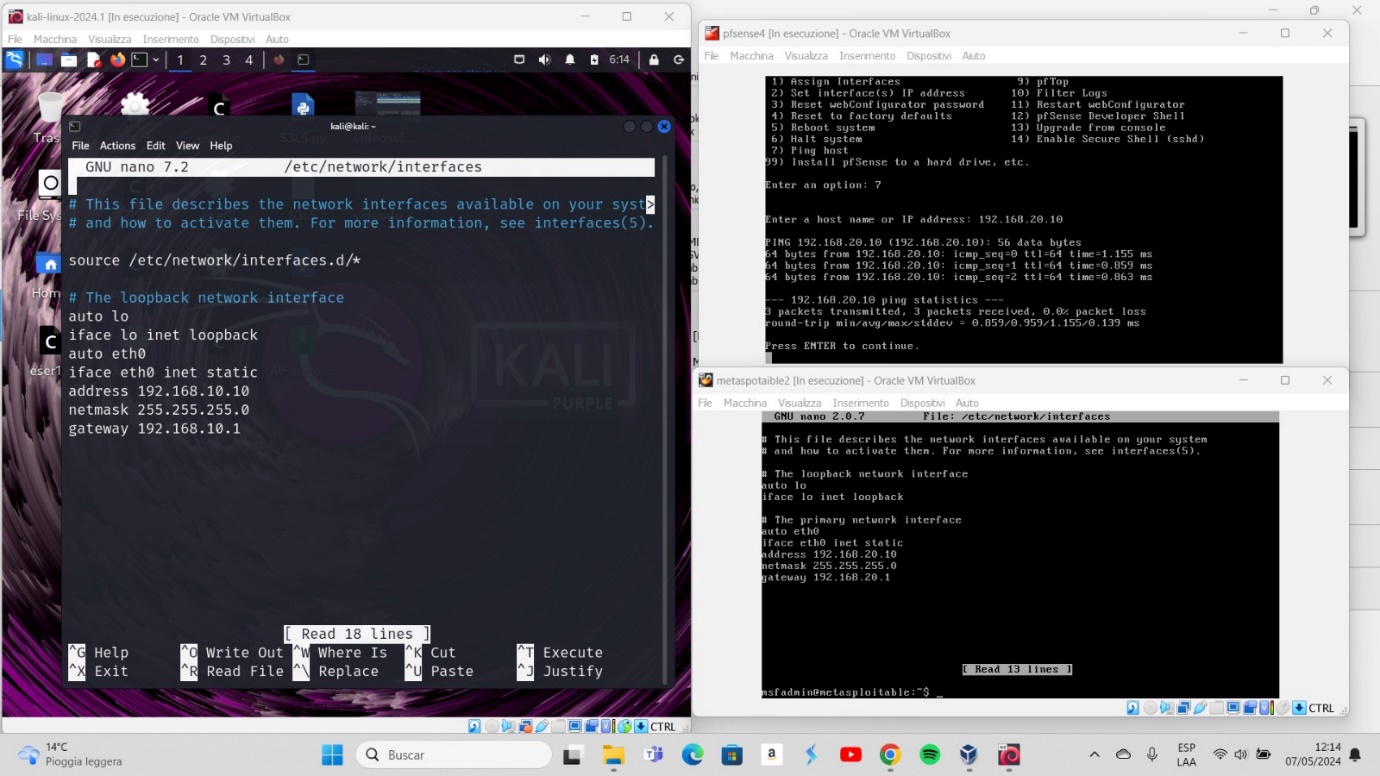
