Report Teorico esercitazione 3

Che cos'è un firewall

Un firewall è uno strumento molto importante per la sicurezza informatica. Può essere un programma oppure un dispositivo fisico e serve a proteggere un computer o una rete da accessi non autorizzati.

Il suo compito principale è controllare il traffico di rete, cioè i dati che entrano e che escono da una rete. In pratica, il firewall fa da "filtro" tra la rete interna e Internet, decidendo quali comunicazioni possono passare e quali devono essere bloccate, in base a regole stabilite in precedenza.

Componenti del firewall

Un firewall può essere composto da software, hardware oppure da entrambi. I suoi componenti principali sono:

- **Motore di controllo del traffico**
  È la parte più importante del firewall. Analizza i dati che passano attraverso la rete e decide se permettere o bloccare il traffico, seguendo le regole di sicurezza impostate.

- **Interfaccia di gestione**
  È lo strumento che permette agli amministratori di configurare il firewall e controllarne il funzionamento. Serve per impostare le regole e monitorare ciò che accade nella rete.

- **Database delle regole**
  È l'insieme delle regole di sicurezza memorizzate nel firewall. Il motore di controllo consulta queste regole per decidere cosa fare con ogni pacchetto di dati che arriva o che esce.

Obiettivo dell'esercitazione

L'obiettivo di questa esercitazione di laboratorio è imparare come segmentare una rete e come configurare una regola di firewall per impedire a una macchina non autorizzata, come **Kali Linux,** di eseguire **scansioni** verso una macchina **vulnerabile**, come **Metasploitable o DVWA.**

In teoria, questo risultato si ottiene separando le macchine in **sottoreti** diverse e creando una regola di blocco sul firewall, in modo che il traffico venga controllato e, se necessario, bloccato.

Per iniziare bisogna rispettare il requisito della **segmentazione** della rete, ovvero l'ambiente dovrebbe essere organizzato utilizzando tre interfacce di rete. In questo modo, la macchina attaccante (**Kali**) e la macchina bersaglio (**Metasploitable**) si trovano su **reti separate** e non possono comunicare direttamente tra loro.
Di conseguenza, **tutto il traffico tra le due macchine deve passare attraverso il firewall PfSense**, che ha il compito di **analizzare il traffico e applicare le regole di sicurezza.***
Dal punto di vista teorico, la macchina virtuale PfSense dovrebbe essere configurata in VirtualBox con tre schede di rete:

- **Interfaccia 1**: collegato in modalità **Bridge**, utilizzato come interfaccia **WAN** per la connessione verso l'esterno.
- **Interfaccia 2**: collegato a una rete interna chiamata ***kalinet***, che rappresenta la **LAN** su cui si trova **Kali Linux.**
- **Interfaccia 3**: collegato a una rete interna chiamata ***metanet***, che rappresenta la rete della **macchina bersaglio .**

Le macchine virtuali di Kali Linux e Metasploitable, sempre in teoria, dovrebbero essere configurate ciascuna con una sola scheda di rete:

- **Kali Linux collegata alla rete interna *kalinet*.**
- **Metasploitable collegata alla rete interna *metanet*.**

In questo modo, la comunicazione tra attaccante e bersaglio avverrebbe solo passando dal firewall, permettendo di applicare una policy che blocchi le scansioni non autorizzate.

Assegnazione delle interfacce di rete

Se impostato bene, il sistema PfSense dovrebbe riconoscere una nuova scheda di rete virtuale, *vtnet2* identificata come **OPT1**.
Questa scheda dovrebbe essere assegnata all'interfaccia chiamata **Rete Bersaglio**, che rappresenta la rete in cui si trova la macchina Metasploitable.

L'assegnazione corretta di questa interfaccia permetterebbe di separare la rete della macchina **Kali** dalla rete della **macchina bersaglio**, garantendo la segmentazione della rete.+

Quindi ipoteticamente avremo :

- **WAN (Vnet0) —> Rete Internet**
- **LAN (Vnet1) —> Rete attaccante**
- **OPT1 Vnet2 —> Rete vittima**

Per consentire la comunicazione controllata tra le diverse reti, le interfacce dovrebbero essere configurate con indirizzi IPv4 statici appartenenti a sottoreti differenti.

Esempio configurazione :

- **Interfaccia LAN (gateway della rete Kali)**: `192.168.30.1/24`
- **Interfaccia Rete Bersaglio (gateway Metasploitable)**: `192.168.60.1/24`

Questa configurazione permetterebbe di mantenere la rete Kali (`192.168.30.x`) separata dalla Rete Bersaglio (`192.168.60.x`), obbligando il traffico a passare attraverso il firewall PfSense.

Dopo aver assegnato la porta *vtnet2* all'interfaccia **Rete Bersaglio**, dovrebbe essere impostato un indirizzo IPv4 statico pari a **192.168.60.1**.

In questo modo, il router PfSense potrebbe instradare il traffico tra la sottorete **192.168.30.x** (LAN) e la sottorete **192.168.60.x** (Rete Bersaglio).

Regola firewall

Per impedire alla macchina Kali di accedere al servizio web DVWA ospitato sulla macchina Metasploitable, dovrebbe essere creata una regola di firewall sull'interfaccia **LAN**.

La regola verrebbe applicata sull'interfaccia LAN perché il firewall controllerebbe il traffico nel punto in cui ha origine, permettendo di bloccare le connessioni non autorizzate prima che raggiungano la Rete Bersaglio.

La regola di filtraggio dovrebbe avere le seguenti caratteristiche:

- **Azione/Action**: Block
- **Interfaccia/Interface**: LAN (traffico proveniente dalla macchina Kali)
- **Protocollo/Protocol**: TCP
- **Sorgente/Source**: `192.168.30.10` (indirizzo IP della macchina Kali)
- **Destinazione /Destination** : `192.168.60.20` (indirizzo IP della Metasploitable)
- **Porta di destinazione/Destination Port**: 80 (porta utilizzata dal servizio web HTTP)

Questa configurazione permetterebbe di colpire esclusivamente il traffico web proveniente dalla macchina Kali, senza interferire con altri tipi di comunicazione.
Tecnicamente bloccando il traffico diretto alla porta TCP 80, la regola dovrebbe impedirebbe l'avvio della connessione HTTP.
Se la macchina Kali tentasse di collegarsi al servizio web o di avviare una scansione, invierebbe un pacchetto iniziale di connessione. Il firewall intercetterebbe questo pacchetto e lo scarterebbe, causando il fallimento della connessione e il conseguente timeout.