

RELAZIONE TECNICA: Configurazione Firewall e Segmentazione di Rete con pfSense

Studente: Caccamo Rocco Paolo

Corso: Cyber Security & Ethical Hacking - Episode **Data:** 12/12/2025

1. Obiettivo dell'Esercitazione

L'obiettivo di questa attività è stato configurare un firewall pfSense per gestire la segmentazione di rete tra una macchina attaccante (Kali Linux) e una macchina vulnerabile (Metasploitable 2). Nello specifico, è stato richiesto di:

1. Isolare le due macchine su sottoreti diverse.
2. Configurare una regola firewall per bloccare il traffico HTTP (Porta 80) verso la macchina target.
3. Garantire che il traffico ICMP (Ping) rimanga consentito per la diagnostica.

2. Topologia di Rete

Utilizzando la console di pfSense, ho configurato le interfacce di rete assegnando indirizzi IP statici per fungere da gateway per le rispettive sottoreti.

La configurazione finale, verificata tramite console, è la seguente:

- **WAN (vtnet0):** Assegnata via DHCP (Rete esterna).
- **LAN (vtnet1):** Gateway **192.168.50.1/24** (Kali Linux).
- **OPT1 (em0):** Gateway **192.168.20.1/24** (Metasploitable).
- Come mostrato nello screenshot seguente, le interfacce sono attive e configurate correttamente.

```
VirtualBox Virtual Machine - Netgate Device ID: 876fa8d858a8fcda863d
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***
WAN (wan)      -> vtnet0      -> v4/DHCP4: 192.168.6.13/22
                           v6/DHCP6: fd28:9e19:28f4:1:a00:27ff:fe12:de2e
64
LAN (lan)      -> vtnet1      -> v4: 192.168.50.1/24
OPT1 (opt1)    -> em0        -> v4: 192.168.20.1/24

8) 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

Enter an option:
Message from syslogd@pfSense at Dec 12 16:51:04 ...
php-fpm[2068]: /firewall_rules.php: Successful login for user 'admin' from: 192
```

3. Configurazione della Policy di Sicurezza (Firewall Rules)

Per soddisfare i requisiti di sicurezza, ho creato una regola firewall specifica sull'interfaccia **LAN** (sorgente del traffico).

La regola è stata configurata per bloccare selettivamente il protocollo TCP destinato alla porta 80 della macchina Metasploitable.

- **Action:** Block
- **Interface:** LAN
- **Protocol:** IPv4 TCP
- **Source:** 192.168.50.10 (IP Kali)
- **Destination:** 192.168.20.10 (IP Metasploitable)
- **Destination Port:** 80 (HTTP)

La regola è stata posizionata in cima alla lista per garantirne la priorità rispetto alla regola predefinita "Default allow LAN to any".

The screenshot shows a web-based firewall configuration interface. At the top, there's a navigation bar with 'Firewall / Rules / LAN'. Below it, a sub-navigation bar has tabs for 'Floating', 'WAN', 'LAN' (which is selected and highlighted in red), and 'OPT1'. The main area is titled 'Rules (Drag to Change Order)'. It contains a table with the following data:

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	4/1.26 MiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0/1 KiB	IPv4 TCP	192.168.50.10	*	192.168.20.10	80 (HTTP)	*	none			
<input type="checkbox"/>	8/7.35 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	

At the bottom of the table are several action buttons: Add, Add, Delete, Toggle, Copy, Save, and Separator.

4. Test di Verifica

Al termine della configurazione, ho eseguito dei test di connettività dalla macchina Kali Linux verso la macchina Metasploitable per verificare l'efficacia delle regole.