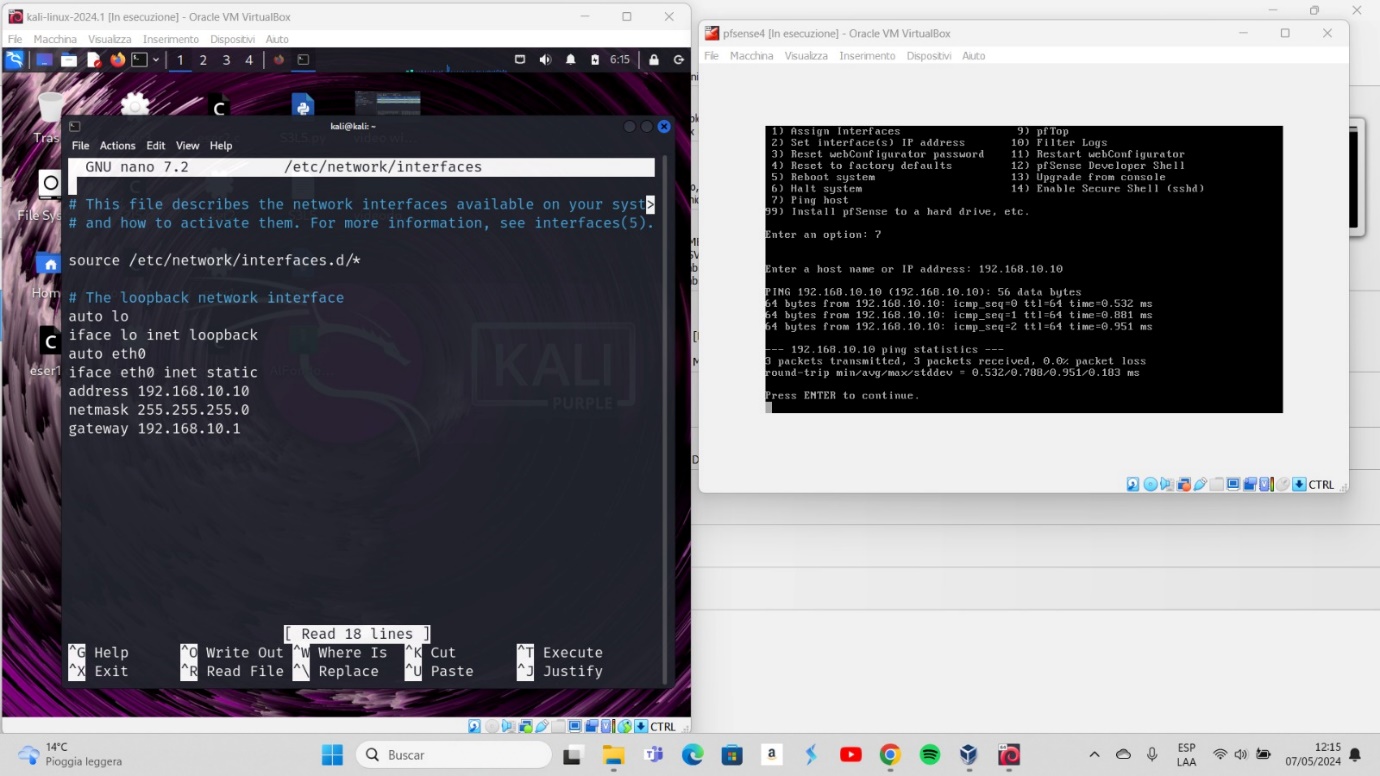
**Report creazione policy Pfsense**

