

Report sulla Configurazione di un Ambiente di Test con pfSense come Switch Logico

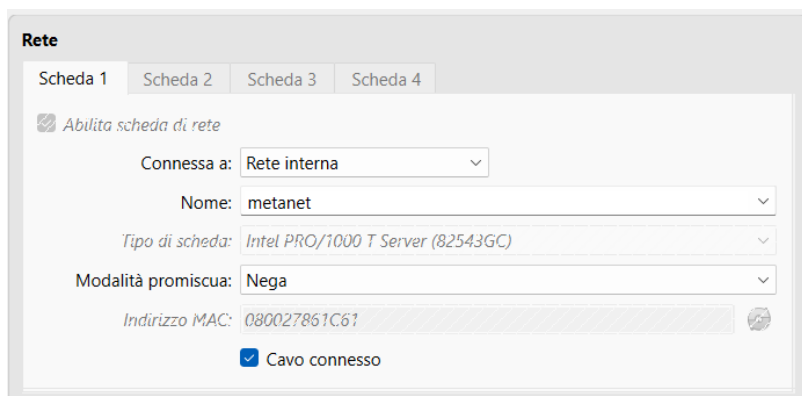
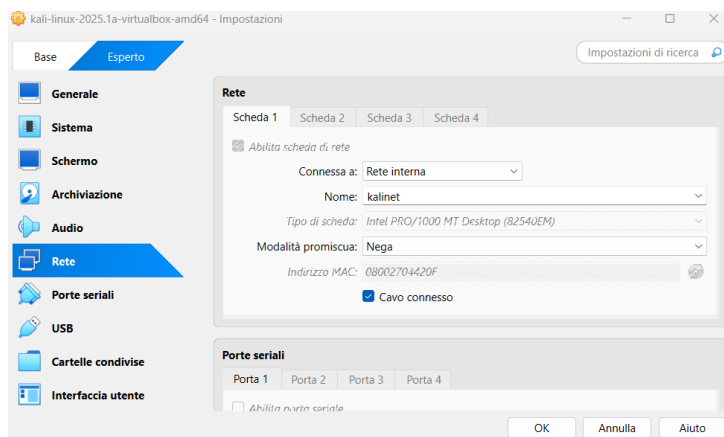
Introduzione

Il presente report descrive la configurazione di un ambiente di test di sicurezza informatica utilizzando VirtualBox e tre macchine virtuali: pfSense, Kali Linux e Metasploitable. L'obiettivo principale è configurare pfSense in modo da fungere da router/firewall interconnettendo due reti logiche distinte su cui risiedono Kali Linux e Metasploitable, e implementare una regola firewall per bloccare l'accesso a DVWA (Damn Vulnerable Web Application) ospitata su Metasploitable dalla macchina Kali Linux.

Architettura di Rete Virtuale

L'ambiente di test è stato realizzato utilizzando reti interne di VirtualBox per isolare le macchine virtuali e simulare scenari di rete reali. Sono state create le seguenti reti interne:

- **kalinet:** Rete interna dedicata alla macchina Kali Linux.
- **metanet:** Rete interna dedicata alla macchina Metasploitable.



La macchina virtuale pfSense è stata configurata con tre interfacce di rete virtuali:

- **WAN (Scheda Bridge):** Connessa alla rete fisica dell'host per l'accesso iniziale all'interfaccia web di pfSense e per eventuali aggiornamenti.
- **LAN (Rete Interna: kalinet):**

Interfaccia connessa alla rete interna su cui risiede Kali Linux.

- **OPT1 (Rete Interna: metanet):** Interfaccia connessa alla rete interna su cui risiede Metasploitable, per semplicità verrà mostrata solamente la scheda interna di kali.

In questa configurazione, pfSense agisce come un router che interconnette le due reti interne (kalinet e metanet), gestendo il traffico tra di esse e applicando le regole firewall definite. Dal punto di vista logico, pfSense svolge il ruolo di uno switch di livello 3 (router) che segmenta le due reti.

Configurazione degli Indirizzi IP Tramite pfSense

pfSense è stato configurato per gestire l'assegnazione degli indirizzi IP alle macchine virtuali Kali Linux e Metasploitable attraverso il servizio DHCP su ciascuna delle reti interne.

1. Configurazione dell'Interfaccia per kalinet:

- L'interfaccia di pfSense connessa a kalinet (denominata "LAN" durante la configurazione iniziale o successivamente rinominata) è stata configurata con un indirizzo IP statico all'interno della sottorete desiderata 192.168.10.1/24.

```

The IPv4 OPT1 address has been set to 192.168.50.1/24
You can now access the webConfigurator by opening the following URL in your web browser:
    http://192.168.50.1/

Press <ENTER> to continue.
VirtualBox Virtual Machine - Netgate Device ID: 8dacb7973e63f1d3ec04

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

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.109.43/24
LAN (lan)      -> em1      -> v4: 192.168.10.1/24
OPT1 (opt1)    -> em2      -> v4: 192.168.50.1/24

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 (ssh)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option:

```

Configurazione dell'Interfaccia per metanet:

- La terza interfaccia di pfSense connessa a metanet (denominata "OPT1" o rinominata in modo appropriato, ad esempio "METANET_INT") è stata configurata con un indirizzo IP statico in una sottorete diversa 192.168.50.1/24.

