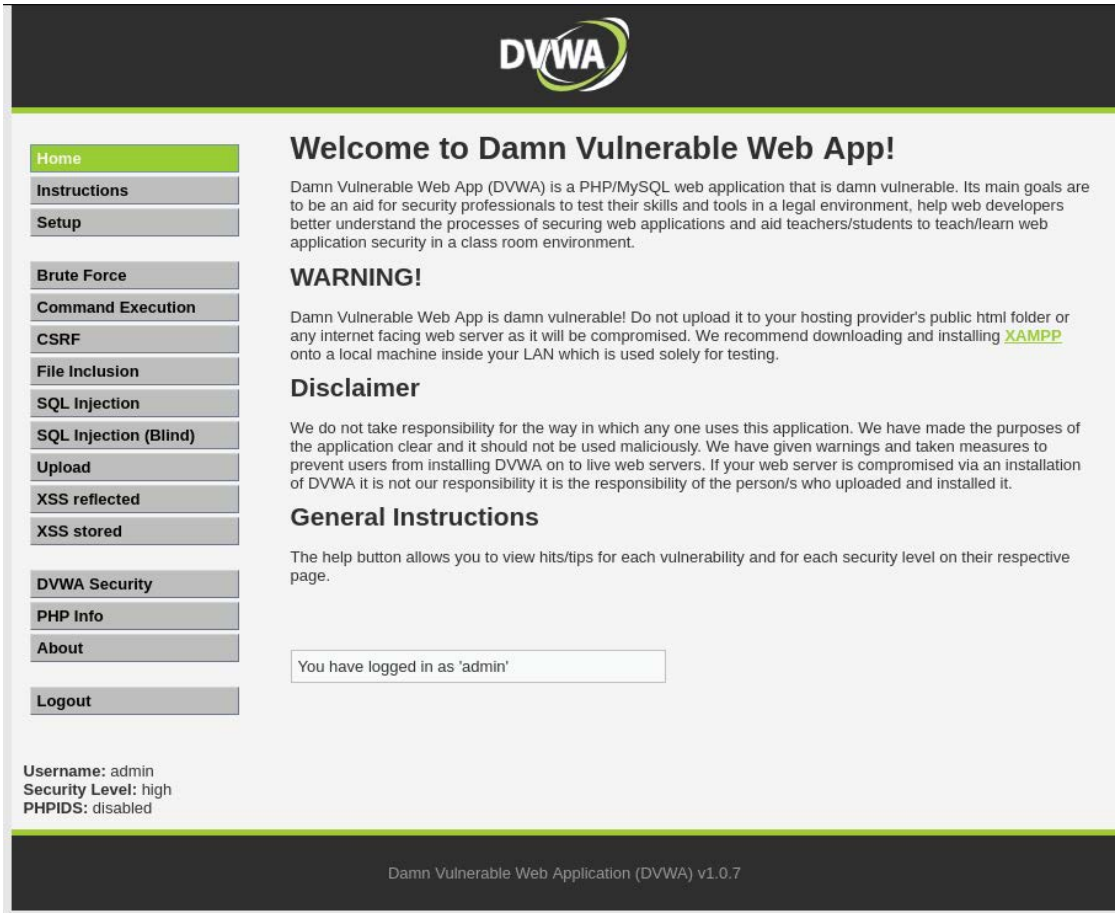
ping da kali verso metasploitable2

È anche stato necessario impostare una nuova regola nel firewall della LAN, che facesse in modo di bloccare eventuali tentativi di scan da parte di kali nei confronti della macchina target.

