

# Relazione progetto individuale

## U1-S3-L5

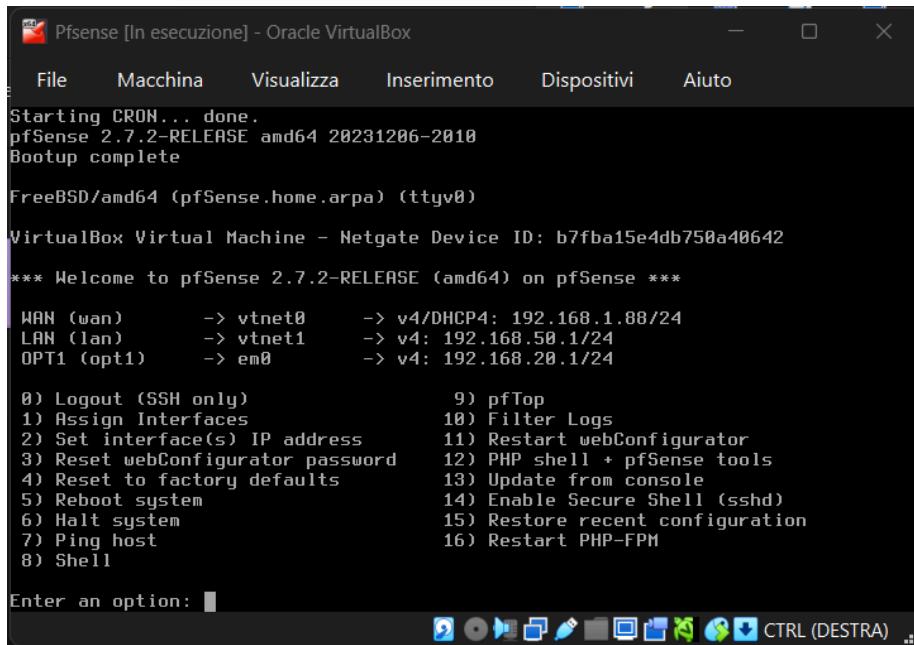
## Configurazione del Firewall pfSense

Questo esercizio ha avuto come obiettivo la creazione e l'applicazione di una regola firewall su pfSense per bloccare l'accesso al servizio **DVWA** (su Metasploitable) dalla macchina **Kali Linux**. Un requisito fondamentale dell'esercizio è che le macchine Kali e Metasploitable fossero su reti diverse, gestite da interfacce separate del firewall pfSense.

### 1. Configurazione Dettagliata delle Interfacce di pfSense

Per soddisfare il requisito di reti separate, sono state aggiunte due nuove interfacce di rete (LAN, OPT1) oltre all'interfaccia WAN già presente e la configurazione degli indirizzi IP è stata eseguita da terminale di pfSense.

Di seguito il dettaglio della configurazione applicata:



Pfsense [In esecuzione] - Oracle VirtualBox

```
File Macchina Visualizza Inserimento Dispositivi Aiuto

Starting CRON... done.
pfSense 2.7.2-RELEASE amd64 20231206-2010
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: b7fba15e4db750a40642

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

WAN (wan)      -> vtne0      -> v4/DHCP4: 192.168.1.88/24
LAN (lan)      -> vtne1      -> v4: 192.168.50.1/24
OPT1 (opt1)    -> em0       -> 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

Enter an option: 
```

Le due macchine connesse alle interfacce sono state settate in DHCP di modo che venisse loro assegnato in automatico un indirizzo IP

**Kali Linux** è stata collegata all'interfaccia **LAN** e ha ricevuto l'indirizzo IP 192.168.50.151 con subnet mask /24.

**Metasploitable** è stata collegata all'altra interfaccia **OPT1** e ha ricevuto l'indirizzo IP 192.168.20.11 con subnet mask /24.

