

# ESERCIZIO: Creare una regola firewall su pfSense

**Traccia:** Creare una regola firewall su pfSense per bloccare l'accesso alla web app DVWA (installata su Metasploitable) da parte della macchina Kali Linux, impedendo anche la scansione delle porte.

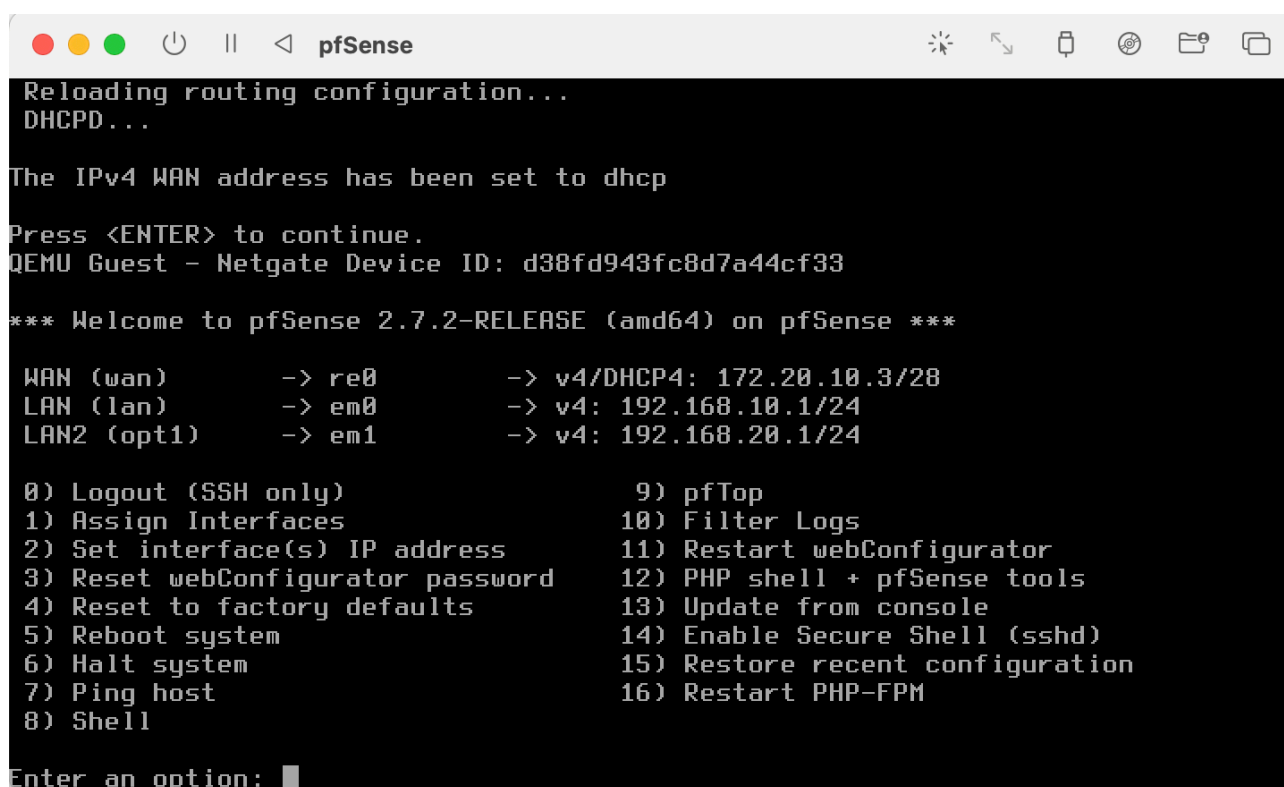
## 1. Premessa

**DVWA (Damn Vulnerable Web Application)** è un'applicazione web volutamente vulnerabile, progettata per scopi didattici e di test. Viene comunemente utilizzata in ambienti di laboratorio per esercitazioni di **penetration testing**, analisi delle vulnerabilità e **simulazioni di attacchi informatici**.

L'obiettivo di DVWA è fornire una piattaforma sicura dove studenti, ethical hacker e professionisti della cybersecurity possano esercitarsi nel trovare e correggere vulnerabilità tipiche delle applicazioni web, come SQL injection, XSS (Cross Site Scripting), file inclusion e molto altro.

In questa esercitazione, DVWA è installata sulla macchina **Metasploitable** e rappresenta il bersaglio da proteggere. Utilizzeremo **pfSense**, un firewall open-source, per bloccare l'accesso non autorizzato da parte di **Kali Linux**, una distribuzione orientata al penetration testing.

