W9D1 – Pratica PfSense

DATA

Cybersecurity Analyst

Studente:

Andrea Scarmagnani

Docente:

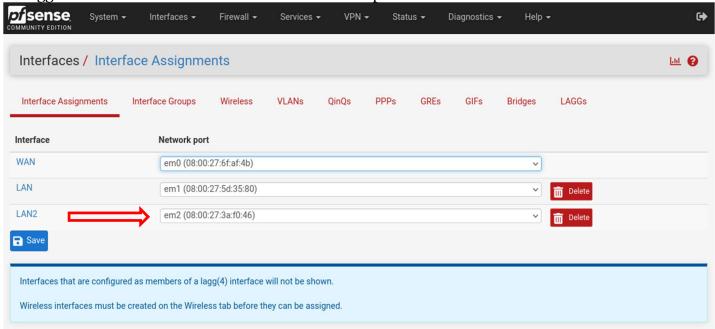
Giuseppe Placanica

Traccia:

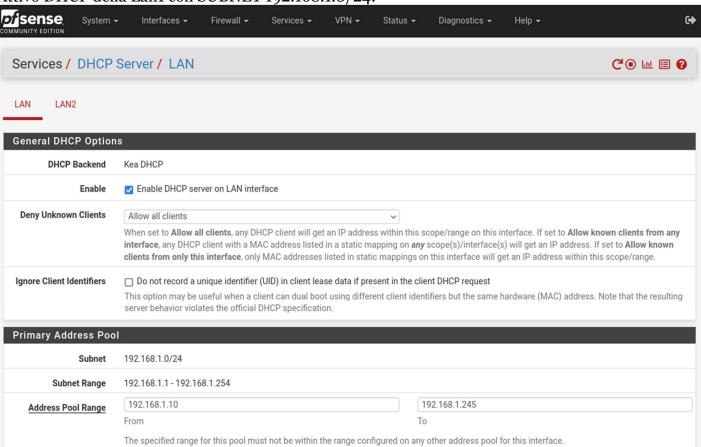
- -Sulla base di quanto visto, creare una regola firewall che blocchi l'accesso alla DVWA (su metasploitable) dalla macchina Kali Linux e ne impedisca di conseguenza lo scan (fare uno screenshot che dimostri che prima lo scan per DVWA funzionava e ora non funziona più).
- -Un requisito fondamentale dell'esercizio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

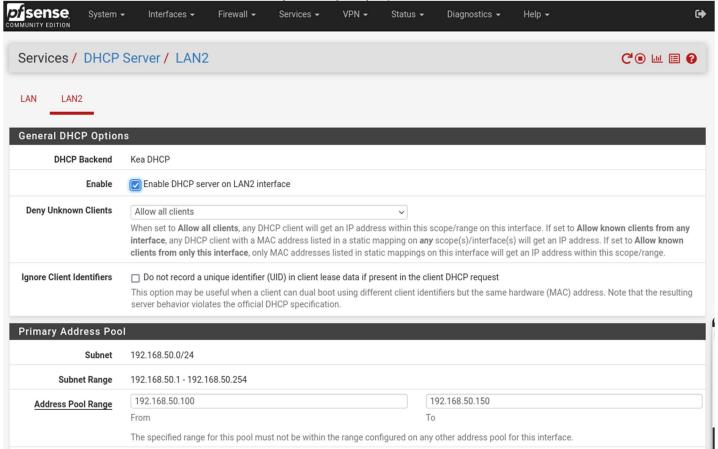
Ho aggiunto la scheda di rete alla macchina virtuale pfsense.



Attivo DHCP della Lan1 con SUBNET 192.168.1.0/24:



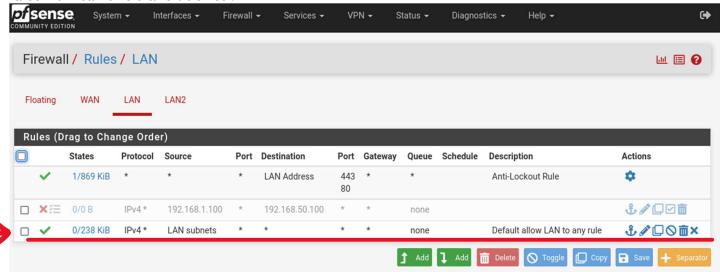
Attivo DHCP della Lan2 con SUBNET 192.168.50.0/24:



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

```
Epicode-Metasploitable2 [In esecuzione] - Oracle VM VirtualBox
                                                                                                                                              kali@3 packets transmitted, 0 received, 100% packet loss, time 2014ms
                                                          File Actions Edit View Help
         -ST 192.168.50.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-1;
                                                                                                                             Mask:255.255.255.0
Nmap scan report for 192.168.50.100 Host is up (0.013s latency).
Not shown: 977 closed tcp ports (conn-refused)
         STATE SERVICE
PORT
21/tcp
         open ftp
22/tcp
                ssh
         open
23/tcp
                telnet
          open
25/tcp
          open
                 smtp
                                                                      Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
53/tcp
                 domain
          open
80/tcp
          open
111/tcp
                rpcbind
                                                                      UP LOOPBACK RUNNING MTÛ:16436 Metric:1
         open
139/tcp
445/tcp
                                                                      RX packets:491 errors:0 dropped:0 overruns:0 frame:0 TX packets:491 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:0
          open
                netbios-ssn
         open
                microsoft-ds
512/tcp
513/tcp
         open
                exec
                                                                      RX bytes:215321 (210.2 KB) TX bytes:215321 (210.2 KB)
         open
                login
514/tcp
                shell
         open
                                                           msfadmin@metasploitable:~$
1099/tcp open
                 rmiregistry
                                                                                                                🖸 🚳 🔃 🗗 🤌 📰 🖭 🚰 🦓 🌮 🛂 CTRL (DESTRA)
1524/tcp open
                ingreslock
2049/tcp open
                nfs
2121/tcp open
                ccproxy-ftp
3306/tcp open
                mysql
5432/tcp open
                postgresql
5900/tcp open
6000/tcp open
                X11
6667/tcp open
8009/tcp open
                ajp13
8180/tcp open
                unknown
Nmap done: 1 IP address (1 host up) scanned in 1.82 seconds
```

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.

5

Cybersecurity Analyst 2023