

# Report configurazione pfSense+kali+metasploit+DVWA

## 1. Configurazione delle reti su pfSense

- Abbiamo avviato pfSense e aperto il menu console.
- Dal menu delle opzioni, abbiamo selezionato l'opzione 2 – Assign Interfaces.
- È stata aggiunta una nuova interfaccia OPT1, collegata a una seconda rete interna di VirtualBox.
- Le interfacce risultano configurate così:
  1. LAN (192.168.50.1/24) → rete "kalinet"
  2. OPT1 (192.168.20.1/24) → rete "intnet"
  3. WAN → collegata al bridge per internet

## 2. Configurazione indirizzi IP

Kali Linux

- Collegata alla rete kalinet (LAN).
- Ha ricevuto l'IP 192.168.50.200 tramite DHCP di pfSense.
- Kali può pingare pfSense (192.168.50.1)

Metasploitable / DVWA

- Collegata alla rete intnet (OPT1).
- Abbiamo assegnato manualmente l'IP:
- 192.168.20.2/24
- gateway 192.168.20.1 (pfSense OPT1)
- Abbiamo abilitato il DHCP solo se richiesto, ma l'IP è stato configurato manualmente.
- Metasploitable può pingare pfSense (192.168.20.1).

## 3. Test di connettività

- Kali → Metasploitable: PING OK
- Kali → pfSense LAN: PING OK
- Kali → DVWA (pagina web): OK prima della regola
- Obiettivo: Kali deve pingare la macchina Meta, ma non deve accedere alla pagina DVWA.

## 4. Creazione regola firewall su pfSense

Regola creata:

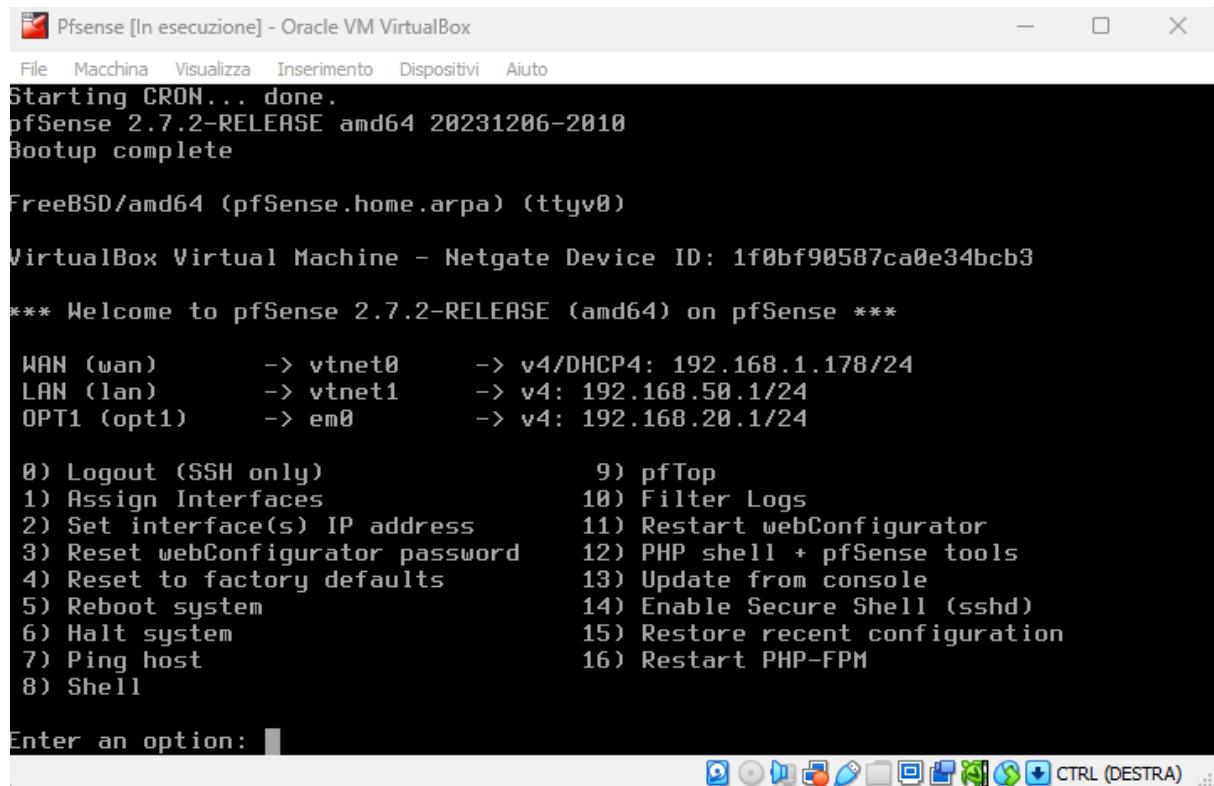
- Action: Block
- Protocol: TCP
- Source: 192.168.50.0/24 (rete Kali)

- Destination: 192.168.20.2 (Metasploitable)
- Destination Port: 80 (HTTP)
- Descrizione: “Blocca Kali da accedere a DVWA”

## Risultato finale

- Kali continua a pingare Metasploitable (ICMP permesso).
- Kali non può più accedere alla pagina DVWA su http://192.168.20.2
- La regola funziona perché blocca solo HTTP, non ICMP.

## Screenshot



Pfsense [In esecuzione] - Oracle VM 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: 1f0bf90587ca0e34bcb3

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

WAN (wan) -> vtnet0 -> v4/DHCP4: 192.168.1.178/24  
LAN (lan) -> vtnet1 -> 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  
8) Shell

Enter an option: [ ]

Icons at the bottom: Home, Help, Log Out, Filter, Log, Web Config, PHP Shell, Update, Restore, FPM, CTRL (DESTRA), ...