## 2. Configurazione iniziale



```
pfSense
Reloading routing configuration...
DHCPD...

The IPv4 WAN address has been set to dhcp

Press <ENTER> to continue.
QEMU Guest - Netgate Device ID: d38fd943fc8d7a44cf33

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> re0      -> v4/DHCP4: 172.20.10.3/28
LAN (lan)      -> em0      -> v4: 192.168.10.1/24
LAN2 (opt1)    -> em1      -> v4: 192.168.20.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

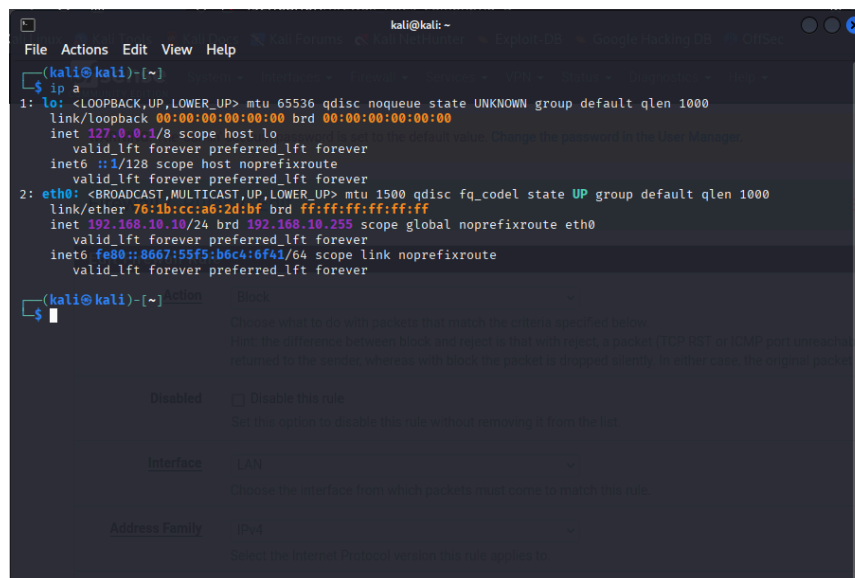
Enter an option: 
```

Per permettere la comunicazione tra le due macchine virtuali (Kali e Metasploitable) passando da pfSense, abbiamo configurato tre interfacce su pfSense:

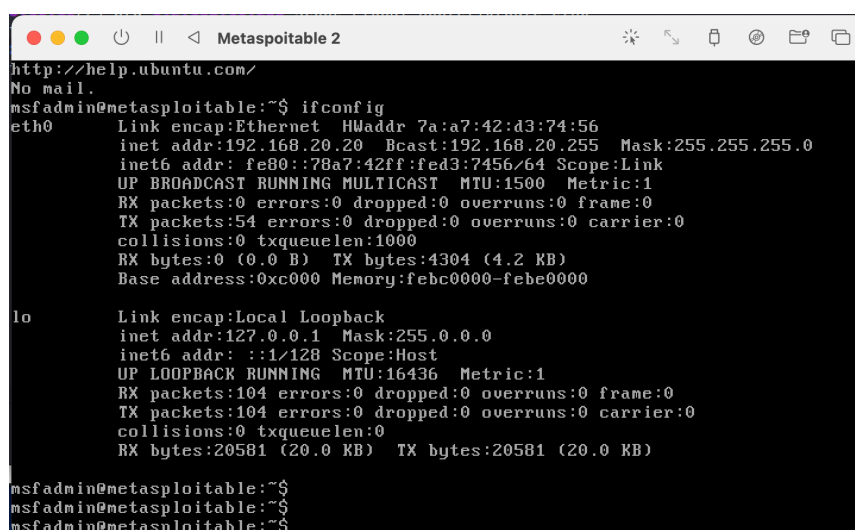
- **WAN (re0)** → DHCP (es. 172.20.10.3/28)
- **LAN (em0)** → 192.168.10.1/24
- **LAN2/OPT1 (em1)** → 192.168.20.1/24

Abbiamo poi assegnato un IP statico alle due macchine:

- **Kali Linux:** 192.168.10.10 → connessa alla LAN
- **Metasploitable:** 192.168.20.20 → connessa a LAN2



```
kali@kali: ~  
File Actions Edit View Help  
$ 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 76:1b:cc:a6:2d:bf brd ff:ff:ff:ff:ff:ff  
    inet 192.168.10.10/24 brd 192.168.10.255 scope global noprefixroute eth0  
        valid_lft forever preferred_lft forever  
    inet6 fe80::8667:55f5:b6c4:6f41/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever  
$
```