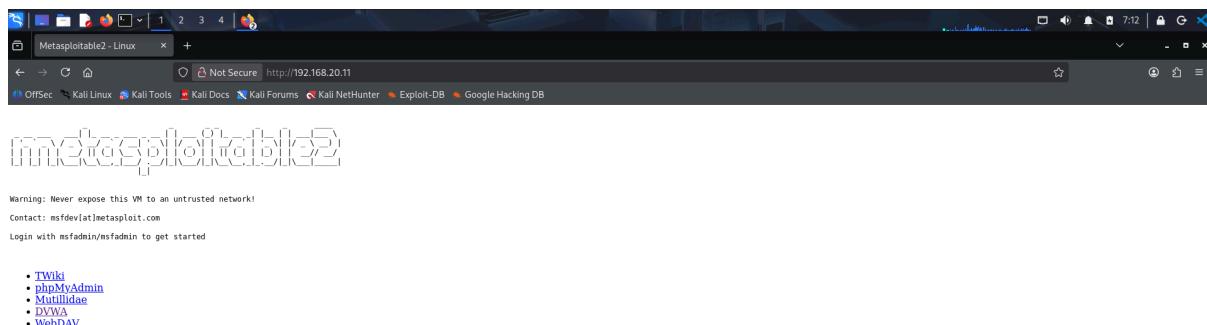
## 2. Test di Accessibilità Pre-Regola

Prima di implementare la regola di blocco, sono stati eseguiti dei test dalla macchina Kali Linux per confermare la connettività e l'accessibilità al servizio web sulla macchina Metasploitable (IP 192.168.20.11).

### A. Accesso al Server Web

È stato tentato l'accesso all'indirizzo IP di Metasploitable dalla macchina Kali Linux.

- **Risultato:** L'accesso alla pagina web all'indirizzo <http://192.168.20.11> ha avuto successo, mostrando la pagina di benvenuto di Metasploitable .



### B. Test di Connettività (Ping)

È stato eseguito un comando ping dalla macchina Kali Linux verso l'IP di Metasploitable per verificare la connettività ICMP.

- **Comando:** ping 192.168.20.11.
- **Risultato:** Il ping ha avuto successo, con 11 pacchetti trasmessi e 11 ricevuti .

A screenshot of a terminal window titled 'kali@kali: ~'. The user has run the command 'ping 192.168.20.11'. The terminal output shows 11 packets transmitted, 11 received, with 0% packet loss and a round-trip time of 10017ms. The output also includes statistics for the ping, such as rtt min/avg/max/mdev values.

### 3. Applicazione della Regola Firewall (LAN Interface)

L'obiettivo era bloccare l'accesso al servizio web (porta 80) di Metasploitable (192.168.20.11) dalla macchina Kali (192.168.50.151). Poiché il traffico ha origine dalla rete **LAN** (Kali), la regola è stata applicata sull'interfaccia **LAN** del firewall.

La regola creata è la seguente :

Azione	Protocollo	Sorgente	Porta Sorgente	Destinazione	Porta Destinazione	Descrizione
<b>Blocca</b>	IPv4 TCP	192.168.50.151 (Kali IP)	*	192.168.20.11 (Meta IP)	<b>80 (HTTP)</b>	Blocco mirato del traffico

- **Azione (Action): Blocca (Block).**
- **Interfaccia (Interface): LAN.**
- **Protocollo (Protocol): IPv4 TCP.**
- **Sorgente (Source):** È stato specificato l'indirizzo IP esatto della macchina Kali Linux: **192.168.50.151**.
- **Destinazione (Destination):** È stato specificato l'indirizzo IP di Metasploitable: **192.168.20.11**.
- **Porta Destinazione (Destination Port Range): 80 (HTTP),** la porta del servizio web DVWA.

Questa regola è stata posizionata in modo da precedere la regola di default **Default allow LAN to any rule** per assicurarne l'efficacia.

The screenshots show the pfSense Firewall Rules configuration for three different interfaces:

- LAN Interface:** Shows a single rule blocking traffic from 192.168.50.151 (Kali IP) to port 80 (HTTP) on the LAN interface.
- WAN Interface:** Shows a series of rules including an anti-lockout rule, a default allow rule for LAN to any rule, and a default allow rule for LAN IPv6 to any rule.
- OPT1 Interface:** Shows no rules defined for this interface.