Creazione della Regola Firewall per Bloccare l'Accesso a DVWA

L'obiettivo è impedire alla macchina Kali Linux (IP: 192.168.10.10), situata sulla rete kalinet, di accedere all'applicazione DVWA ospitata su Metasploitable (IP: 192.168.50.101), situata sulla rete metanet. Per fare ciò, è stata creata una regola firewall su pfSense.

1. Navigazione alla Sezione Firewall Rules:

- Nell'interfaccia web di pfSense, è stato navigato su "Firewall" -> "Rules".
- È stata selezionata la scheda corrispondente all'interfaccia da cui proviene il traffico che si desidera bloccare, ovvero l'interfaccia connessa alla rete di Kali Linux ("LAN").

2. Creazione della Regola di Blocco:

- È stata aggiunta una nuova regola con le seguenti specifiche:
 - **Action:** Block (Blocca il traffico corrispondente alla regola).
 - **Interface:** LAN (Applica la regola al traffico in entrata sull'interfaccia LAN di pfSense, ovvero il traffico proveniente dalla rete kalinet).
 - **Protocol:** TCP (DVWA comunica tipicamente tramite il protocollo TCP sulla porta 80 (HTTP) o 443 (HTTPS)).
 - **Source:**
 - **Type:** Single host or alias
 - **Address:** Indirizzo IP della macchina Kali Linux (192.168.10.10).

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: OPT1
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 Network 192.168.10.10 / 24

[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:**
 - **Type:** Single host or alias
 - **Address:** Indirizzo IP della macchina Metasploitable (192.168.50.101).
 - **Port:** web (Alias predefinito che include le porte 80 e 443). In alternativa, si sarebbe potuta specificare la porta 80.
- **Description:** Blocca accesso DVWA da Kali a Metasploitable (o una descrizione simile).

Destination

Destination ☐ Invert match Address or Alias 192.168.50.101

Destination Port Range HTTP (80) From Custom To Custom

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

Extra Options

Log ☒ Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description block DVWA from Kali
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options [Display Advanced](#)

Rule Information

Tracking ID	1744974922
Created	4/18/25 11:15:22 by admin@192.168.10.10 (Local Database)
Updated	4/18/25 11:18:05 by admin@192.168.10.10 (Local Database)

[Save](#)

- **Log:** (Opzionale)
Abilitato per registrare i pacchetti bloccati da questa regola per scopi di verifica.

3. Applicazione delle Modifiche:

- Dopo aver configurato la regola, è stato fondamentale

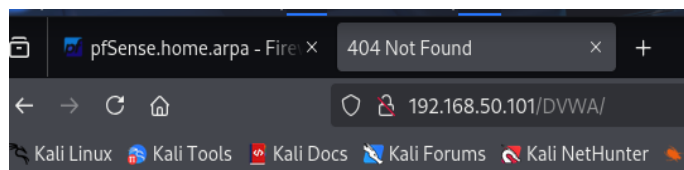
fare clic sul pulsante "Save" e successivamente su "Apply Changes" per rendere effettiva la regola sul firewall di pfSense.

Verifica della Regola Firewall

Per verificare l'efficacia della regola firewall, sono stati eseguiti i seguenti test dalla macchina Kali Linux (IP: 192.168.10.10):

1. Tentativo di Accesso Web a DVWA:

- È stato aperto un browser web su Kali Linux e si è tentato di accedere all'indirizzo IP di Metasploitable seguito dal percorso di DVWA (<http://192.168.50.101/dvwa/>). Il tentativo di connessione è fallito, indicando che il firewall di pfSense ha bloccato la richiesta.



Not Found

The requested URL /DVWA/ was not found on this server.

Apache/2.2.8 (Ubuntu) DAV/2 Server at 192.168.50.101 Port 80

```
(kali@kali)~$ nmap 192.168.50.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-18 07:48 EDT
Nmap scan report for 192.168.50.101
Host is up (0.71s 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

Nmap done: 1 IP address (1 host up) scanned in 2.32 seconds
```

2. Scansione delle Porte con Nmap:

- È stato utilizzato lo strumento nmap da Kali Linux per scansionare le porte TCP della macchina Metasploitable, in particolare la porta 80. Il risultato della scansione ha mostrato che la porta 80 era "closed", indicando che il firewall stava bloccando le connessioni a quella porta.

Conclusioni

La configurazione descritta ha permesso di isolare le macchine Kali Linux e Metasploitable su due reti logiche distinte (kalinet e metanet), interconnesse e protette dal firewall pfSense. La regola firewall implementata sull'interfaccia LAN di pfSense ha bloccato con successo il traffico proveniente da Kali Linux (IP: 192.168.10.10) e diretto verso l'applicazione DVWA ospitata su Metasploitable (IP: 192.168.50.101) sulla porta web, dimostrando la capacità di pfSense di segmentare la rete e applicare politiche di sicurezza specifiche basate sugli indirizzi IP delle macchine.