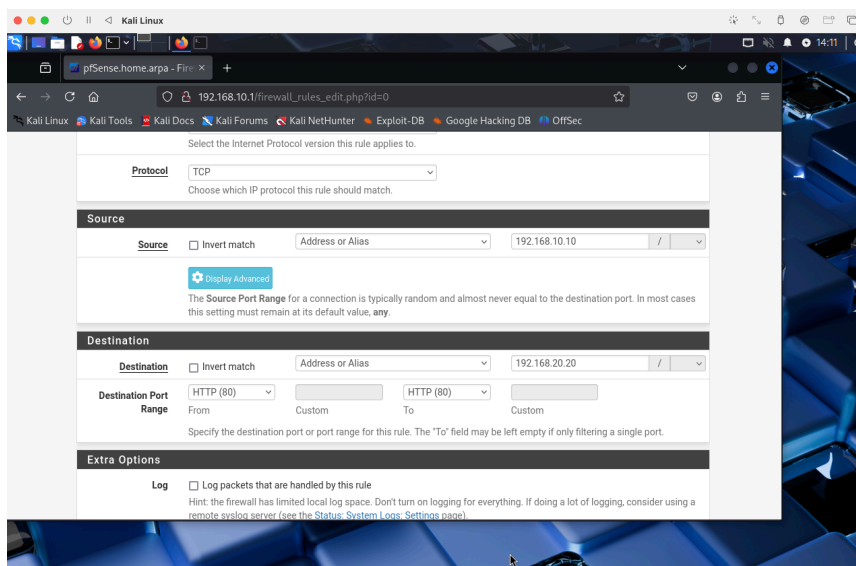
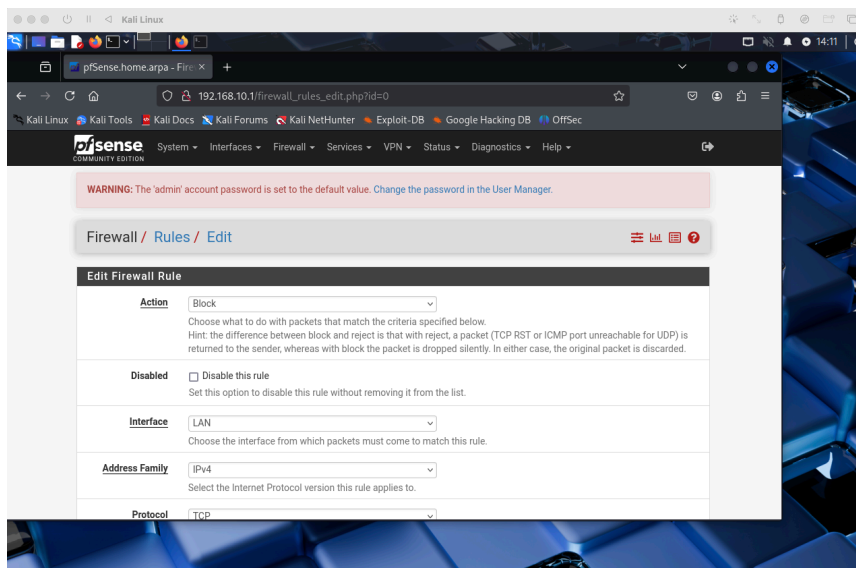
```
Metasploitable 2  
http://help.ubuntu.com/  
No mail.  
msfadmin@metasploitable:~$ ifconfig  
eth0      Link encap:Ethernet  HWaddr 7a:a7:42:d3:74:56  
          inet addr:192.168.20.20  Bcast:192.168.20.255  Mask:255.255.255.0  
          inet6 addr: fe80::78a7:42ff:fed3:7456/64  Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:54 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:0 (0.0 B)  TX bytes:4304 (4.2 KB)  
          Base address:0xc000  Memory:febc0000-febe0000  
  
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:104 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:104 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:20581 (20.0 KB)  TX bytes:20581 (20.0 KB)  
  
msfadmin@metasploitable:~$  
msfadmin@metasploitable:~$  
msfadmin@metasploitable:~$
```