**1)Configurazione delle Reti**

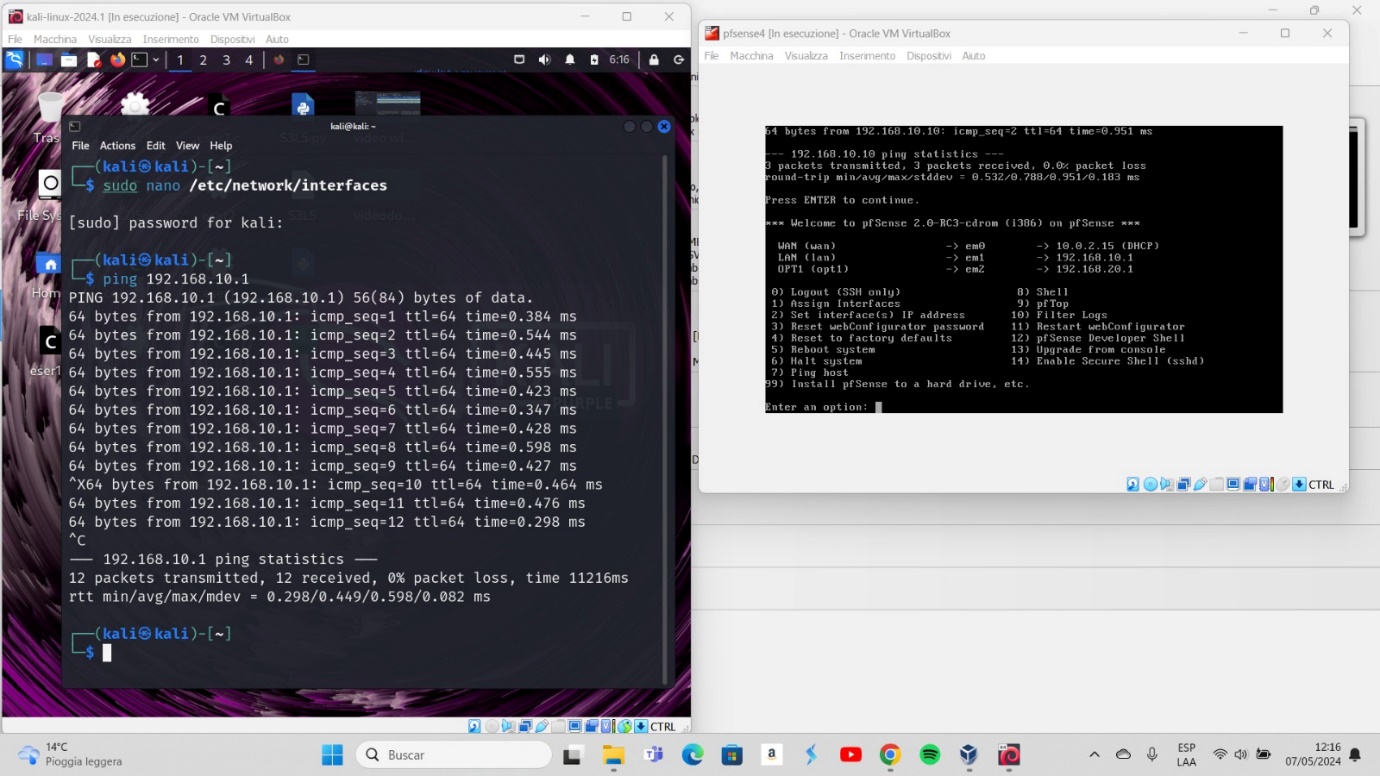


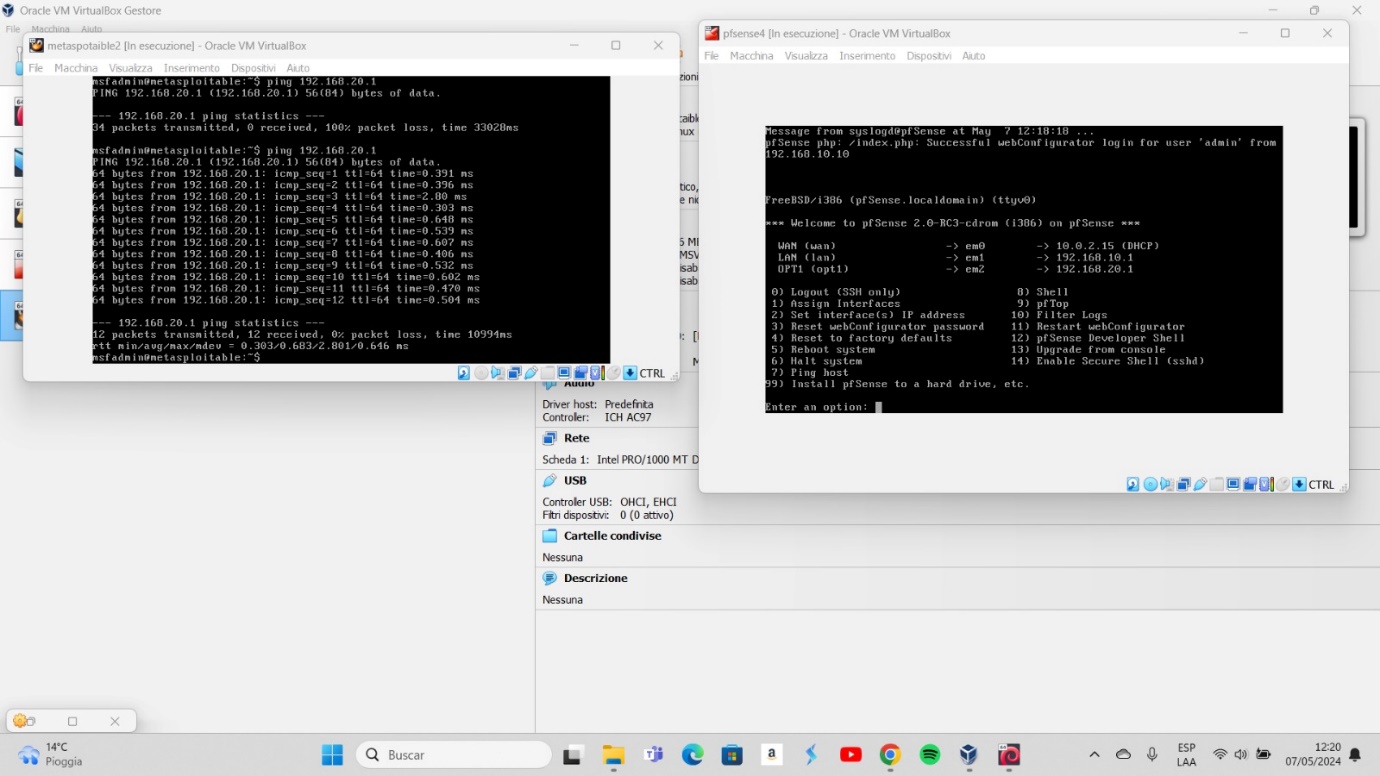
Per prima cosa sono andato a creare tre reti distinte gestite da pfSense, utilizzato come gateway. Queste reti permettono la comunicazione tra differenti macchine virtuali (Kali Linux e Metasploitable) anche se si trovano in reti diverse. Ecco i dettagli delle configurazioni di rete per ciascuna macchina:



- Kali Linux è configurato con un indirizzo IP statico 192.168.10.10, con maschera di sottorete 255.255.255.0 e gateway 192.168.10.1.

- Metasploitable (DVWA) è configurato con un indirizzo IP statico 192.168.20.10, con maschera di sottorete 255.255.255.0 e gateway 192.168.20.1.



****

**2)Configurazione di pfSense**

PfSense funge da gateway centrale e gestisce il traffico tra le diverse reti. Dalle immagini, è evidente che pfSense è configurato con diverse interfacce per gestire il traffico in modo specifico:

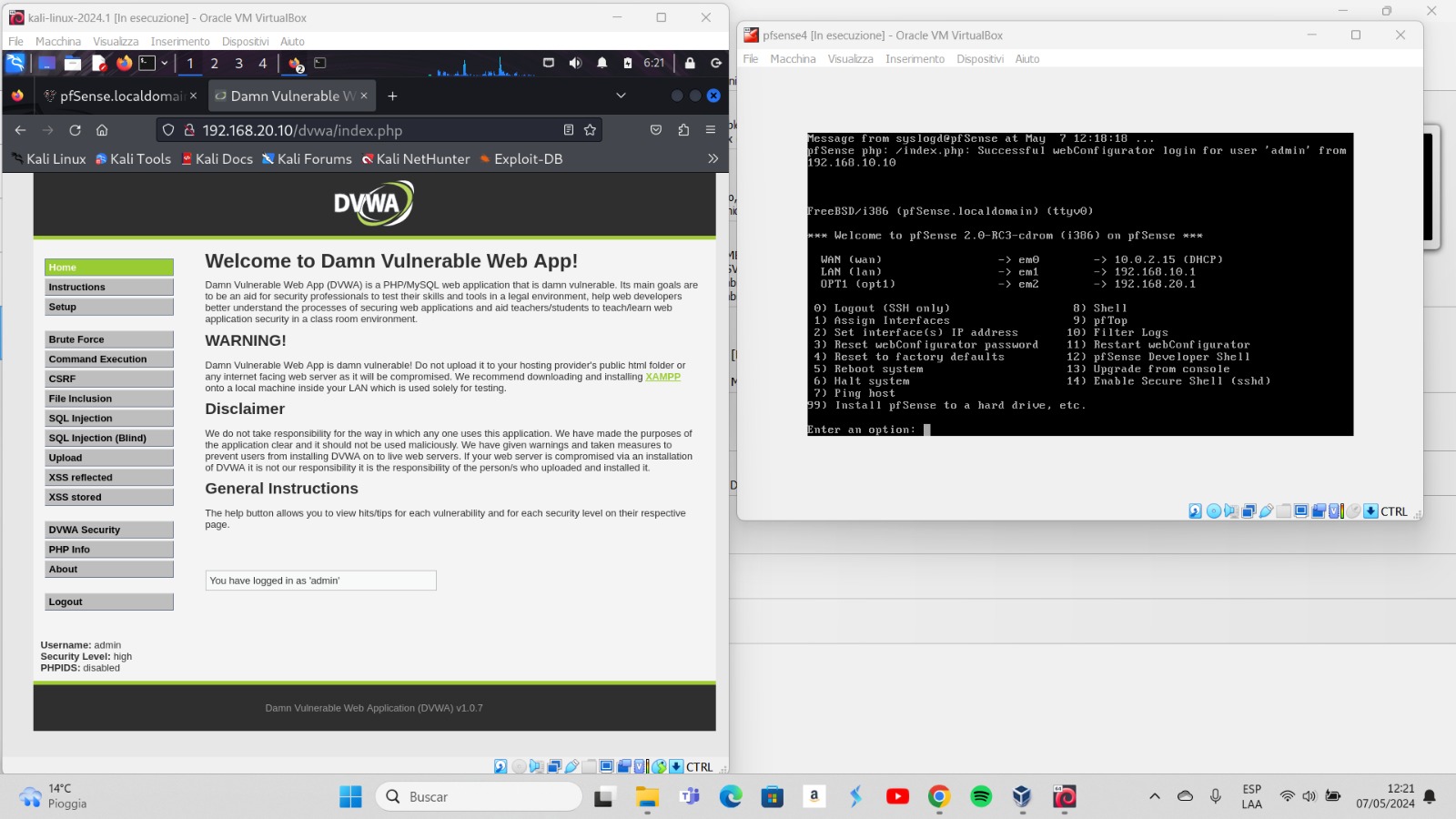
Immagine che contiene testo, schermata, Carattere

