W9D1 – Pratica PfSense

DATA

Cybersecurity Analyst

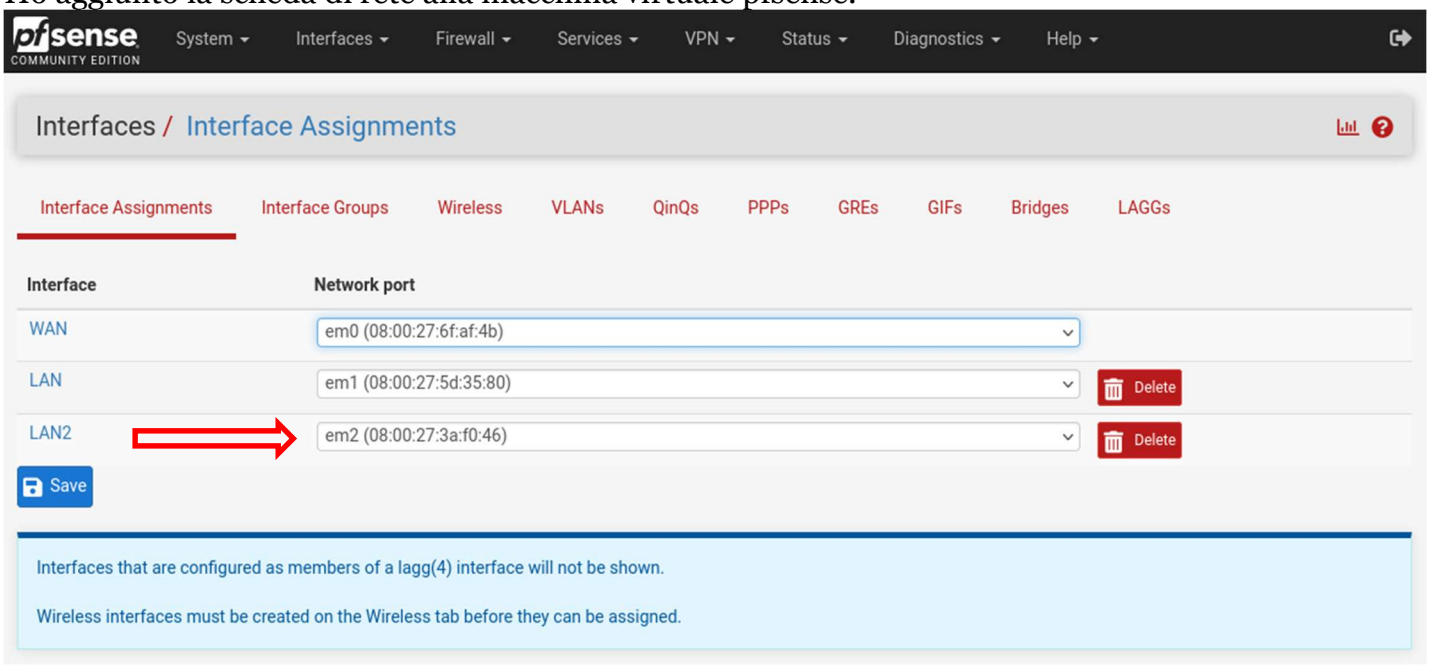
Studente:
Andrea Scarmagnani
Docente:
Giuseppe Placanica

Traccia:
-Sulla base di quanto visto, creare una regola firewall che blocchi l'accesso alla DVWA (su metasploitable) dalla macchina Kali Linux e ne impedisca di conseguenza lo scan (fare uno screenshot che dimostri che prima lo scan per DVWA funzionava e ora non funziona più).