### 3. Accesso a DVWA

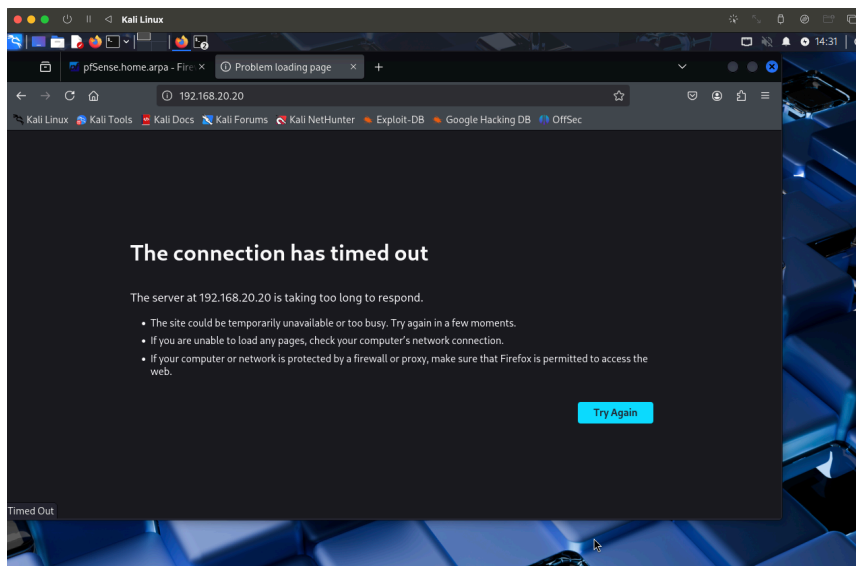
Aprendo il browser su Kali e digitando `http://192.168.20.20`, l'accesso alla web app **DVWA** ospitata su Metasploitable è concesso e visibile. Questo conferma che la comunicazione su **porta 80** (HTTP) è attiva tra le due VM.

### 4. Creazione della regola firewall (blocco HTTP)

Dal pannello di pfSense abbiamo creato una regola sulla **interfaccia LAN** per bloccare il traffico proveniente da Kali verso Metasploitable su porta 80:

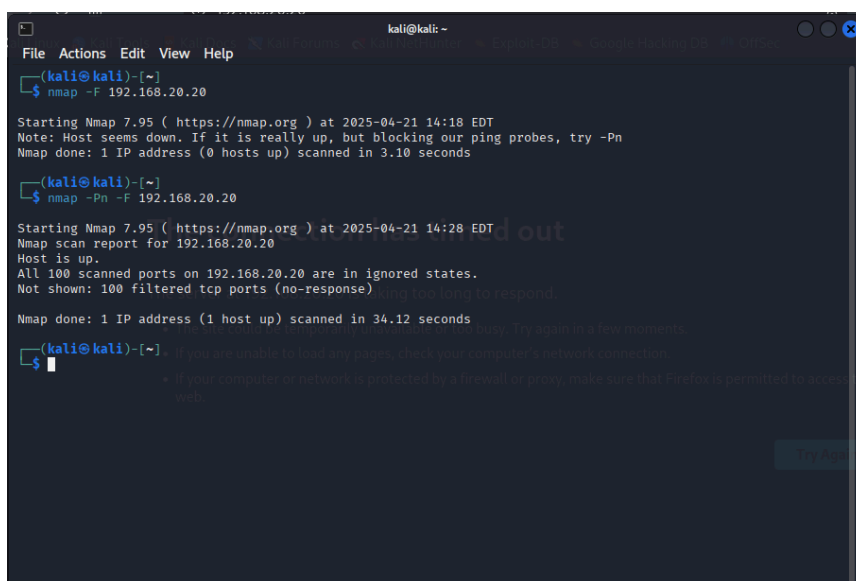


Salvata la regola e applicate le modifiche, abbiamo testato nuovamente l'accesso a DVWA da browser: **accesso negato**, la pagina non si carica più. Obiettivo raggiunto.



## 5. Verifica finale con Nmap

Per testare se la regola firewall blocca correttamente anche le **scansioni delle porte**, abbiamo eseguito due comandi Nmap dalla macchina Kali verso Metasploitable:



### Primo test:

```
nmap -F 192.168.20.20
```

### Risultato primo test:

Il firewall pfSense **blocca le richieste di ping ICMP**, quindi Nmap *presume* che l'host sia spento.

### Secondo test (senza ping):

```
nmap -Pn -F 192.168.20.20
```

### Risultato secondo test:

L'host è attivo, ma **tutte le porte risultano "filtered"**, ovvero i pacchetti vengono intercettati e scartati dal firewall **senza risposta**, rendendo impossibile sapere se la porta sia chiusa o aperta.

Questo comportamento dimostra che la regola firewall è **efficace sia contro accessi web (HTTP)** sia contro **tentativi di scansione delle porte**, migliorando la sicurezza della rete.

## 6. CONCLUSIONI

Abbiamo implementato con successo una regola firewall su pfSense per impedire l'accesso HTTP da una macchina (Kali) verso un servizio vulnerabile (DVWA su Metasploitable) situato in un'altra rete.

Questo tipo di esercitazione mostra l'importanza del **controllo del traffico inter-LAN** e della capacità di isolare servizi potenzialmente pericolosi tramite firewall.

Un ambiente ben segmentato con regole precise migliora la **sicurezza interna** e permette una gestione efficace degli accessi tra le varie componenti di rete.