4.1 Test Connessione ICMP (Ping)

Ho eseguito un comando `ping` verso l'indirizzo 192.168.20.10. **Esito:** Positivo. Il firewall permette il passaggio dei pacchetti ICMP poiché la regola di blocco è specifica solo per il protocollo TCP. Ciò dimostra che il routing tra le due reti funziona correttamente.

```

Session Actions Edit View Help
(kali㉿kali)-[~]
└─$ ip link
1: tor <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 <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:00:27:1f:b7:23 brd ff:ff:ff:ff:ff:ff
        inet 192.168.50.10/24 brd 192.168.50.255 scope global noprefixroute eth0
            valid_lft forever preferred_lft forever
            inet6 fe80::1dbb:1cfe:ec1c:7ad3/64 scope link noprefixroute
                valid_lft forever preferred_lft forever

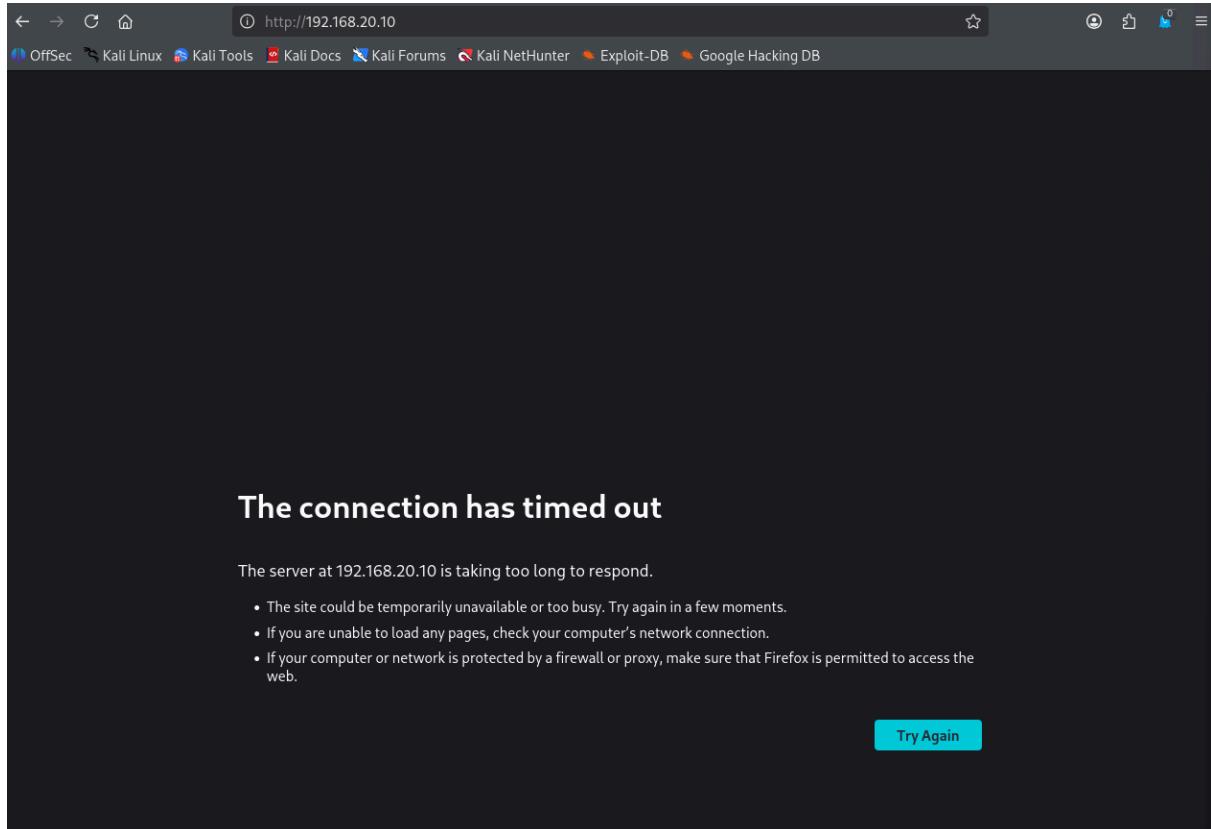
(kali㉿kali)-[~]
└─$ ping 192.168.20.10
PING 192.168.20.10 (192.168.20.10) 56(84) bytes of data.
64 bytes from 192.168.20.10: icmp_seq=1 ttl=63 time=0.266 ms
64 bytes from 192.168.20.10: icmp_seq=2 ttl=63 time=0.368 ms
64 bytes from 192.168.20.10: icmp_seq=3 ttl=63 time=0.302 ms

```

4.2 Test Accesso Web (HTTP)

Ho tentato di accedere al servizio web DVWA tramite browser all'indirizzo

http://192.168.20.10. **Esito:** Negativo (Timeout). Il browser non riesce a stabilire una connessione, andando in timeout. Questo conferma che il firewall sta scartando silenziosamente i pacchetti diretti alla porta 80, impedendo l'accesso al sito web vulnerabile.



5. Conclusioni

L'esercitazione è stata completata con successo. La separazione delle reti è stata implementata correttamente e le regole firewall

agiscono con la granularità richiesta, bloccando servizi specifici senza isolare completamente l'host a livello di rete.