

Esame S3L5

Marco Falchi

Consegna:



Esercizio
Pfsense

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. 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.

Considerazioni pre esercizio:

La consegna dell'esercizio si presenta per me di difficile comprensione inizialmente ma con un po' di logica capisco cosa devo fare e mi accorgo subito che ho bisogno di informarmi usando le slide per ricordare alcuni comandi passati all'interno della metasploitable e che sarà una prova abbastanza complessa a livello logico.

Report tecnico

L'obiettivo primario di questa attività era la configurazione di una regola firewall su un sistema pfSense per gestire e filtrare il traffico di rete in un ambiente controllato. Nello specifico, si intendeva bloccare l'accesso da una macchina Kali Linux al servizio web DVWA (Damn Vulnerable Web Application), ospitato su una macchina virtuale Metasploitable2.

Prerequisiti

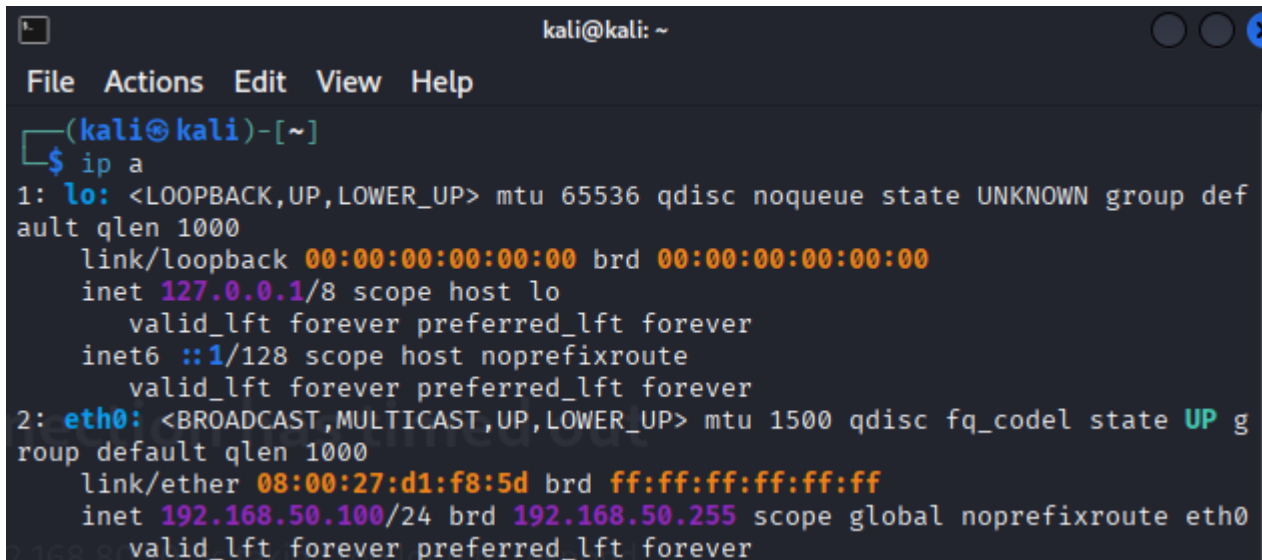
Per soddisfare i requisiti, le due macchine virtuali sono state configurate su due sottoreti separate:

- Macchina Kali Linux: configurata con l'indirizzo IP statico 192.168.50.100/24.

Macchina Metasploitable2: configurata con indirizzo IP statico 192.168.80.101/24 e gateway 192.168.80.1

```
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:12:ff:6c brd ff:ff:ff:ff:ff:ff
    inet 192.168.80.101/24 brd 192.168.80.255 scope global eth0
    inet6 fe80::a00:27ff:fe12:ff6c/64 scope link
        valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$
```

```
msfadmin@metasploitable:~$ route add default gw 192.168.80.1
```



```
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:d1:f8:5d brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.100/24 brd 192.168.50.255 scope global noprefixroute eth0
        valid_lft forever preferred_lft forever
```

Configurazione interfaccia

È stata creata una nuova interfaccia su pfSense, denominata "Meta", per gestire il traffico della rete dedicata alla macchina Metasploitable2.

