

Test settimanale S3L5

Creazione pratica di una regola Firewall

PfSense è una delle soluzioni firewall open-source più apprezzate per la sua flessibilità, affidabilità e la vasta gamma di funzionalità che offre, fornisce un'interfaccia web intuitiva per la gestione delle configurazioni di rete.

In questa relazione, mi concentrerò sulla creazione di una regola firewall utilizzando pfSense in un ambiente di test che comprende una macchina Kali Linux e una macchina Metasploitable. Kali Linux, una distribuzione Linux dedicata al penetration testing e alla sicurezza informatica, sarà utilizzata come macchina per simulare attacchi o test di penetrazione. Metasploitable, invece, è una macchina virtuale intenzionalmente vulnerabile progettata per fornire un ambiente sicuro in cui apprendere e sperimentare tecniche di attacco e difesa.

Il mio obiettivo è dimostrare come configurare una regola firewall su pfSense per bloccare specifici tipi di traffico, in questo caso, il traffico HTTP tra Kali Linux e Metasploitable. Questo esercizio non solo mi aiuta a comprendere i concetti fondamentali di configurazione del firewall, ma fornisce anche una base pratica per sviluppare competenze essenziali nella gestione della sicurezza di rete. L'ambiente di test mi permette di esplorare e comprendere l'impatto delle regole firewall senza compromettere la sicurezza di una rete di produzione.

Procedura di Configurazione:

Prima di accedere all'interfaccia web di pfSense, è essenziale configurare correttamente l'indirizzo IP di pfSense stesso. Questo passo assicura che pfSense sia sulla stessa rete delle altre macchine ma con un indirizzo IP univoco.

Dopodiché bisogna accedere all'interfaccia web di pfSense tramite un browser su Kali Linux utilizzando l'indirizzo IP dell'interfaccia LAN di pfSense.

Bisogna selezionare FIREWALL>RULES nel menu principale dell'interfaccia del web.

di conseguenza creare di una nuova Regola

Cliccando su ADD (é indifferente il verso della freccia) nella schedan dell'interfaccia appropriata, in questo caso é LAN

APPARIRÁ LA SCHERMATA DELLA CONFIGURAZIONE DELLA REGOLA





→ ↻ 🏠 192.168.2.6/firewall_rules_edit.php?if=lan ☆

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

pfsense
COMMUNITY EDITION

☰

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Firewall / Rules / Edit    

Edit Firewall Rule

Action	Pass
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	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.
Interface	LAN
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

- Action: Impostare su "Block" per bloccare il traffico.
- Interface: Selezionare l'interfaccia corretta (es. LAN).
- Protocol: Selezionare TCP.
- Source: Inserire l'indirizzo IP di Kali Linux.
- Destination: Inserire l'indirizzo IP di Metasploitable****.
- Destination Port Range: Impostare su 80 per bloccare il traffico HTTP.

**** Per accedere all'indirizzo IP di Metasploitable bisogna andare sulla macchina e avviarla con nome utente e password e poi scrivere "ifconfig"

```
Nmap done: 1 IP address (0 hosts up) scanned in 3.138 seconds
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:dc:bc:9c
          inet addr:192.168.129.24  Bcast:192.168.129.255  Mask:255.255.254.0
          inet6 addr: 2a02:a03f:664c:ca01:a00:27ff:fedc:bc9c/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fedc:bc9c/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:553 errors:0 dropped:0 overruns:0 frame:0
          TX packets:163 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:63230 (61.7 KB)  TX bytes:20951 (20.4 KB)
```

In questo caso é **192.168.129.24**

Dopodiché si passa al salvataggio e all'applicazione , cliccando su "SAVE" per salvare via regola e successivamente cliccare su "APPLY CHANGES" per applicare le modifiche

Non basta altro che metter alla prova la Regola verificandola

1.Test del Traffico:

- Bisogna Utilizzare Kali Linux per lanciare un test verso Metasploitable, utilizzando -nmap per verificare che il traffico HTTP sia bloccato.

```
(kali@kali)-[~]
$ nmap -p 80 [IP_di_Metasploitable] 192.168.2.6/firewall_rules.php?it=lan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-13 09:09 EST
Failed to resolve "[IP_di_Metasploitable]".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.12 seconds
```

```
(kali@kali)-[~]
$ ping 192.168.129.24
ping: connect: La rete non è raggiungibile
```

2. Risultati Attesi:

- Il traffico HTTP verso Metasploitable dovrebbe essere bloccato, confermando che la regola di pfSense è stata applicata correttamente.

In conclusione:

L'ambiente di test con Kali Linux e Metasploitable ha offerto un'opportunità sicura per sperimentare e imparare, senza il rischio di compromettere una rete di produzione. Questi strumenti e tecniche costituiscono la base su cui posso costruire ulteriori strategie

di sicurezza, adattandole alle esigenze specifiche di qualsiasi infrastruttura di rete con cui lavorerò in futuro.

In conclusione, la gestione efficace delle regole firewall non solo protegge le risorse di rete, ma migliora anche la mia capacità di garantire la sicurezza e l'integrità dei dati in un mondo sempre più interconnesso. Continuerò a esplorare e ad apprendere nuove tecniche per rimanere aggiornata sulle migliori pratiche di sicurezza informatica.