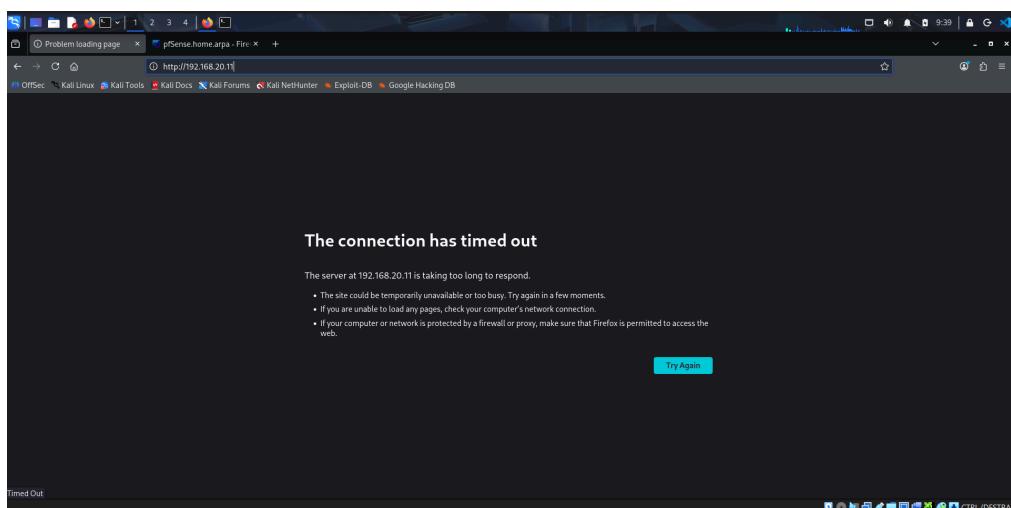
## 4. Test Post-Regola (Verifica del Blocco)

Dopo aver applicato e salvato la regola sul firewall, sono stati eseguiti nuovamente i test per confermare che l'accesso fosse bloccato, ma la connettività di base fosse mantenuta.

### A. Accesso al Server Web (DVWA)

È stato ritentato l'accesso alla pagina web DVWA (porta 80) dalla macchina Kali.

- **Risultato:** L'accesso al sito <http://192.168.20.11> è fallito. Il browser ha restituito un errore di "The connection has timed out" (Timeout della connessione). Ciò conferma che il traffico TCP verso la porta 80 è stato interrotto dalla regola.



### B. Test di Connettività (Ping)

È stato eseguito nuovamente il comando ping dalla macchina Kali Linux verso l'IP di Metasploitable.

- **Risultato:** Il ping ha continuato a funzionare normalmente. Questo conferma che il blocco è stato applicato in modo preciso solo al protocollo **TCP** (porta 80), lasciando inalterato il protocollo **ICMP** (Ping).

```
kali@kali: ~
Session Actions Edit View Help
[(kali㉿kali)-~]
$ ping 192.168.20.11
PING 192.168.20.11 (192.168.20.11) 56(84) bytes of data.
64 bytes from 192.168.20.11: icmp_seq=1 ttl=63 time=53.3 ms
64 bytes from 192.168.20.11: icmp_seq=2 ttl=63 time=2.63 ms
64 bytes from 192.168.20.11: icmp_seq=3 ttl=63 time=4.35 ms
64 bytes from 192.168.20.11: icmp_seq=4 ttl=63 time=2.52 ms
64 bytes from 192.168.20.11: icmp_seq=5 ttl=63 time=11.7 ms
64 bytes from 192.168.20.11: icmp_seq=6 ttl=63 time=13.3 ms
^C
--- 192.168.20.11 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5011ms
rtt min/avg/max/mdev = 2.520/14.632/53.291/17.801 ms
[(kali㉿kali)-~]
$
```