L'interfaccia è stata poi abilitata e configurata con i seguenti parametri:

- Descrizione: Meta
- Tipo di Configurazione IPv4: Static IPv4
- Indirizzo IPv4: 192.168.80.1 con una subnet mask di /24

Interfaces / Meta (em0)

General Configuration

Enable

☒ Enable interface

Description

Meta

Enter a description (name) for the interface here.

IPv4 Configuration Type

Static IPv4

IPv6 Configuration Type

None

MAC Address

xxxxxxxxxxxx

This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xxxxxxxx:xxxx:xx or leave blank.

MTU

If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS

If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Speed and Duplex

Default (no preference, typically autoselect)

Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Static IPv4 Configuration

IPv4 Address

192.168.80.1

/ 24

IPv4 Upstream gateway

None

+ Add a new gateway

Interface	Network port
WAN	vtnet0 (08:00:27:12:de:2e)
LAN	vtnet1 (08:00:27:8f:67:9f)
Meta	em0 (08:00:27:47:7a:11)

Save

Delete

Delete

Creazione della Regola Firewall

Successivamente, è stata definita una regola sul firewall per implementare il blocco del traffico desiderato. La regola è stata configurata come segue:

- **Action:** Block. Questa azione scarta i pacchetti in modo silente, senza inviare una risposta al mittente.
- **Interface:** LAN. La regola si applica al traffico in ingresso dall'interfaccia LAN, dove è connessa la macchina Kali Linux.
- **Address Family:** IPv4
- **Protocol:** TCP
- **Source:** 192.168.50.100 (Indirizzo IP della macchina Kali Linux)
- **Destination:** 192.168.80.101 (Indirizzo IP della macchina Metasploitable)
- **Destination Port Range:** HTTP (porta 80)

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

192.168.80.101

/

Destination Port Range

HTTP (80)

From

Custom

To

HTTP (80)

Custom

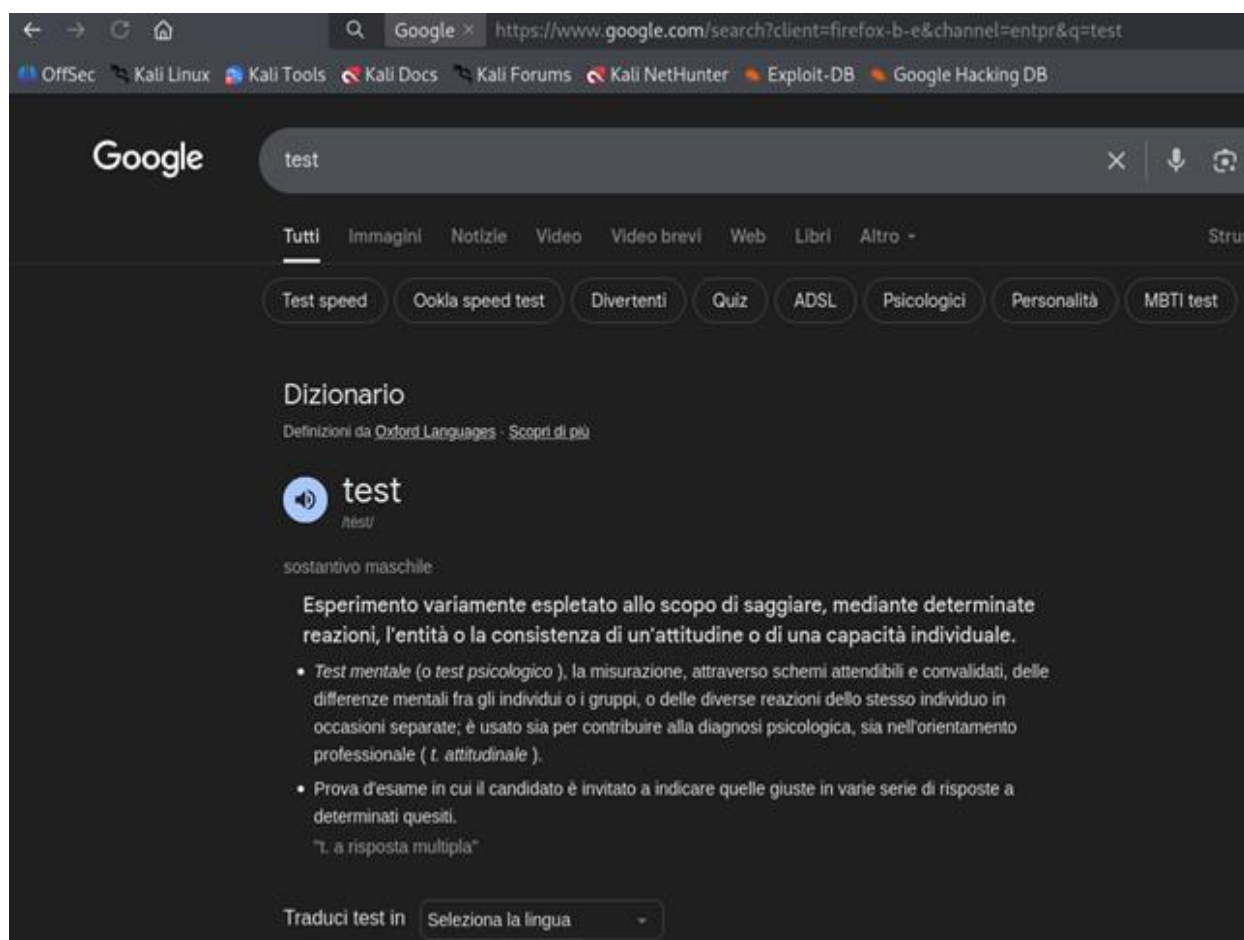
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Test e Verifica dei Risultati