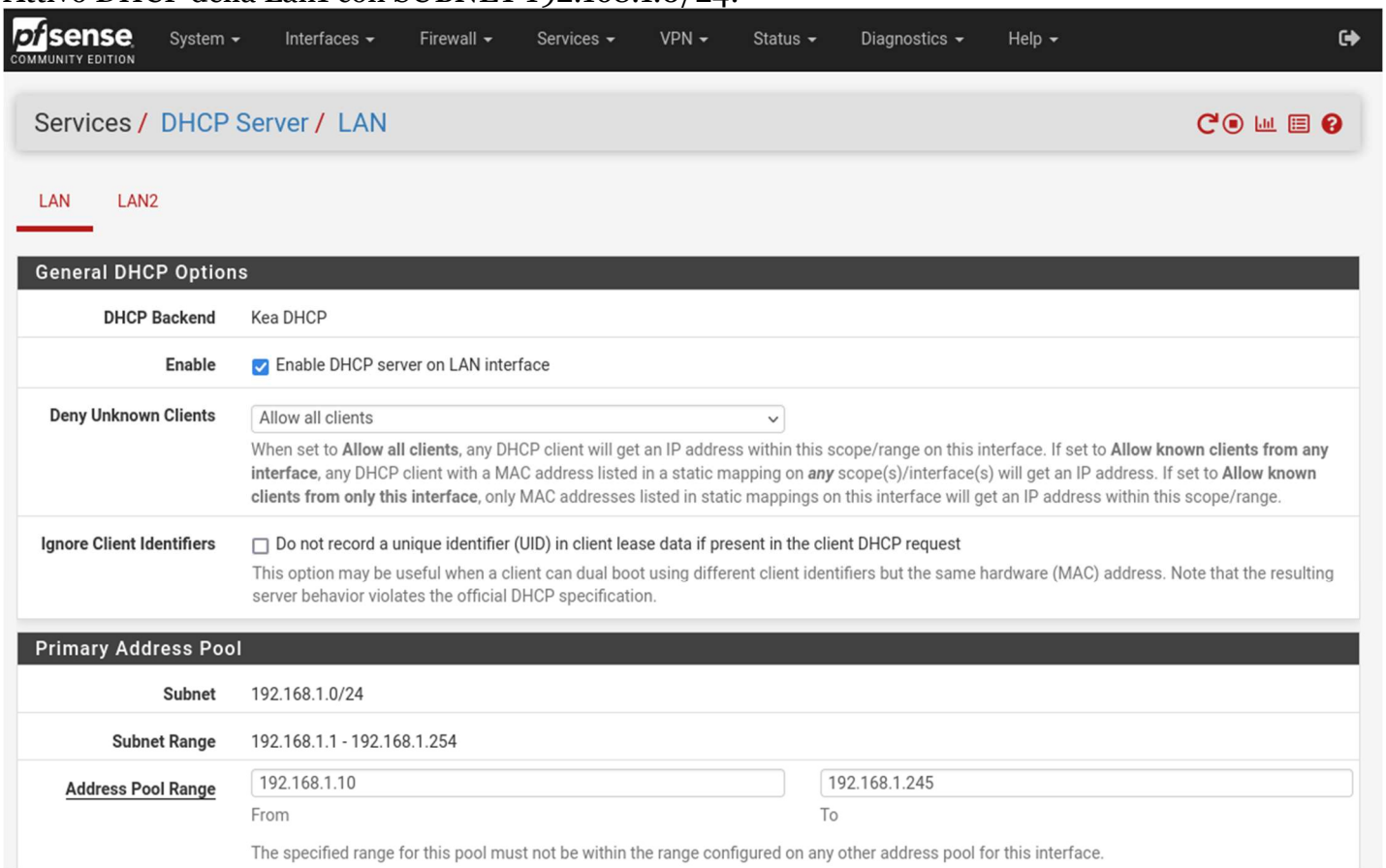
-Un requisito fondamentale dell'esercizio è che le macchine Kali e Metasploitable siano su reti diverse, potete aggiungere una nuova interfaccia di rete a Pfsense in modo tale da gestire una ulteriore rete. Connettetevi poi in Web GUI per attivare la nuova interfaccia e configurarla.

Esecuzione:

