

CREAZIONE POLICY PFSENSE

L'esercitazione di oggi consisteva nella creazione di una regola firewall all'interno del tool Pfsense.

FASE 1

Nella prima fase abbiamo settato tutto l'ambiente in modo che la nostra macchina kali potesse accedere alla pagina di DVWA. Il tutto passando per il firewall Pfsense che avrebbe "filtrato" oppure no il tutto.

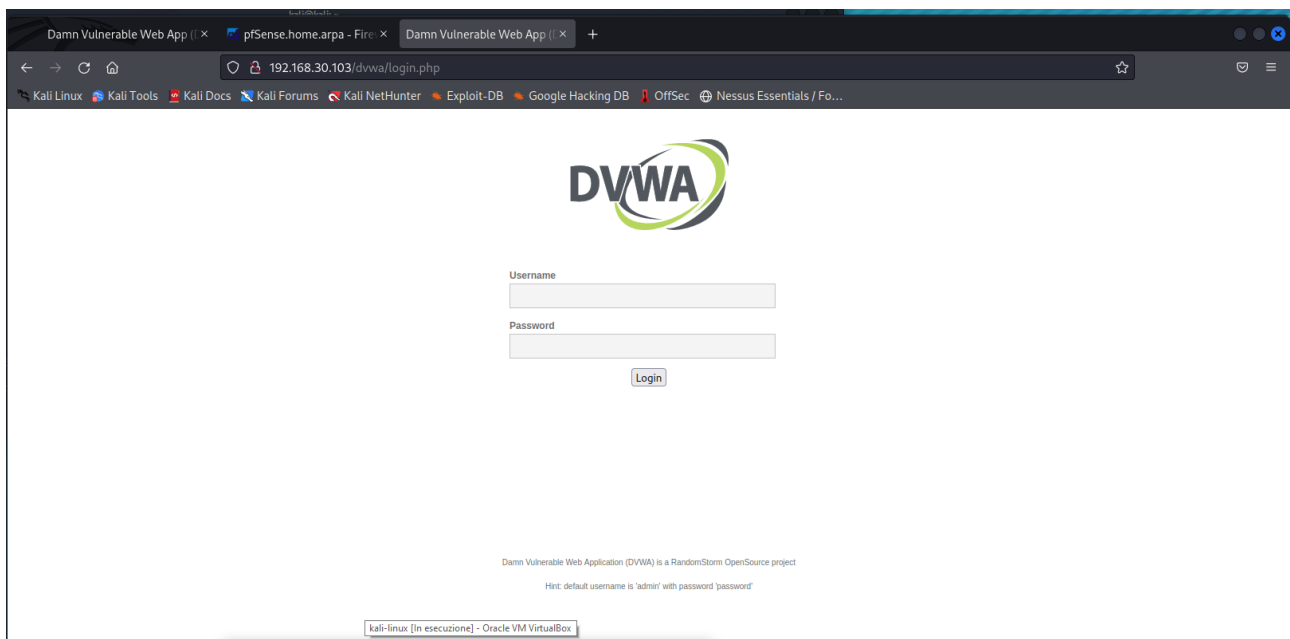
Tabella riepilogo Macchine

Macchine	IP ADDRESS	GATEWAY
Kali Linux	192.168.50.100	192.168.30.103
Metaespoitable (DVWA)	193.158.30.103	192.168.50.103

FASE 2

Nella Seconda fase abbiamo testato che tutte le macchine comunicassero per poi andare a creare la policy.

Andando a collegarci all'indirizzo IP 192.168.30.103 possiamo notare che le due macchine comunicano tra di loro



Tornando sul terminale, tramite il comando “**sudo nmap -sS 192.160.30.103**” abbiamo effettuato uno scan che ci ha riportato i seguenti valori.

```
File Actions Edit View Help
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:86:14:54 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.22 seconds

(kali@kali)-[~]
$ sudo nmap -sS 192.168.30.103
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-21 18:26 EST
Nmap scan report for 192.168.30.103
Host is up (0.000095s 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
53/tcp    open  domain
80/tcp    open  http
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
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:86:14:54 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 13.23 seconds

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



FASE 3

La terza e ultima fase consisteva nella creazione della policy del firewall. Questa policy doveva bloccare l'accesso a DVWA da parte di Kali e di conseguenza lo scan.

