

CS0424IT — ESERCITAZIONE S5L1 - REGOLA FIREWALL

Simone La Porta



TRACCIA

Creare una regola firewall che blocchi l'accesso alla DVWA (su metasploitable) dalla macchina Kali Linux e ne impedisca di conseguenza lo scan. 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.

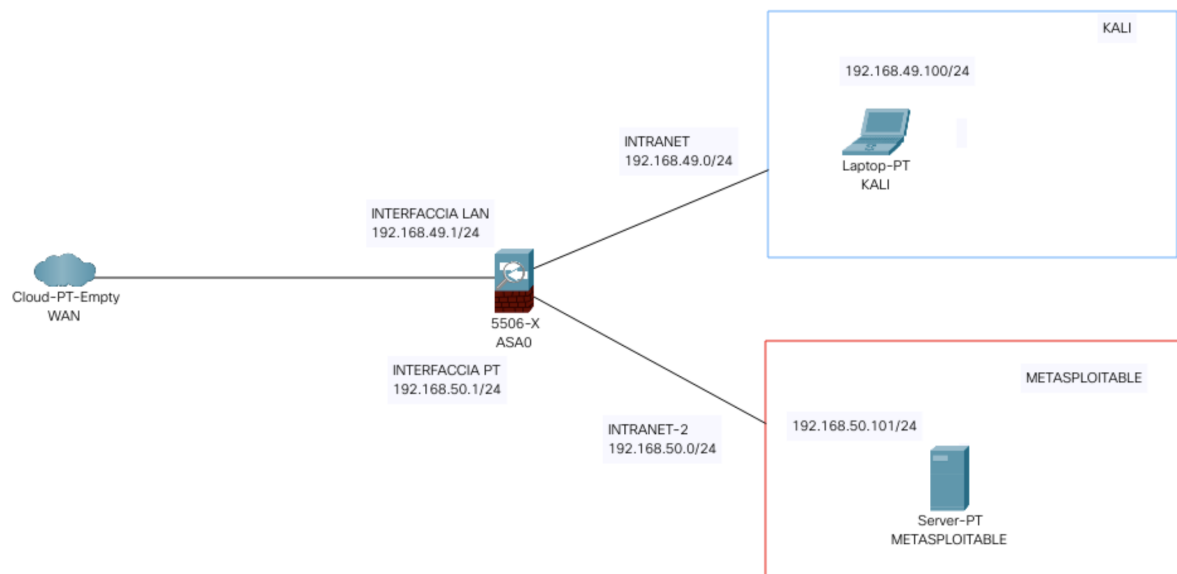
SVOLGIMENTO

Assicurarsi che pfSense sia configurato correttamente su una macchina virtuale con tre schede di rete:

- **NAT** (interfaccia WAN)
- **Rete interna (intnet)** (interfaccia LAN)
- **Rete interna (pfsense)**

Configurare le interfacce di rete su pfSense aggiungendo e configurando la nuova interfaccia:

1. **Interfaces** → **Assignments**.
2. Aggiungere una nuova interfaccia, la terza scheda di rete (chiamata OPT1).



3. Assegnare un nome all'interfaccia, OPT1.
4. Configurare l'indirizzo IP dell'interfaccia OPT1, 192.168.49.1/24.

```
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***
WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
LAN (lan)      -> em1      -> v4: 192.168.50.1/24
OPT1 (opt1)    -> em2      -> v4: 192.168.49.1/24
```

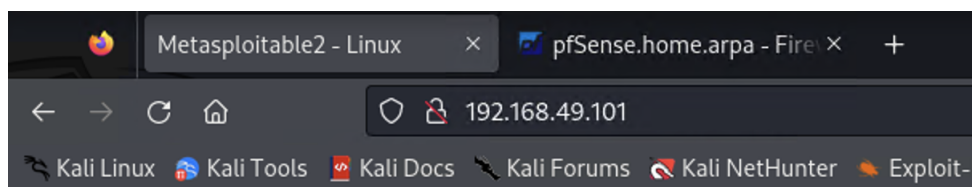
Verifica della connettività

1. **Ping da Kali Linux a Metasploitable2:** tramite terminale su Kali Linux e pingare l'IP di Metasploitable2 per assicurarsi che ci sia connettività.

```
ping 192.168.49.101
```

2. **Accedere alla DVWA:** tramite browser su Kali Linux provare ad accedere a DVWA sull'IP di Metasploitable2.

```
(kali@kali)-[~]
$ ping 192.168.49.101
PING 192.168.49.101 (192.168.49.101) 56(84) bytes of data.
64 bytes from 192.168.49.101: icmp_seq=1 ttl=63 time=3.80 ms
64 bytes from 192.168.49.101: icmp_seq=2 ttl=63 time=5.46 ms
64 bytes from 192.168.49.101: icmp_seq=3 ttl=63 time=7.89 ms
64 bytes from 192.168.49.101: icmp_seq=4 ttl=63 time=7.92 ms
64 bytes from 192.168.49.101: icmp_seq=5 ttl=63 time=7.07 ms
64 bytes from 192.168.49.101: icmp_seq=6 ttl=63 time=8.75 ms
64 bytes from 192.168.49.101: icmp_seq=7 ttl=63 time=9.68 ms
^C
— 192.168.49.101 ping statistics —
7 packets transmitted, 7 received, 0% packet loss, time 6015ms
rtt min/avg/max/mdev = 3.800/7.222/9.678/1.857 ms
```



Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

- [TWiki](#)
- [phpMyAdmin](#)
- [Mutillidae](#)
- [DVWA](#)
- [WebDAV](#)

Creazione della regola firewall














Accedere alla Web GUI di pfSense e andare su **Firewall** → **Rules** e selezionare l'interfaccia LAN1.

