REPORT S3/L4

Creazione policy Pfsense

Traccia

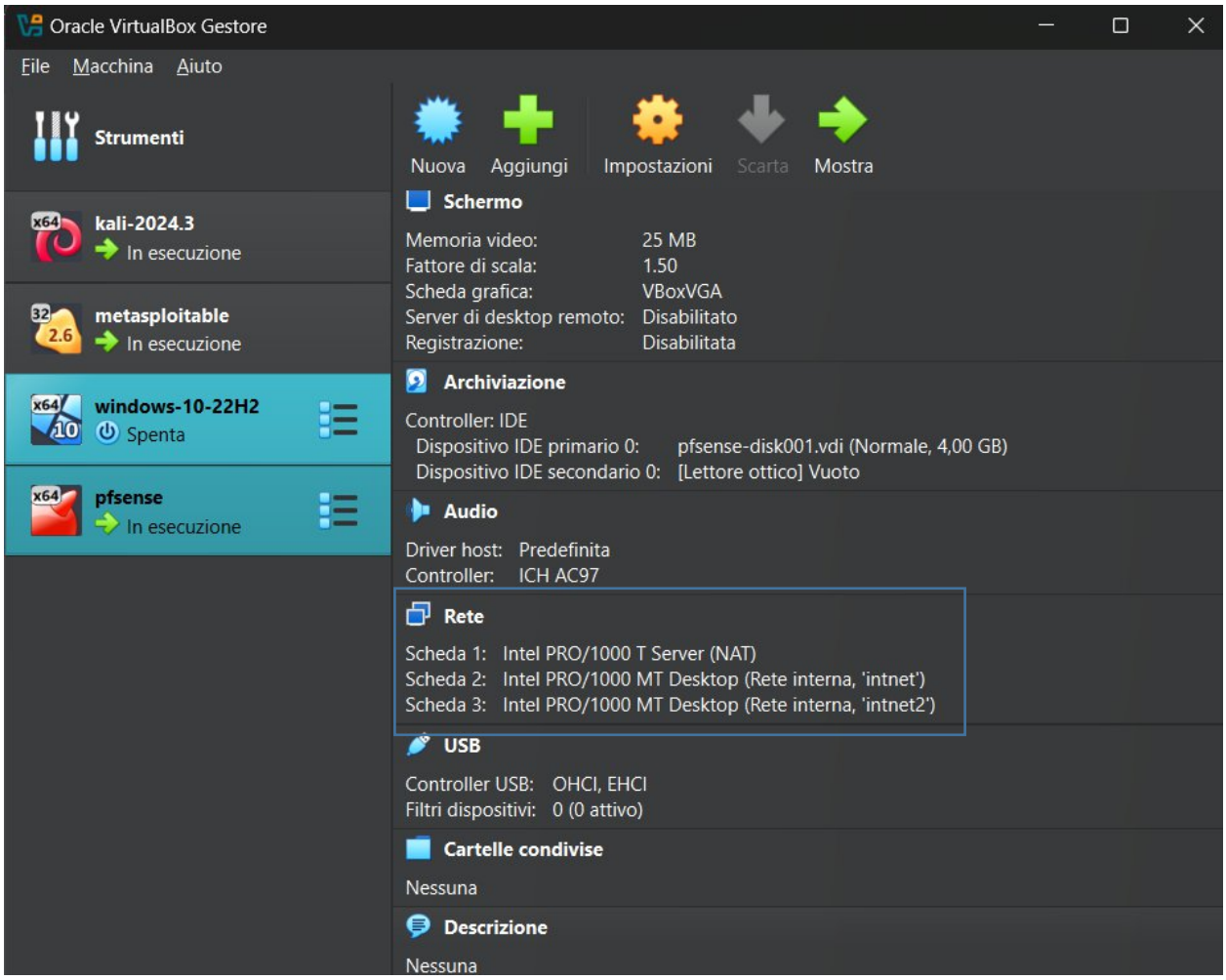
Creare una regola firewall che blocchi l'accesso alla DVWA (su metasploitable) dalla macchina Kali Linux e ne impedisca di conseguenza lo scan.