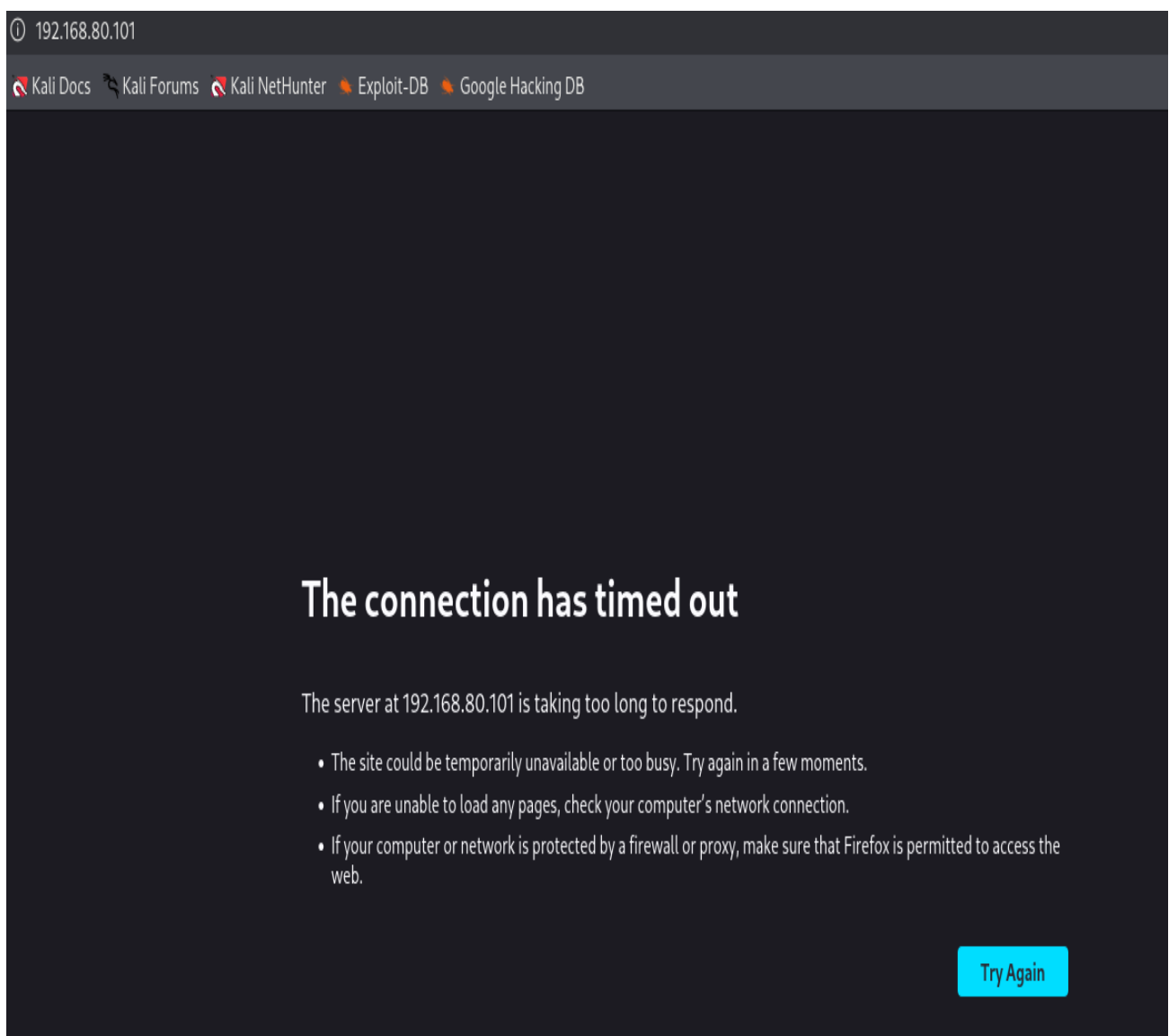
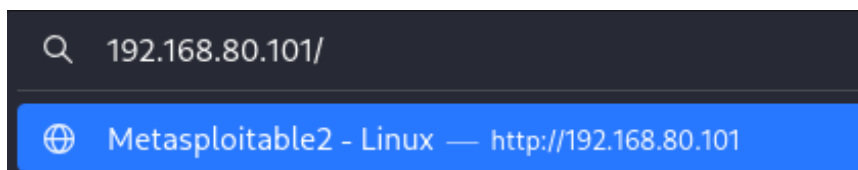
Per validare l'efficacia della configurazione, sono stati eseguiti dei test di connettività dalla macchina Kali Linux.

