PENETRATION TESTING

TASK

- Dopo aver configurato Kali, Metaspoitable e Pfsense, tra cui, le prime due in rete Interna e l'ultima abilitando altre due reti aggiuntive, dobbiamo permettere che le tre macchina possano pingarsi tra di loro (dimostrazione successivamente). Pertanto è necessario che le macchine Kali e Metaspoitable siano su reti diverse.
- Creare una regola Firewall che non consenta l'accesso alla DVWA da Kali e ne impedisca lo scan.

ANALISI E VALUTAZIONI:

Per prima cosa andiamo a configurare kali e metaspoitable con due reti differenti, rispettivamente con questi indirizzi:

MACCHINA	INDIRIZZO IP ADDRESS	RETE		
Kali	192.168.50.100	Rete 1 (LAN1)		
Metaspoitable	192.168.90.101	Rete 2 (LAN2)		
Pfsense	192.168.50.103	NAT, Rete 1 (LAN1), Rete 2 (LAN2)		

Per entrare nel sito di pfsense da kali dobbiamo inserire l'indirizzo ipv4 per la macchina e per farlo basta inserire nel terminale di pfsense il tasto "1" per la modifica dell'indirizzo e inseriamo rispettivamente solo per l'indirizzo Ipv4 192.168.50.103.

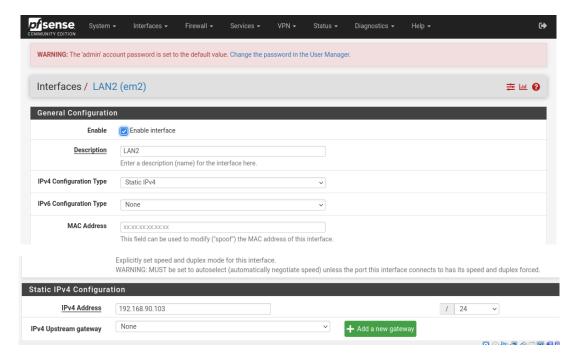
Successivamente possiamo andare ad impostare una nuova rete per pfsense e per farlo entriamo nel sito da Kali utilizzando il suo indirizzo IP impostato. La nuova rete servirà per poter collegare rispettivamente le due macchine Kali e Metaspoitable, di fatti la configurazione per la LAN1 e la LAN2 (rete che creeremo clicclando su ADD da "Interfacess -> Assignment") sarà rispettivamente questa:

• LAN1

of sense System	Interfaces ▼	Firewall 🕶	Services -	VPN →	Status ▼	Diagnostics ▼	Help →	•	
WARNING: The 'admin' acc	ount password is set to	the default valu	e. Change the p	assword in th	ne User Manage	r.			
Interfaces / LAN	1 (em1)							⋣ Ш ②	
General Configuration	n								
Enable	☑ Enable interface								
Description	LAN1 Enter a description (name) for the interface here.								
IPv4 Configuration Type	Static IPv4								
IPv6 Configuration Type	None								
MAC Address	XX:XX:XX:XX:XX								



