

In questa esercitazione ho lavorato alla configurazione di pfSense in un ambiente virtuale, con l'obiettivo di creare due reti interne separate e, alla fine, bloccare l'accesso a DVWA da parte della macchina Kali Linux.

L'esercizio sembrava semplice sulla carta, ma ha richiesto una serie di passaggi e diagnosi per far funzionare tutto correttamente.

1. Preparazione dell'ambiente

Per prima cosa ho importato la macchina pfSense tramite il file OVA fornito.

Successivamente ho sistemato le schede di rete su VirtualBox:

- La **WAN** l'ho lasciata in NAT, così pfSense può uscire su Internet.
- La **LAN** l'ho configurata come rete interna chiamata "laboratorio".
- Ho aggiunto una terza scheda, per creare la **LAN2**, impostandola su un'altra rete interna chiamata "laboratorio2".

Quando ho avviato pfSense, tuttavia, riconosceva solo due interfacce.

Per far comparire la terza ho dovuto entrare nel menu di pfSense e usare l'opzione *Assign Interfaces* per aggiungere manualmente l'interfaccia em2, che poi ho abilitato e rinominato come **LAN2** tramite la web GUI.

2. Configurazione delle reti interne

La LAN era già funzionante con l'indirizzo 192.168.50.1.

La nuova LAN2 l'ho configurata con IP **192.168.51.1/24**, come richiesto dall'architettura dell'esercizio.

A questo punto ho collegato Metasploitable alla rete "laboratorio2".

Però qui è arrivato il primo problema serio: Metasploitable accettava i comandi di configurazione della rete, ma al riavvio li perdeva completamente.

Il motivo è che questa distribuzione usa un vecchio sistema di configurazione della rete, per cui è necessario modificare direttamente il file:

/etc/network/interfaces

Inserendo manualmente indirizzo IP, netmask e gateway.

Dopo questa modifica e un riavvio, Metasploitable ha finalmente ottenuto l'indirizzo corretto: **192.168.51.101**.

3. Primo grande ostacolo: Metasploitable non pinga pfSense

Nonostante tutto fosse configurato bene, Metasploitable non riusciva a pingare pfSense. La cosa curiosa era che da pfSense *io riuscivo a pingare Metasploitable*, ma non il contrario.

Questa situazione mi ha fatto capire che:

- la rete fisica funzionava,
- l'indirizzamento era corretto,
- la macchina era raggiungibile...

...ma qualcosa bloccava il traffico in ingresso verso pfSense.

La causa era pfSense stesso: le nuove interfacce (OPT1/LAN2) non vengono gestite come la LAN principale. pfSense, per motivi di sicurezza, blocca automaticamente qualsiasi traffico entrante su interfacce aggiuntive finché non si aggiungono regole manuali.

Per risolvere il problema, ho creato una regola firewall su LAN2 che permettesse almeno il traffico ICMP (ping) verso l'indirizzo della LAN2 di pfSense.

Una volta applicata la regola corretta, Metasploitable ha finalmente iniziato a pingare pfSense senza problemi.

Questo è stato il passaggio chiave che ha sbloccato tutto.

4. Applicazione della regola firewall per bloccare DVWA

A questo punto l'ambiente aveva:

- Kali e Windows sulla rete 192.168.50.x
- Metasploitable sulla rete 192.168.51.x
- pfSense in mezzo a fare routing tra le due reti

Era quindi possibile passare alla parte finale dell'esercizio:

bloccare l'accesso di Kali alla DVWA su Metasploitable (porta 80).

Ho creato una regola sulla LAN (la rete di Kali) che blocca il traffico TCP proveniente dall'indirizzo 192.168.50.100 verso 192.168.51.101 sulla porta 80.

Prima di applicare la regola, ho verificato con nmap da Kali che la porta 80 fosse effettivamente aperta su Metasploitable.

Dopo aver applicato la regola, ho ripetuto il test e nmap riportava:

Host seems down.

0 hosts up.

Questo risultato indica che il traffico verso DVWA è completamente bloccato e persino invisibile da Kali.

L'obiettivo dell'esercitazione, quindi, è stato raggiunto.

5. Conclusioni

L'esercitazione mi ha permesso di:

- configurare pfSense con più interfacce,
- diagnosticare problemi di routing e firewalling,
- capire come pfSense gestisce il traffico su interfacce aggiuntive,
- configurare staticamente Metasploitable intervenendo nel file /etc/network/interfaces,
- creare e testare regole firewall mirate.

Le difficoltà principali sono state due:

1. **Metasploitable non applicava l'IP statico**, costringendomi a modificare manualmente il file di configurazione della rete.
2. **pfSense bloccava automaticamente tutto il traffico in ingresso su LAN2**, rendendo impossibile pingarlo finché non è stata creata una regola apposita.

Una volta superati questi ostacoli, l'ambiente ha funzionato come previsto e la regola per bloccare DVWA è risultata efficace.