Navigazione su siti web con porta non controllata dal firewall: La navigazione verso siti esterni che utilizzano il protocollo HTTPS (porta 443), come Google, ha funzionato correttamente.

Questo dimostra che la regola non ha interrotto la connettività generale della macchina ai siti con porte https 443.



Navigazione su siti web con porta controllata dal firewall: Il tentativo di accesso via browser all'indirizzo `http://192.168.80.101` è fallito, generando un errore di "The connection has timed out". Questo risultato è coerente con l'azione "Block" della regola firewall, che scarta i pacchetti senza notificare il client, causando un timeout della richiesta



Test scansione porte senza firewall

```
└─$ nmap -n 192.168.80.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-18 08:30 EDT
Nmap scan report for 192.168.80.101
Host is up (0.0013s 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
```

e

Al fine di verificare lo stato di connettività iniziale, ho proceduto con una scansione delle porte da Kali Linux verso metasploitable2. Questa operazione è stata eseguita con la regola di filtraggio del firewall temporaneamente disattivata, ha confermato quindi che le porte di servizio erano tutte aperte.

Test scansione con firewall

```
(kali㉿kali)-[~]
└─$ nmap -n 192.168.80.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-18 08:31 EDT
Nmap scan report for 192.168.80.101
Host is up (0.0010s 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    filtered  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
```

Ho successivamente proceduto con una scansione delle porte da Kali Linux verso metasploitable2 ma questa volta con le regole di filtraggio firewall attive, ha confermato quindi che le porte di servizio erano tutte aperte tranne quella bloccata dal nostro firewall che è quindi filtrata.

Conclusione

I test effettuati confermano il successo della configurazione. La regola firewall implementata su pfSense blocca efficacemente il traffico sulla porta 80 (HTTP) proveniente dalla macchina Kali Linux e diretto alla macchina Metasploitable2, come richiesto dall'obiettivo. L'accesso al servizio DVWA è stato quindi inibito, mantenendo al contempo la connettività per altri servizi di rete. L'obiettivo dell'esercizio è stato pienamente raggiunto.

Considerazioni post esercizio:

Alla fine dell'esercitazione sono totalmente conscio di ciò che ho fatto e sicuro del mio esercizio, è stata una sfida nella parte iniziale capire come configurare tutto, ho invece trovato facile e logico configurare il firewall, ho avuto diversi problemi durante l'esercitazione ma si trattava sempre di piccoli problemi che ho poi risolto dopo poco con la logica.