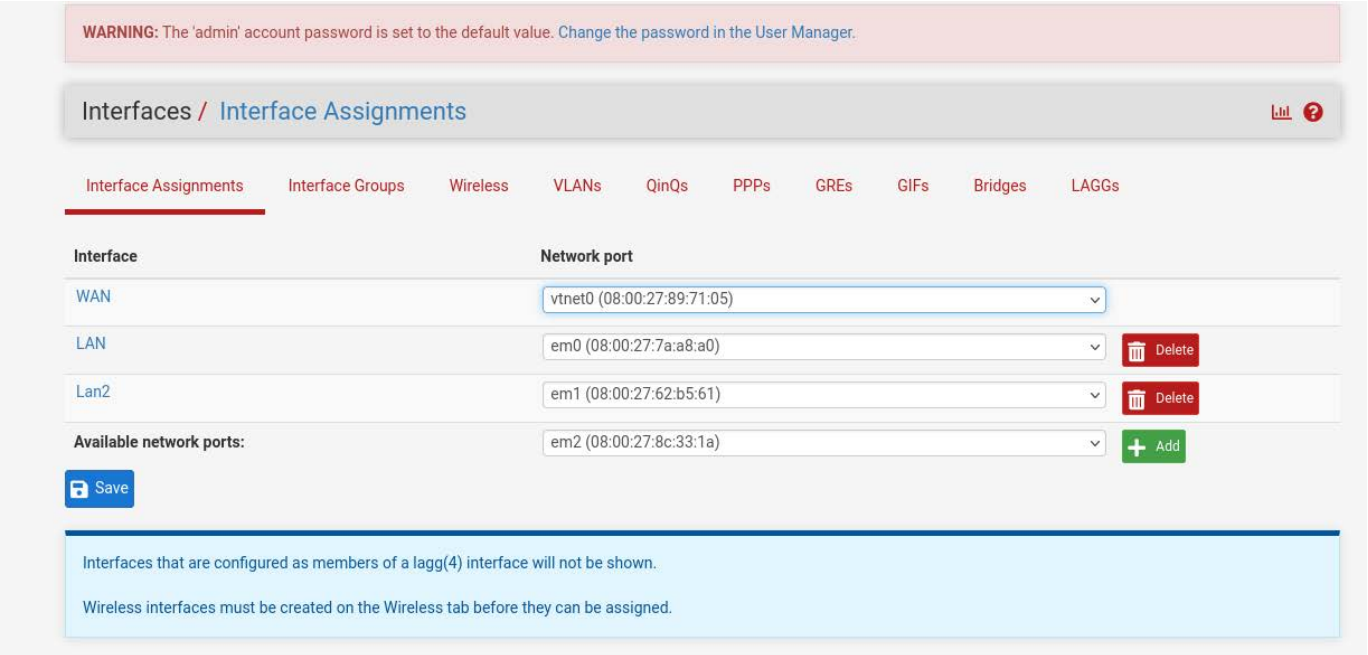


Se adesso andiamo ad abilitare la nuova regola (la seconda) non potremmo più andare ad effettuare l'accesso su dvwa e ad effettuare una scansione verso metasploitable.
Questa regola consiste nell'impostare la sezione action su "Block", impostare l'indirizzo IP di kali nella sezione sorgente e quello di metasploitable nella sezione destinazione. Una volta impostata la regola basta salvarla ed applicarla tramite gli appositi bottoni.

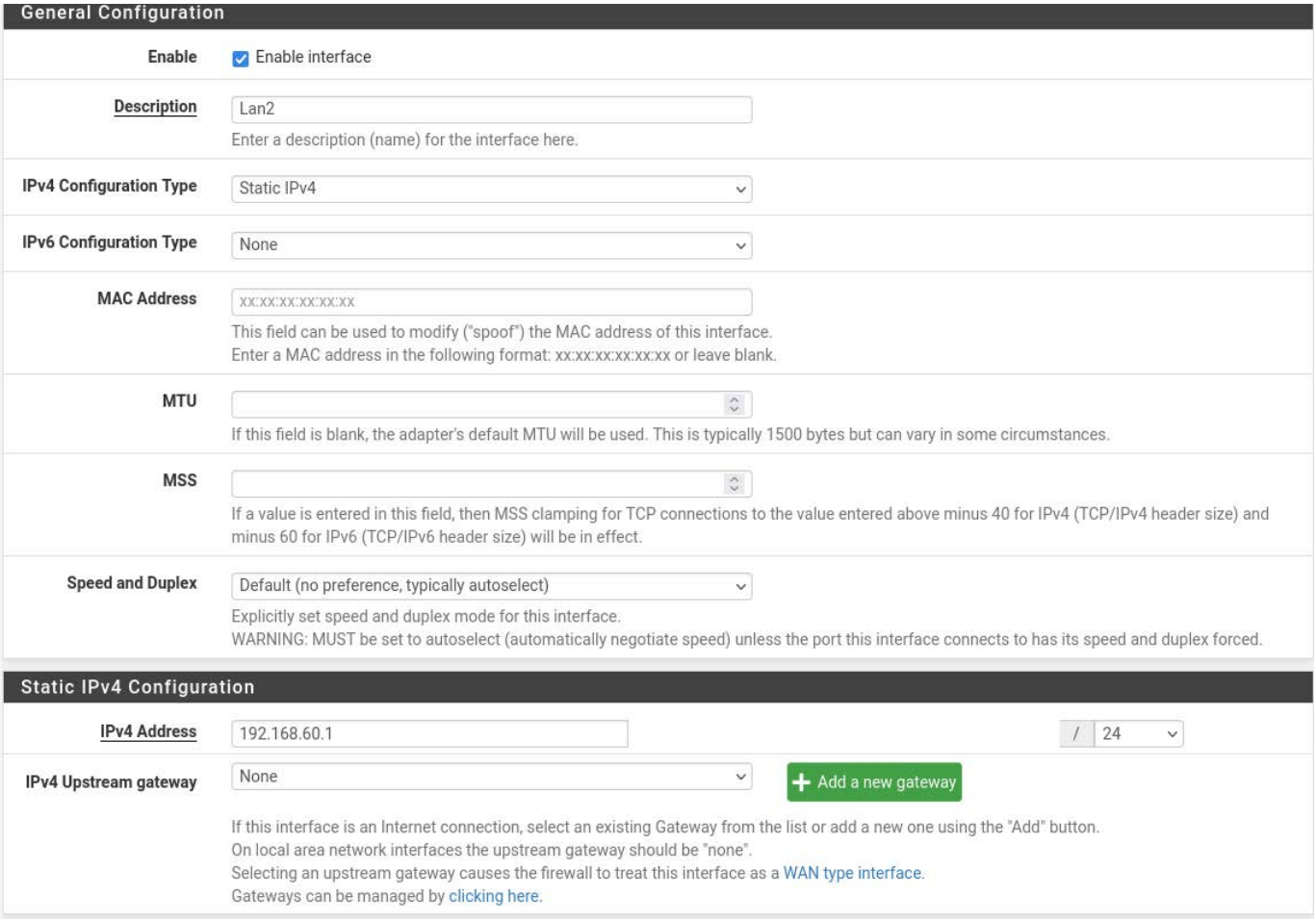
Per verificare il corretto funzionamento della regola basta andare sul browser e digitare il link di accesso a dvwa.