Descrizione generata automaticamente

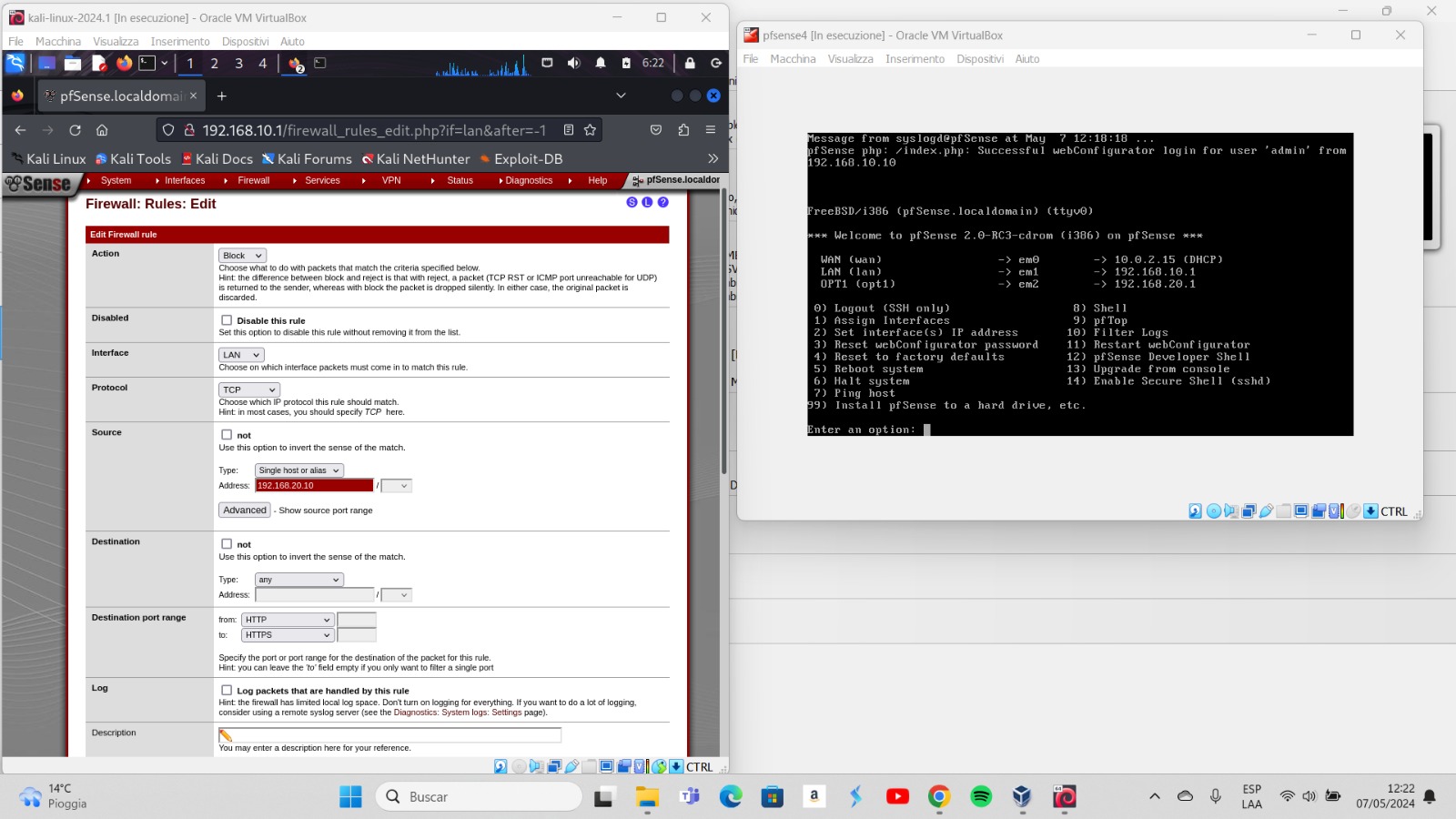
- Interfaccia LAN (em1) assegnata all'IP 192.168.10.1.

- Interfaccia OPT1 (em2) assegnata all'IP 192.168.20.1.

**3)Configurazione della Regola Firewall**

****

Sono andato a creare una regola firewall specifica per bloccare il traffico TCP dalla macchina Kali Linux (192.168.10.10) verso qualsiasi indirizzo nella rete dove si trova Metasploitable. La regola è configurata come segue:



- **Azione: Block**, che impedisce il traffico specificato.

- **Interfaccia: LAN**, specificando che la regola si applica al traffico proveniente dalla LAN su cui è situata la macchina Kali Linux.

- **Protocollo: TCP**, mirato a bloccare sessioni TCP che potrebbero essere usate per attacchi o scansione.