Svolgimento

Per arrivare a configurare le regole firewall su pfSense abbiamo innanzitutto bisogno di configurare le due reti da associare alle VM di Kali Linux e Metasploitable2.

Pertanto nella configurazione di rete di VMbox di pfSense accendiamo 3 schede di rete, di cui:

- La prima sarà configurata in NAT per la connessione verso l'esterno
- La seconda sarà configurata su rete interna intnet e scheda di rete Intel PRO/1000 MT
- La terza sarà configurata su rete interna intnet2 e scheda di rete Intel PRO/1000 MT

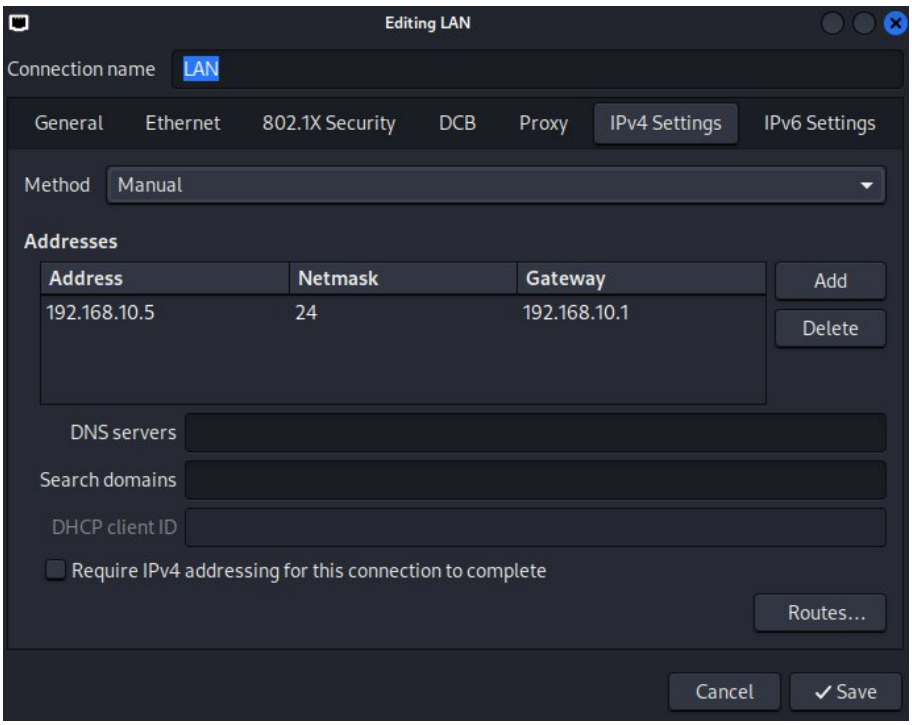


Fatto ciò avviamo la macchina di pfSense e una volta arrivati al menu principale configuriamo la prima rete em1 assegnando l'indirizzo 192.168.10.1/24

```
Starting CRON... done.
pfSense 2.7.2-RELEASE amd64 20231206-2010
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: fcb4f62440195b2d1a50

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 10.0.2.15/24
 LAN (lan)       -> em1        -> v4: 192.168.10.1/24
 LAN2 (opt1)     -> em2        -> v4: 192.168.20.1/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option:
```