LAN2



Dopo di che facciamo un scansione di DVWA con nmap -sS e andiamo a vedere le porte aperte sull'indirizzo IP target. Il risultato sarà pressocchè questo:

```
(kali@ kali)-[~]

$ sudo nmap 192.168.90.101 -sS

[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-21 13:10 EST

Nmap scan report for 192.168.90.101 (192.168.90.101)

Host is up (0.0039s latency).

Not shown: 977 closed tcp ports (reset)

PORT STATE SERVICE

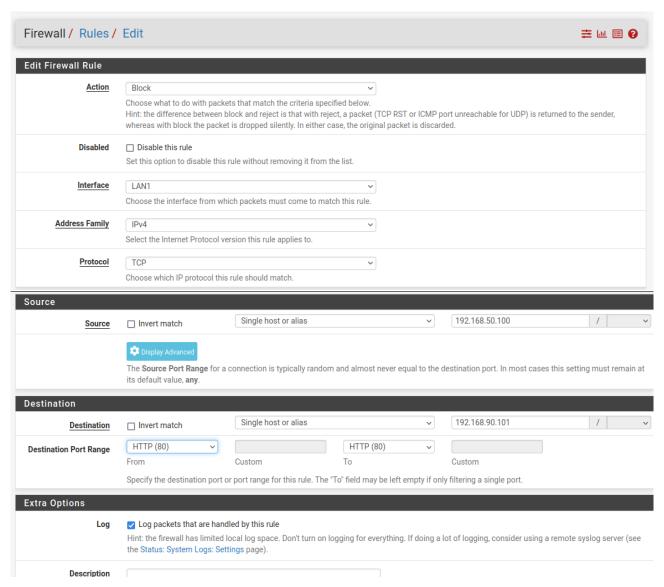
21/tcp open ftp

22/tcp open ssh

23/tcp open telnet

25/tcp open smtp
 25/tcp
53/tcp
                     open
open
                                           smtp
domain
80/tcp open
111/tcp open
139/tcp open
445/tcp open
                                           http
rpcbind
netbios-ssn
 445/tcp open
512/tcp open
                                           exec
login
shell
 513/tcp open
514/tcp open
514/tcp open
1099/tcp open
1524/tcp open
2049/tcp open
2121/tcp open
3306/tcp open
5432/tcp open
5900/tcp open
                                           rmiregistry
ingreslock
                                           nfs
                                           mysql
postgresql
                                           vnc
X11
 6000/tcp open
6667/tcp open
 8009/tcp open
8180/tcp open
                                           ajp13
unknown
  Nmap done: 1 IP address (1 host up) scanned in 1.02 seconds
```

Il risultato che dovremmo ottenere dal firewall che andremo a creare sarà il filtraggio sulla porta 80. Per la creazione del firewall basterà entrare sempre su pfsense e andare su "Firewall":



Così facendo andiamo a fare nuovamente un test per vedere se le macchine Kali e Metaspoitable continuano a pingarsi tra loro:

```
(kali@ kali)-[~]
$ ping 192.168.90.101
PING 192.168.90.101 (192.168.90.101) 56(84) bytes of data.
64 bytes from 192.168.90.101: icmp_seq=1 ttl=63 time=1.07 ms
64 bytes from 192.168.90.101: icmp_seq=2 ttl=63 time=0.984 ms
64 bytes from 192.168.90.101: icmp_seq=3 ttl=63 time=1.62 ms
^Z
zsh: suspended ping 192.168.90.101
```

Il ping funziona e di conseguenza il firewall però blocca l'accesso al sito dvwa e ora andando a testare la scansione, il firewall và a filtrare i pacchetti della porta 80 di cui abbiamo inserito:

```
-(kali⊕kali)-[~]
 -$ <u>sudo</u> nmap 192.168.90.101 -sS
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-21 13:16 EST
Nmap scan report for 192.168.90.101 (192.168.90.101)
Host is up (0.014s latency).
Not shown: 977 closed tcp ports (reset)
PORT
         STATE
                   SERVICE
21/tcp
         open
                   ftp
22/tcp
                   ssh
         open
23/tcp open
                   telnet
                  smtp
25/tcp open
53/tcp open
                   domain
80/tcp filtered http
111/tcp open
                  rpcbind
111/tcp open rpcbind
139/tcp open netbios-ssn
445/tcp open
                   microsoft-ds
512/tcp open
                   exec
513/tcp open login
514/tcp open shell
                rmiregistry
ingreslock
nfs
ccproxy-ftp
mysql
postgresql
vnc
                   rmiregistry
1099/tcp open
1524/tcp open
2049/tcp open
2121/tcp open
3306/tcp open
5432/tcp open
5900/tcp open
                   X11
6000/tcp open
6667/tcp open
                   irc
8009/tcp open
                   ajp13
8180/tcp open
                   unknown
Nmap done: 1 IP address (1 host up) scanned in 2.08 seconds
```