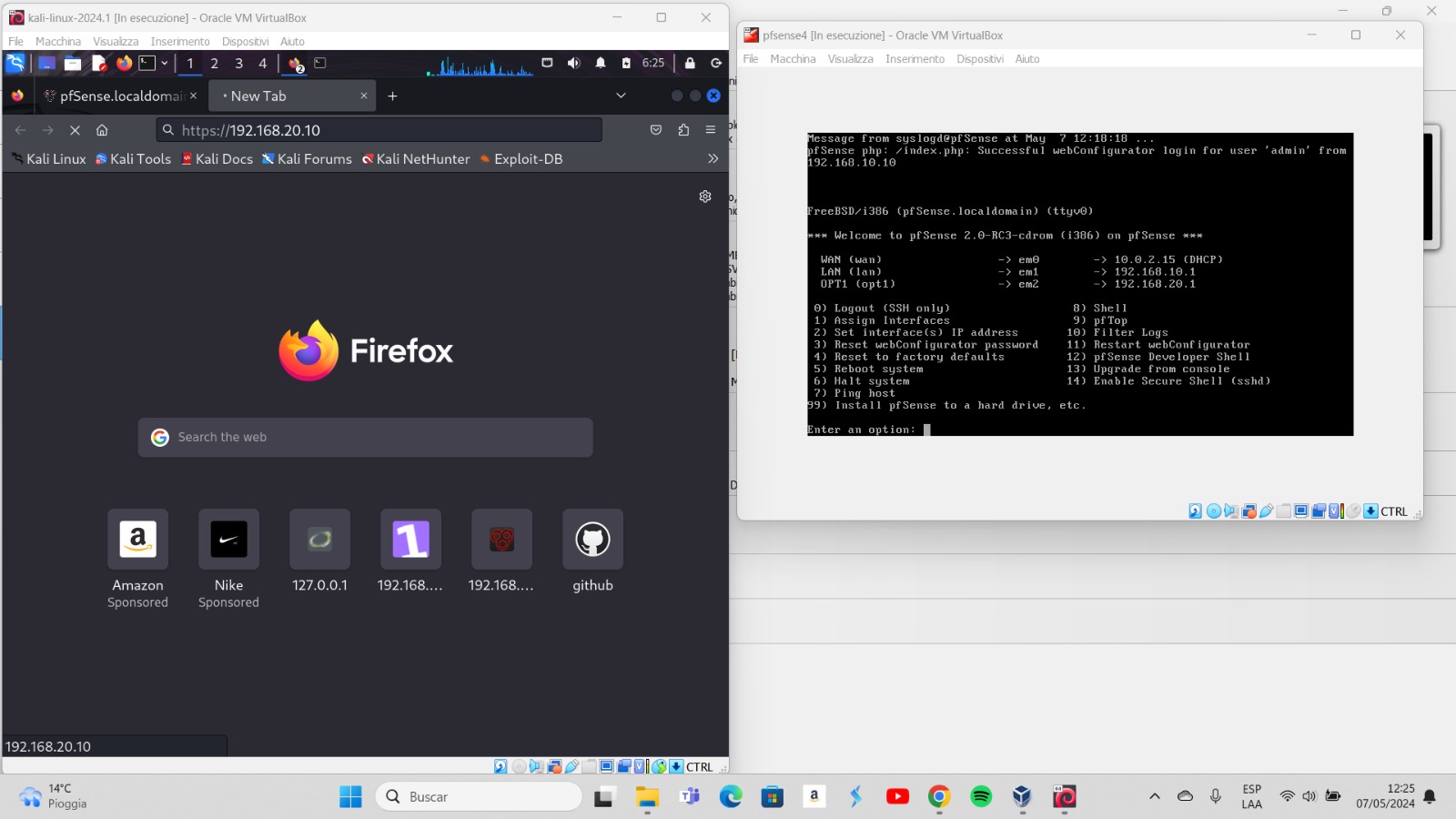
- **Indirizzo Sorgente:** 192.168.10.10, l'IP di Kali Linux.

- **Indirizzo Destinazione**: **Qualsiasi**, poiché la regola si applica a qualsiasi tentativo di connessione da Kali Linux verso reti esterne.

- **Porte Destinazione:** **HTTP a HTTPS** ,che sono comuni porte web usate da DVWA.

**4)Test e Verifica**

Dagli screenshot, è visibile che dopo aver applicato la regola, il tentativo di accedere a DVWA tramite il browser da Kali Linux non riesce, confermando l'efficacia della regola firewall.



In conclusione, il setup realizzato garantisce che nonostante le due macchine virtuali siano in grado di comunicare attraverso pfSense, il traffico non desiderato, in questo caso specifico gli accessi a DVWA da Kali Linux, è bloccato efficacemente dal firewall impostato in pfSense.