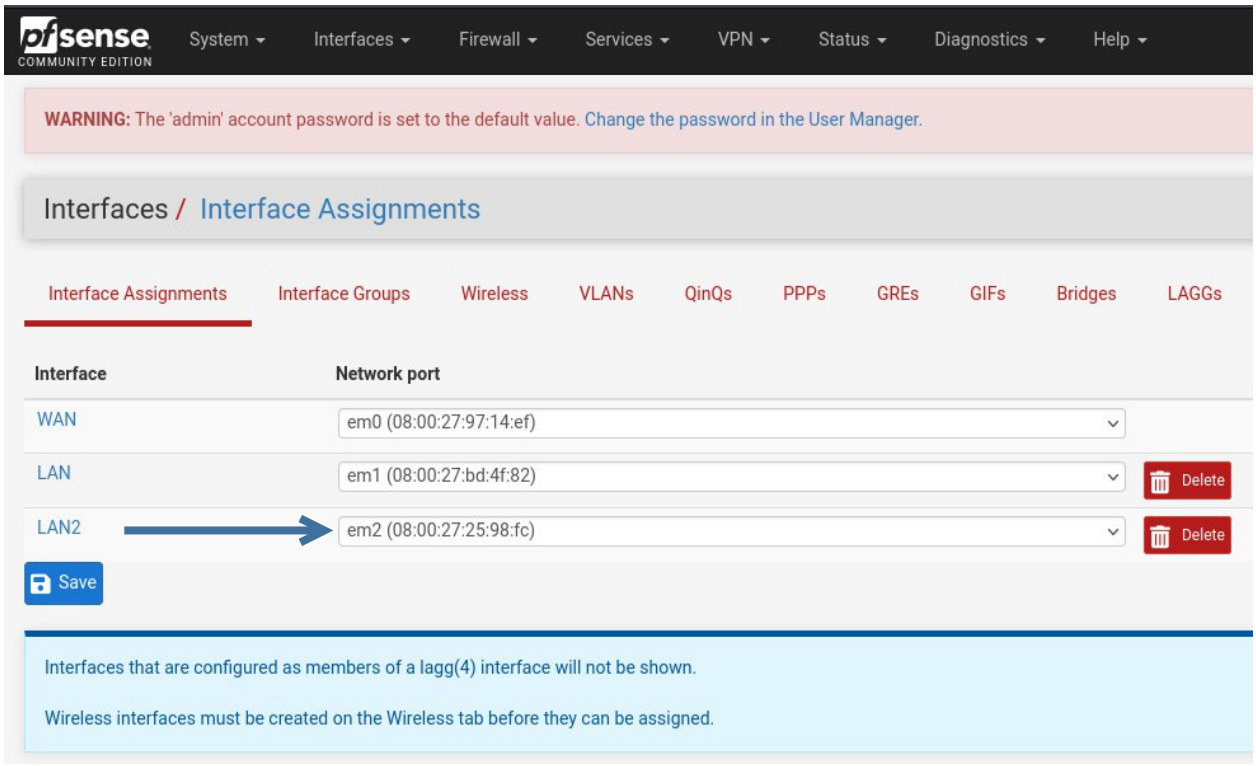
Avviamo quindi la macchina di Kali Linux e dalle impostazioni di rete facciamo in modo che questa macchina sia parte della rete chiamata LAN.

In particolare nella scheda IPv4 Settings cambiamo il Method in Manual ed aggiungiamo un indirizzo ip statico appartenente alla rete. Per questa macchina si è scelto l'indirzzo 192.168.10.5/24, come si può vedere dallo screen in basso.



