

Esercitazione M3D3

Regola pfSense

Ettore Farris – 31/12/2023

1) Descrizione sintetica dell'esercitazione

L'esercitazione è finalizzata ad acquisire dimestichezza con pfSense e le impostazioni del firewall. L'esercizio consiste in:

- Avere due reti LAN interne su VirtualBox, una per Kali e una per Metasploitable con due indirizzi IP diversi che possono entrare in comunicazione grazie a pfSense;
- Far accedere Kali alla seconda rete tramite pfSense visitando il sito hostato sulla porta 80 di Metasploitable;
- Creare una regola firewall per impedire a Kali di accedere alla porta 80 di Metasploitable.

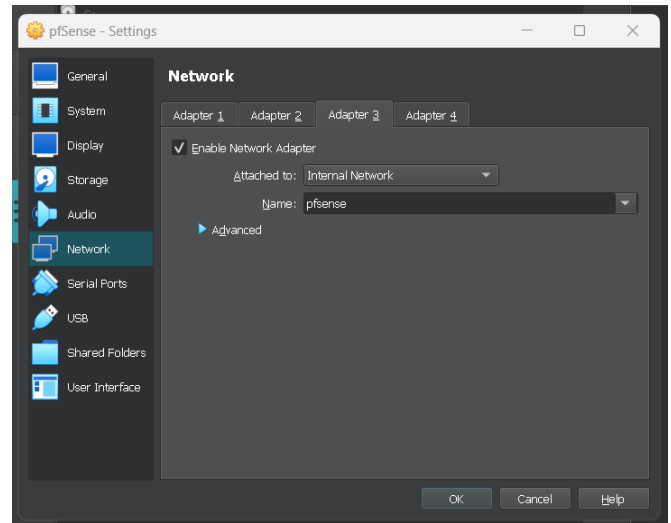
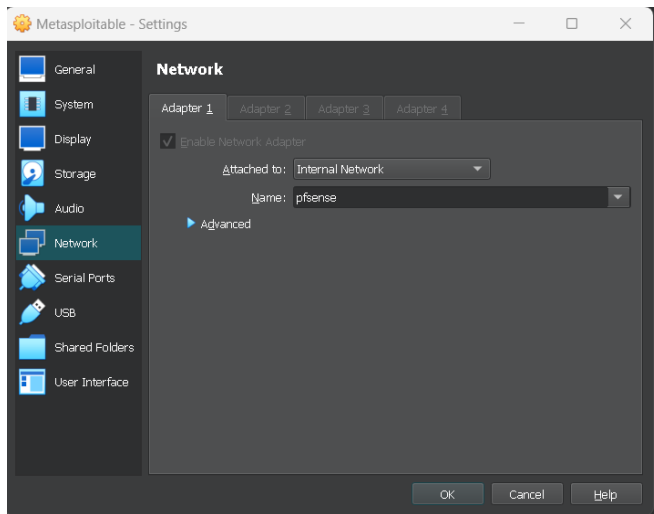
2) Svolgimento

- Creazione seconda rete interna

Su VirtualBox, dalle lezioni precedenti, abbiamo già una rete interna a cui appartiene Kali. Ne creiamo una seconda chiamata "*pfsense*".

Sulle impostazioni di rete di Metasploitable, abilitiamo una sola scheda di rete in modalità interna e assegnamola alla rete *pfsense*.

Sulle impostazioni di pfSense, abilitiamo una terza scheda di rete in modalità interna (in totale ce ne saranno una NAT e due interne) e assegnamola a *pfsense*.



- Configurazione rete

Per prima cosa cambiamo indirizzo IP alla macchina Metasploitable e assegnamogli 192.168.32.101 e default gateway 192.168.32.1 modificando il solito file */etc/network/interfaces*.

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:2b:56:8f
          inet addr:192.168.32.101  Bcast:192.168.32.255  Mask:255.255.255
          inet6 addr: fe80::a00:27ff:fe2b:568f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:460 errors:0 dropped:0 overruns:0 frame:0
          TX packets:123 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:158878 (155.1 KB)  TX bytes:28022 (27.3 KB)
          Base address:0xd020 Memory:f0200000-f0220000
```

Successivamente, su pfSense, si può notare una terza interfaccia. A questa, assegnamo l'indirizzo IP 192.168.32.1 dato che questa sarà il default gateway di Metasploitable.

