

Report S3/L5

Indice:

- 1) Introduzione → Obiettivo dell'esperimento**
 - 2) Setup Iniziale → Configurazione IP, pfSense, reti**
 - 3) Verifica della connettività (prima del firewall) → Ping (con screenshot dei risultati)**
 - 4) Test dopo il Firewall → Ping, nmap e accesso web (con screenshot di errori/accesso negato)**
 - 5) Conclusione**
-

1) Introduzione

L'obiettivo è andare a creare una policy Pfsense implementando un firewall in un sistema controllato di virtual box per **proteggere** una macchina vulnerabile (Metasploitable) dagli **attacchi** provenienti da Kali Linux.

2) Setup iniziale

Prima di tutto da virtual box andiamo in impostazioni rete creando delle schede di rete con "**rete interna**", l'obiettivo è far comunicare kali con Pfsense e separatamente in un'altra rete anche Metasploitables 2 con Pfsense.

Ora configuriamo gli ip statici:

metasploitable2

```

GNU nano 2.0.7           File: /etc/network/interfaces           Modified

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
    address 192.168.40.101
    netmask 255.255.255.0
    gateway 192.168.40.1

```

ctrl+x per salvare

```

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:e8:90:26
          inet addr:192.168.40.101 Bcast:192.168.40.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fee8:9026/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:64 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B) TX bytes:4752 (4.6 KB)
          Base address:0xd240 Memory:f0820000-f0840000

```

Ora l'ip è statico su Metasploitable.

così come sugli altri.

3) Verifica della connettività (prima del firewall) → Ping (con screenshot dei risultati)

```

[+] (kali㉿kali)-[~]
$ ping -c 4 192.168.40.101
PING 192.168.40.101 (192.168.40.101) 56(84) bytes of data.
64 bytes from 192.168.40.101: icmp_seq=1 ttl=64 time=0.355 ms
64 bytes from 192.168.40.101: icmp_seq=2 ttl=64 time=0.410 ms
64 bytes from 192.168.40.101: icmp_seq=3 ttl=64 time=0.389 ms
64 bytes from 192.168.40.101: icmp_seq=4 ttl=64 time=0.372 ms

--- 192.168.40.101 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3067ms

```

come possiamo notare il ping su metasploitable funziona su kali linux, questo significa che il sistema metasploitables è vulnerabile, ora configureremo come da consegna il firewall e

dimostreremo cosa cambia

4) Test dopo il Firewall → Ping fallito = successo del sistema difensivo

```
[root@kali ~]# $ ping -c 4 192.168.40.101
PING 192.168.40.101 (192.168.40.101) 56(84) bytes of data.
From 192.168.50.100 icmp_seq=1 Destination Host Unreachable
From 192.168.50.100 icmp_seq=2 Destination Host Unreachable
From 192.168.50.100 icmp_seq=3 Destination Host Unreachable
From 192.168.50.100 icmp_seq=4 Destination Host Unreachable

--- 192.168.40.101 ping statistics ---
4 packets transmitted, 0 received, +4 errors, 100% packet loss, time 3067ms
```

come possiamo notare dopo l'utilizzo di Pfsense come firewall metaspitable resta [protetto](#) dal ping di kali

5) Conclusione

L'esperimento ha dimostrato l'efficacia di pfSense come firewall nel proteggere una macchina vulnerabile (Metasploitable) dagli attacchi provenienti da Kali Linux.

Nella prima fase, abbiamo verificato la connettività tra le macchine: **Kali riusciva a pingare Metasploitable senza restrizioni, confermando che la macchina vulnerabile era esposta.** Successivamente, è stata implementata una regola firewall su pfSense per bloccare il traffico proveniente da Kali, impedendo ogni tentativo di connessione.

Dopo aver attivato la regola, il ping da Kali a Metasploitable ha dimostrando che la comunicazione era stata effettivamente bloccata. Questo risultato conferma che la configurazione del firewall ha avuto successo, migliorando la sicurezza della rete e limitando l'accesso non autorizzato.

L'esercizio ha evidenziato l'importanza della segmentazione della rete e della gestione delle policy di sicurezza per proteggere macchine vulnerabili da possibili attacchi.

Luca Tavani