prima di attivare la regola potevamo entrare senza problemi, una volta settato correttamente il firewall, l'unica cosa che otterremo sarà una pagina con errore di caricamento.



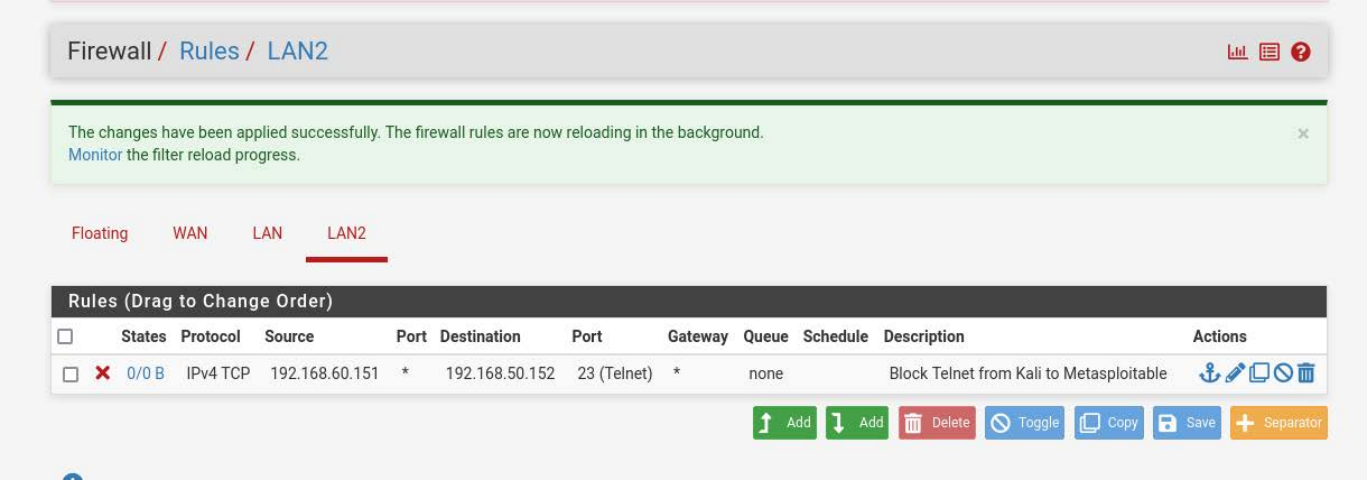
Creazione nuova rete LAN2



Configurazione LAN2

Esercizio Bonus
Impostare una regola su pfsense per bloccare da kali il telnet verso metasploitable.

Per bloccare il telent di kali verso metasploitable dobbioamo creare una regola nel Firewall della LAN2, che impedisca la comunicazione tramite la porta 23, che sarebbe la porta utilizzata da Telnet.



Andiamo ad impostare l'indirizzo IP di kali nella sezione Sorgente e quello di Metasploitable nella sezione Destinazione.

Per verificare il corretto funzionamento della regola, oltre a salvarla ed applicarla possiamo effettuare un tentativo di connessione Telnet da Kali a Metasploitable, tramite il comando: telnet 192.168.50.152