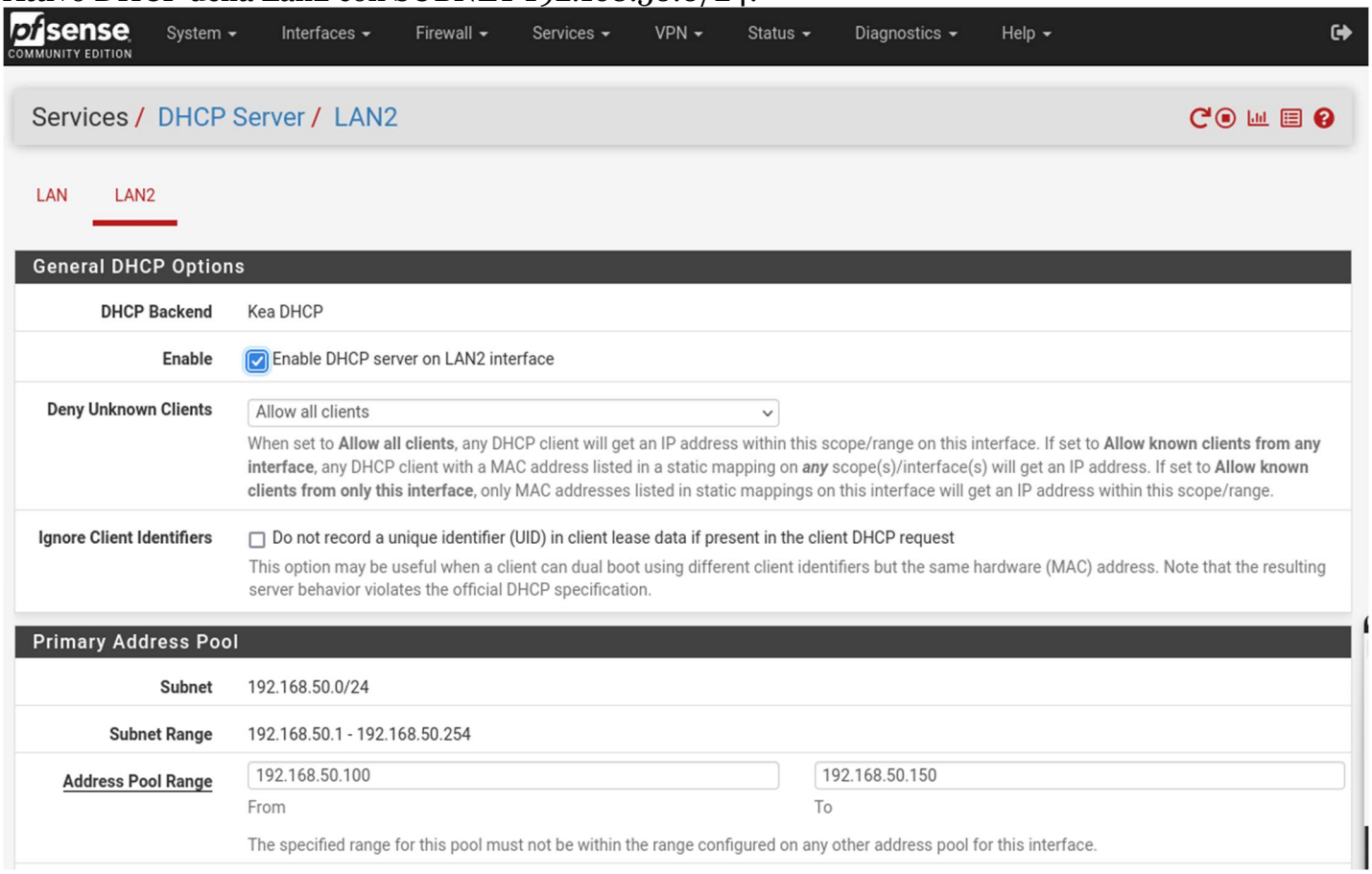
Ho aggiunto la scheda di rete alla macchina virtuale pfsense.



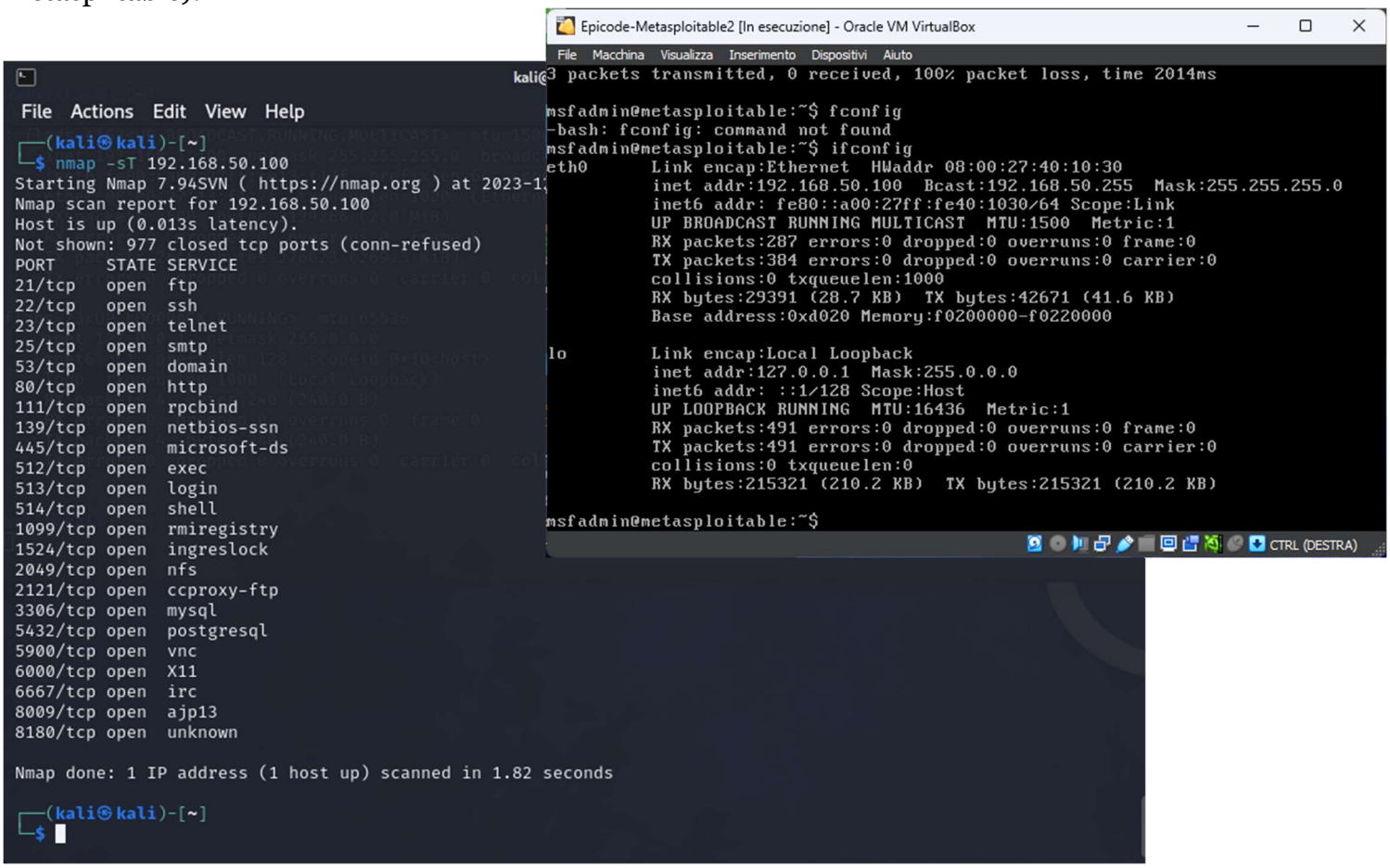
Attivo DHCP della Lan1 con SUBNET 192.168.1.0/24:



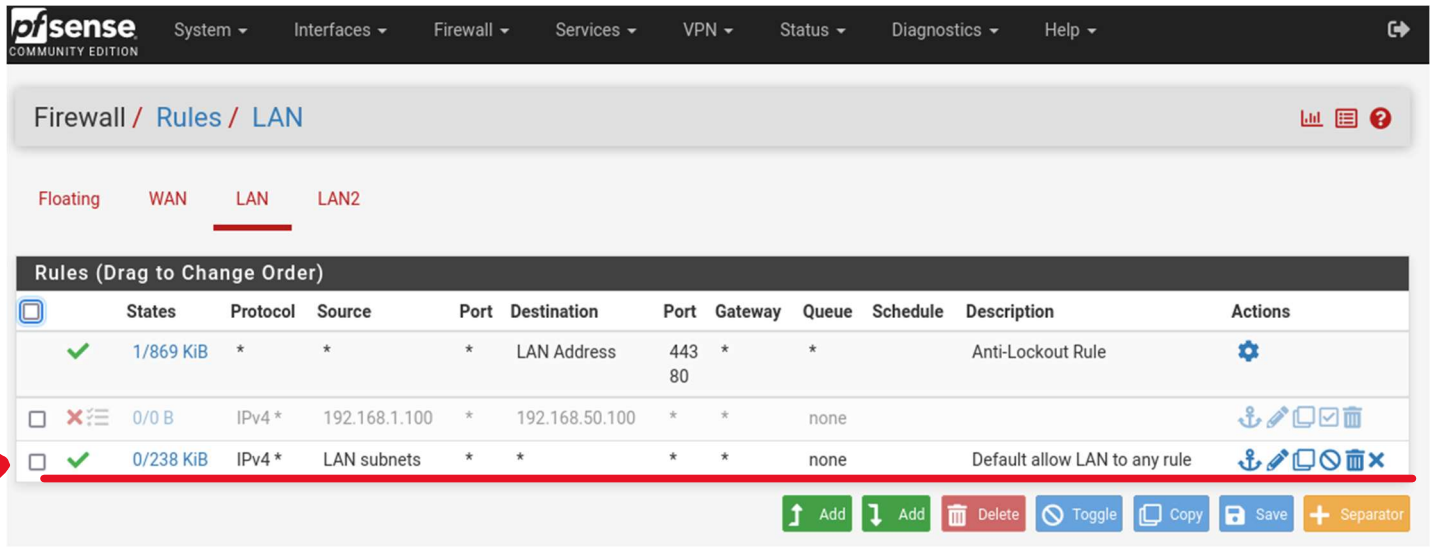
Attivo DHCP della Lan2 con SUBNET 192.168.50.0/24:



Dalla machina KALI(192.168.1.100) esegue nmap -sT 192.168.50.100 (Indirizzo della macchina metasplitable):



Le due macchine comunicano perché il firewall di PfSense, ha una regola (nella Lan1) che permette la comunicazione tra le due reti.



Dopo l'attivazione della regola qui sotto, la macchina Kali non è in grado di raggiungere la macchina metasploitable.

Ecco il risultato dello stesso comando nmap -sT 192.168.50.100:

```
┌──(kali㉿kali)-[~]
└─$ nmap -sT 192.168.50.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-12-28 08:37 EST
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.11 seconds
```

L'host non è raggiungibile.

Cybersecurity Analyst 2023