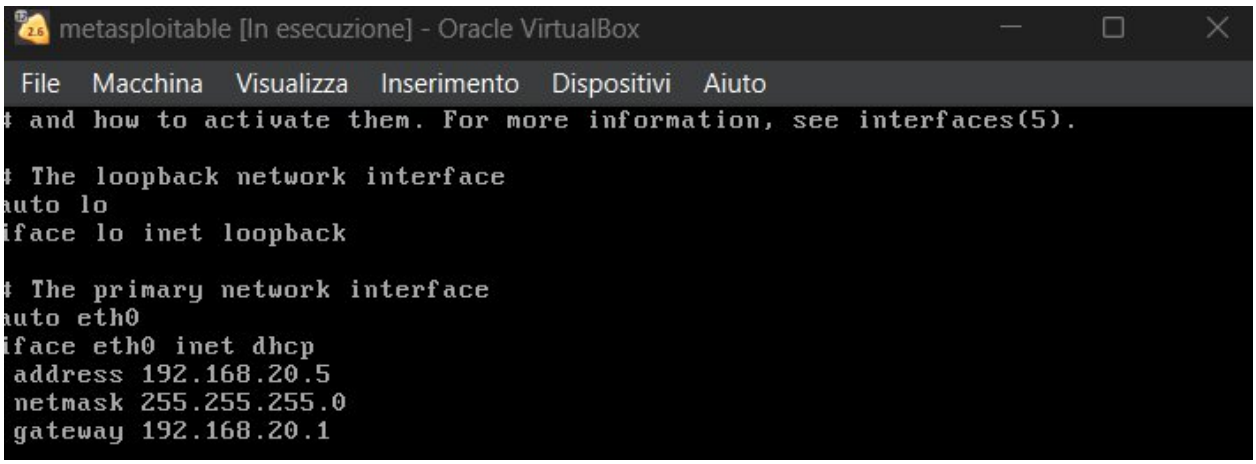
Possiamo, a questo punto, entrare sulla dashboard di pfSense all'indirizzo 192.168.10.1 e dopo aver effettuato il login dobbiamo attivare la seconda interfaccia LAN2 a cui andremo a collegare la macchina di Metasploitable.

Aggiungiamo quindi l'interfaccia dal menu Interfaces -> Assignement e la associamo alla rete em2, come mostra lo screen sotto



Ripetiamo gli stessi passaggi fatti su Kali anche per la macchina di Metasploitable2, con la differenza che quest'ultimo sistema non possiede una GUI, pertanto indirizzo ip statico della macchina, subnet e gateway andranno scritti nel file che si trova al path /etc/network/interfaces

Vediamo dallo screen che per la macchina di Meta è stato scelto l'indirizzo 192.168.20.5/24



Adesso che abbiamo configurato le due LAN e una macchina su ogni rete dobbiamo stabilire delle regole firewall su pfSense così da permettere alle due macchine di poter comunicare.

Per fare una prima prova, nella configurazione della regola, si è scelto di non specificare una rete o un'indirizzo IP specifico come sorgente o destinatario della comunicazione, pertanto la regola è stata creata come segue sia su LAN che su LAN2:

Proviamo a pingare Meta da Kali e viceversa per vedere se la rete è stata configurata correttamente ed otteniamo:

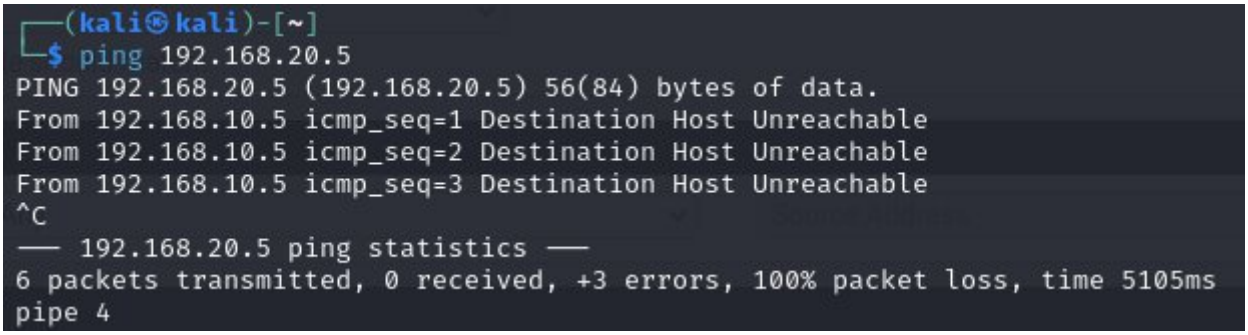


Figura 1. Ping da Kali su Meta

Figura 1. Ping da Meta su Kali

È abbastanza evidente che è stato commesso uno o più errori nella configurazione della rete perchè le due macchine non si raggiungono a vicenda. Nonostante le diverse prove effettuate, cambiando gateway, regole firewall, configurazione di rete su VMbox non si è riusciti a portare a termine questa operazione, pertanto neanche l'esercizio assegnato.