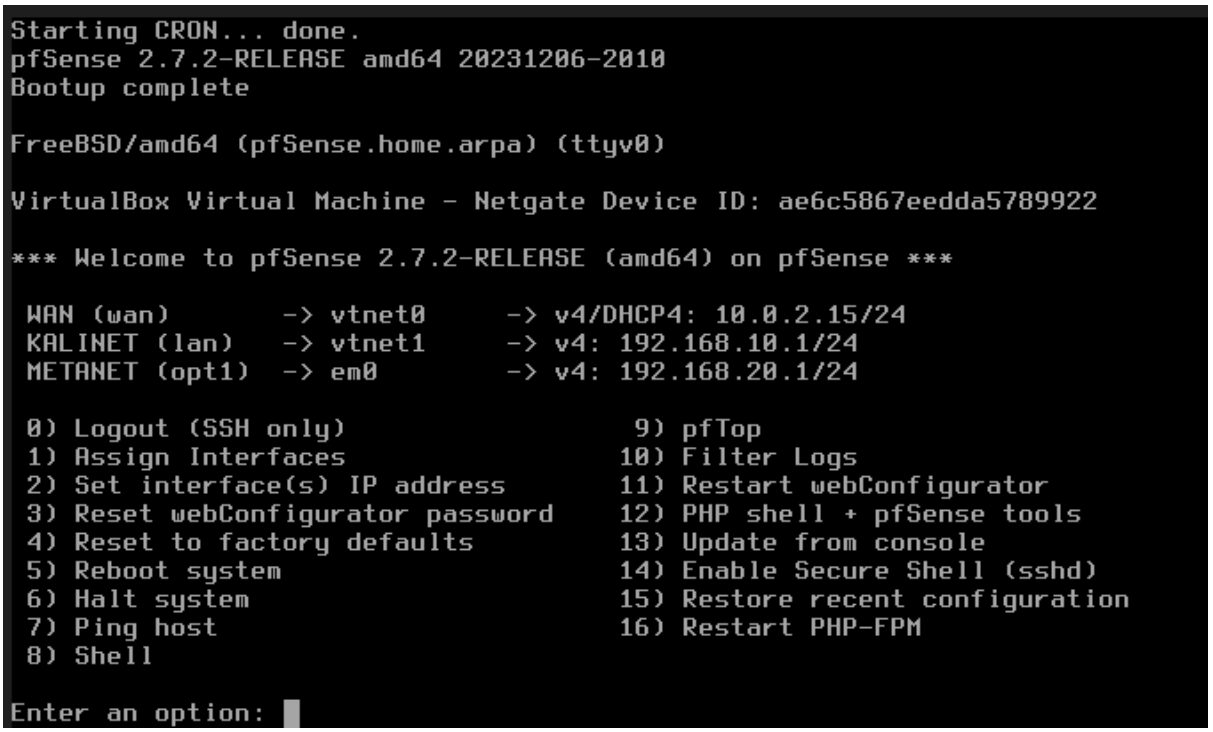
CREAZIONE FIREWALL

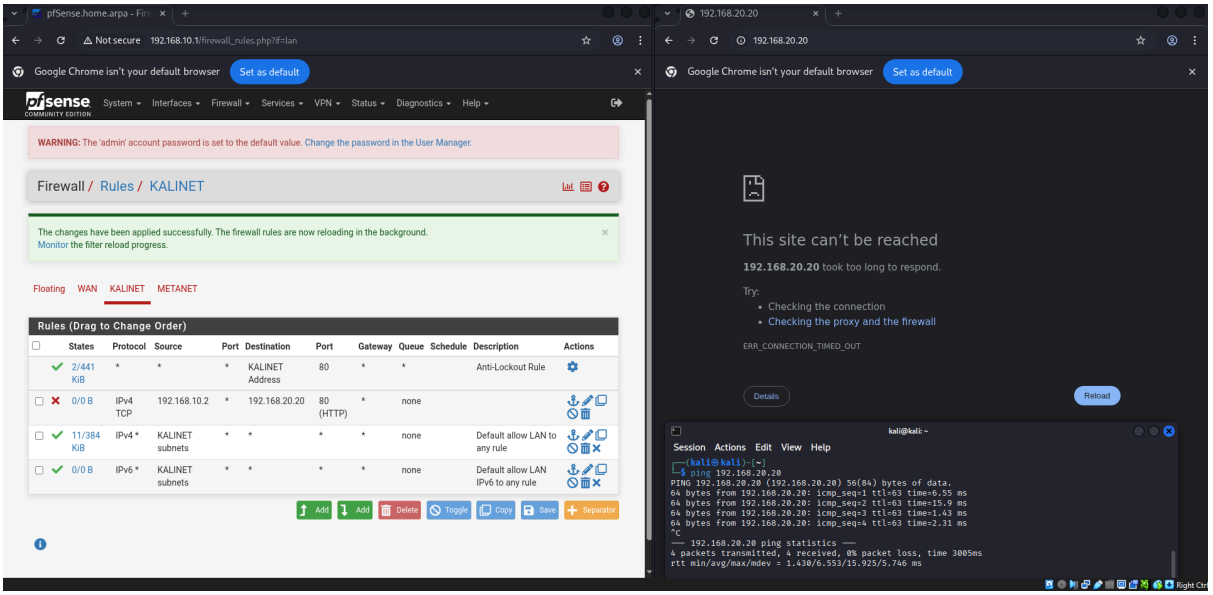
La relazione descrive la creazione di un firewall virtuale con pfSense in VirtualBox per controllare il traffico tra Kali Linux (rete 192.168.10.0/24) e Metasploitable2 (rete 192.168.20.0/24), mostrando sia il caso in cui l'accesso alla DVWA è bloccato sia quello in cui è consentito.

Nel laboratorio sono presenti tre macchine virtuali: pfSense funge da router/firewall con tre interfacce (WAN, KALINET/LAN e METANET/OPT1), Kali è collegata all'interfaccia KALINET e Metasploitable2 all'interfaccia METANET.
L'obiettivo dell'esercitazione è creare regole firewall su pfSense per bloccare selettivamente le connessioni HTTP da Kali verso Metasploitable2 e verificare, tramite browser e ping, la differenza tra traffico filtrato e traffico consentito

Di seguito la configurazione pfsense :



Dopo aver salvato e applicato le regole del firewall, da Kali si testa la connettività verso Metasploitable2: il ping all'indirizzo 192.168.20.20 risponde regolarmente, perché la regola coinvolge solo il traffico TCP sulla porta 80, ma l'accesso HTTP dal browser produce "ERR_CONNECTION_TIMED_OUT".
Questo comportamento dimostra che pfSense filtra il traffico a livello di porta: l'ICMP rimane consentito mentre le richieste HTTP vengono scartate dalla nuova regola di blocco, come si osserva anche dalla colonna "States" che non registra sessioni attive per la regola negata.



Per ripristinare l'accesso alla DVWA è sufficiente disabilitare o cancellare la regola di blocco lasciando attiva soltanto la regola "Default allow LAN to any rule" sull'interfaccia KALINET.
Una volta applicate le modifiche, ricaricando http://192.168.20.20 dal browser di Kali compare la pagina iniziale di Metasploitable2 con i collegamenti a TWiki, phpMyAdmin, Mutillidae, DVWA e WebDAV, confermando che il traffico HTTP tra le due reti ora è nuovamente autorizzato.