

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.

Ho aggiunto la scheda di rete alla macchina virtuale pfsense.

Attivo DHCP della Lan1 con SUBNET 192.168.1.0/24:

W9D1-Pratica-PfSense

Attivo DHCP della Lan2 con SUBNET 192.168.50.0/24:

Pfsense COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

Services / DHCP Server / LAN2

LAN LAN2

General DHCP Options

DHCP Backend	Kea DHCP
Enable	<input checked="" type="checkbox"/> Enable DHCP server on LAN2 interface
Deny Unknown Clients	Allow all clients
Ignore Client Identifiers	<input type="checkbox"/> Do not record a unique identifier (UID) in client lease data if present in the client DHCP request

When set to **Allow all clients**, any DHCP client will get an IP address within this scope/range on this interface. If set to **Allow known clients from any interface**, any DHCP client with a MAC address listed in a static mapping on **any** scope(s)/interface(s) will get an IP address. If set to **Allow known clients from only this interface**, only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.

This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.

Primary Address Pool

Subnet	192.168.50.0/24
Subnet Range	192.168.50.1 - 192.168.50.254
Address Pool Range	192.168.50.100 To 192.168.50.150

The specified range for this pool must not be within the range configured on any other address pool for this interface.

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

```
File Actions Edit View Help
(kali@kali)-[~]
$ nmap -sT 192.168.50.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-11 11:11:11
Nmap scan report for 192.168.50.100
Host is up (0.013s latency).
Not shown: 977 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
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

Nmap done: 1 IP address (1 host up) scanned in 1.82 seconds

(kali@kali)-[~]
$

Epicode-Metasploitable2 [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
kali@3 packets transmitted, 0 received, 100% packet loss, time 2014ms
msfadmin@metasploitable:~$ fconfig
-bash: fconfig: command not found
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:40:10:30
          inet addr:192.168.50.100 Bcast:192.168.50.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe40:1030/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:287 errors:0 dropped:0 overruns:0 frame:0
          TX packets:384 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:29391 (28.7 KB) TX bytes:42671 (41.6 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          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
          RX bytes:215321 (210.2 KB) TX bytes:215321 (210.2 KB)

msfadmin@metasploitable:~$
```

Le due macchine comunicano perché il firewall di PfSense, ha una regola (nella Lan1) che permette la comunicazione tra le due reti.

Firewall / Rules / LAN

Floating WAN LAN LAN2

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	1/869 KiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0/0 B	IPv4 *	192.168.1.100	*	192.168.50.100	*	*	none			
<input type="checkbox"/>	0/238 KiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	

Add Add Delete Toggle Copy Save Separator

Dopo l'attivazione della regola qui sotto, la macchina Kali non è in grado di raggiungere la macchina metasploitable.

Firewall / Rules / LAN

Floating WAN LAN LAN2

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/910 KiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0/0 B	IPv4 *	192.168.1.100	*	192.168.50.100	*	*	none			
<input checked="" type="checkbox"/>	0/238 KiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	

Add Add Delete Toggle Copy Save Separator

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.

Cybersecurity Analyst 2023