Aggiungere la regola:

1. Cliccare su **Add** per creare una nuova regola.
2. Configurare la regola come segue:

- **Action:** Block
- **Interface:** LAN1
- **Address Family:** IPv4
- **Protocol:** Any
- **Source:** Network, 192.168.50.100/24
- **Destination:** Single host or alias, 192.168.49.101 (IP di Metasploitable2)
- **Destination Port Range:** 80 (HTTP)
- **Description:** Block access to DVWA from Kali Linux

3. Cliccare su **Save** e poi su **Apply Changes**.

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/> 	0/0 B	IPv4 TCP	192.168.50.100	*	192.168.49.101	80 (HTTP)	*	none		Blocco DVWA Meta da Kali	  
<input type="checkbox"/> 	22/1.62 MiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	  
<input type="checkbox"/> 	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	  

Conferma dell'impostazione della regola: provando a raggiungere nuovamente la DVWA, si nota che questa sia inaccessibile. In particolare si nota come la risposta del server non sia legata ad un errore 404, ma proprio ad una mancata risposta. Questo comportamento di mancata risposta indica che il firewall pfSense è riuscito a bloccare le richieste.

Firewall / Rules / Edit

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

192.168.49.101

/

Destination Port Range

HTTP (80)

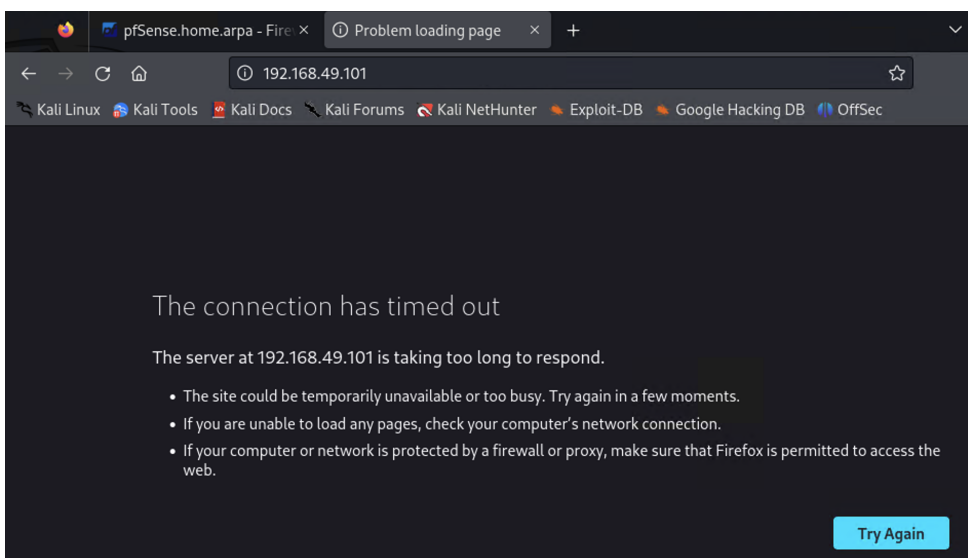
From

Custom

To

Custom

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



BONUS: ricerca backdoor

È stata fatta una scansione nmap di tutte le porte della Metasploitable2 individuando nella porta 1524 una possibile backdoor. Questo è stato confermato dall'accesso tramite Netcat alla shell di Metasploitable2 con privilegi di root.

```
(kali@kali)-[~]
$ sudo nmap -sS -sV 192.168.49.101
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-24 18:43 CEST
Nmap scan report for 192.168.49.101
Host is up (0.019s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            vsftpd 2.3.4
22/tcp    open  ssh            OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet         Linux telnetd
25/tcp    open  smtp           Postfix smtpd
53/tcp    open  domain         ISC BIND 9.4.2
80/tcp    open  http           Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind        2 (RPC #100000)
139/tcp   open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn    Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec           netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell          Netkit rshd
1099/tcp  open  java-rmi       GNU Classpath grmiregistry
1524/tcp  open  bindshell      Metasploitable root shell
2049/tcp  open  nfs            2-4 (RPC #100003)
2121/tcp  open  ccproxy-ftp?
3306/tcp  open  mysql          MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql     PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc            VNC (protocol 3.3)
6000/tcp  open  X11            (access denied)
6667/tcp  open  irc            UnrealIRCd
8009/tcp  open  ajp13          Apache Jserv (Protocol v1.3)
8180/tcp  open  http           Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 175.66 seconds
```

```
(kali@kali)-[~]
$ nc 192.168.49.101 1524
root@metasploitable:/# ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
root@metasploitable:/#
```