```

Available interfaces:
1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)
3 - LAN2 (em2 - dhcp)

Enter the number of the interface you wish to configure: 3

Configure IPv4 address OPT1 interface via DHCP? (y/n) n

Enter the new OPT1 IPv4 address. Press <ENTER> for none:
> 192.168.32.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new OPT1 IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new OPT1 IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

```

```

WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
LAN (lan)      -> em1      -> v4: 192.168.50.1/24
LAN2 (opt1)    -> em2      -> v4: 192.168.32.1/32

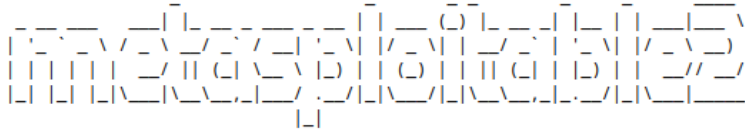
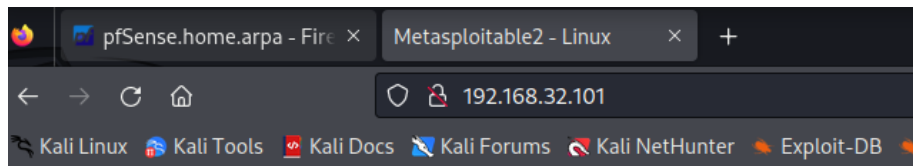
```

Lasciamo invariate le impostazioni di Kali: la macchina appartiene alla prima rete LAN e ha IP 192.168.50.100. L'IP assegnato alla rete LAN di pfSense sarà il default gateway di Kali, e pertanto avrà IP 192.168.50.1.

- Creazione regola firewall

Con le impostazioni appena salvate, la macchina Kali può contattare Metasploitable dato che, anche se appartengono a due reti diverse, pfSense funziona da router e instrada i pacchetti da una rete all'altra.

Facciamo quindi il ping alla macchina Metasploitable e visitiamo il sito web hostato sulla sua porta 80 per provare il funzionamento.



Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

```
(kali㉿kali) - [~]
$ ping 192.168.32.101
PING 192.168.32.101 (192.168.32.101) 56(84) bytes of data.
64 bytes from 192.168.32.101: icmp_seq=1 ttl=63 time=2.82 ms
64 bytes from 192.168.32.101: icmp_seq=2 ttl=63 time=3.92 ms
^C
--- 192.168.32.101 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 2.824/3.371/3.918/0.547 ms
```

Per impedire alla macchina Kali di accedere alla porta 80 di Metasploitable, creiamo una regola firewall dalla dashboard di pfSense andando su *firewall/rules*.

La regola prevede di bloccare le connessioni in uscita dalla macchina Kali verso la porta 80 della macchina Metasploitable e va configurata come segue.

Edit Firewall Rule

Action

Block

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled

☐ Disable this rule

Set this option to disable this rule without removing it from the list.

Interface

LAN

Choose the interface from which packets must come to match this rule.

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

TCP

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match

Address or Alias

192.168.50.100

/

⚙ Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination

☐ Invert match

Address or Alias

192.168.32.101

/

Destination Port Range

HTTP (80)

From

Custom

To

HTTP (80)

Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log

☒ Log packets that are handled by this rule

Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see [this article](#) for more details).

Dopo aver salvato i cambiamenti, proviamo ancora una volta ad effettuare l'accesso. Stavolta la pagina non è accessibile a causa della regola appena inserita.

```

kali@kali:~$ curl -v http://192.168.32.101
* Trying 192.168.32.101:80...
* connect to 192.168.32.101 port 80 failed: Connection timed out
* Failed to connect to 192.168.32.101 port 80 after 131105 ms: Couldn't
connect to server
* Closing connection 0
curl: (28) Failed to connect to 192.168.32.101 port 80 after 131105 ms:
Couldn't connect to server

```

