

Creazione policy Pfsense

L'esercizio chiede di mettere le macchine Kali e metasploitable, su due reti differenti e settare Pfsense(firewall) con due reti interne, una per kali e una per metasploitable. Setto le gli indirizzi ip e di gateway come segue:

Macchina	Indirizzo ip	gateway
kali	192.168.32.100	192.168.32.105
metasploitable	192.168.500.100	192.168.50.101

macchina	Lan1	Lan2
Pfsense (firewall)	192.168.32.105	192.168.50.105

Praticamente il firewall Pfsense è un router, quindi bisogna instradare con le proprie interfacce (LAN1 e LAN2), il gateway delle due macchine poste su due reti differenti.

Faccio uno scan verso la dvwa di Metasploitable e come mostrato di seguito mi rileva tutte le porte con i relativi servizi aperti.

```
(kali@kali)~$ nmap -F 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-29 10:40 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.50.101
Host is up (0.019s latency).
Not shown: 82 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
513/tcp   open  login
514/tcp   open  shell
2049/tcp  open  nfs
2121/tcp  open  cccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
8009/tcp  open  ajp13

Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
```

Ora tramite kali, accedo alla pagina di configurazione di Pfsense (192.168.32.105) e vado ad inserire una regola di firewall, mettendo un blocco alla porta 80 della macchina dvwa di Metasploitable.

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	1 / 4.12 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0 / 42 KiB	IPv4 TCP	192.168.32.100	*	192.168.50.101	80 (HTTP)	*	none			

Così facendo, la porta 80 dell'indirizzo ip di Meta (192.168.50.101) non è raggiungibile, perché c'è un blocco di firewall e anche con lo scan che vedremo di seguito, non rileva nessun servizio.

```
(kali@kali)~$ nmap -F 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-29 10:47 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
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 3.03 seconds
```