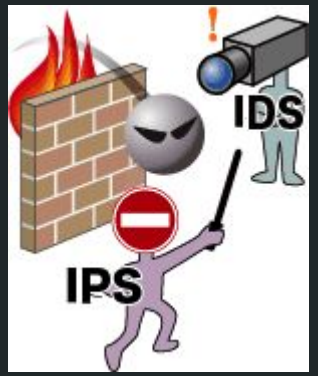
Sistemas de Detección de Intrusos



Alicia Vílchez Ceballos
Antonio Campoy Torrecillas

Sistemas de Detección de Intrusos

-¿Qué es un IDS?

-Tipos de IDS

-¿Por qué instalar un IDS?

-SURICATA

¿Qué es un IDS?

Un Sistema de Detección de Intrusos es una herramienta de seguridad que se emplea para detectar y monitorizar accesos no autorizados a un dispositivo o red.

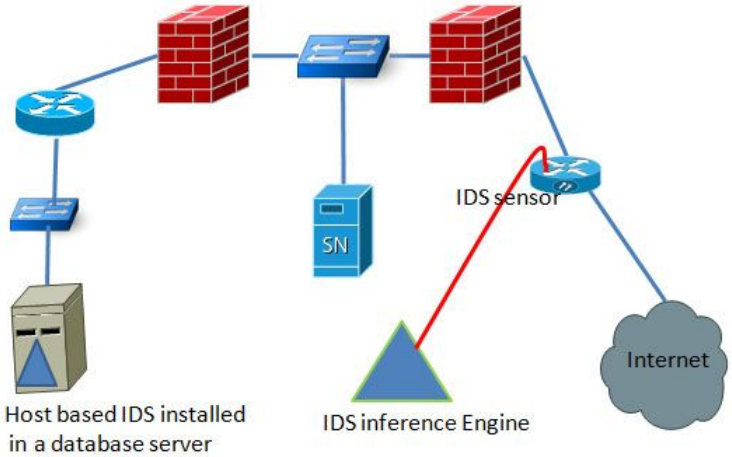
TIPOS DE IDS

Clasificados por su alcance de protección:

-Host IDS

-Net IDS

-Distributed IDS



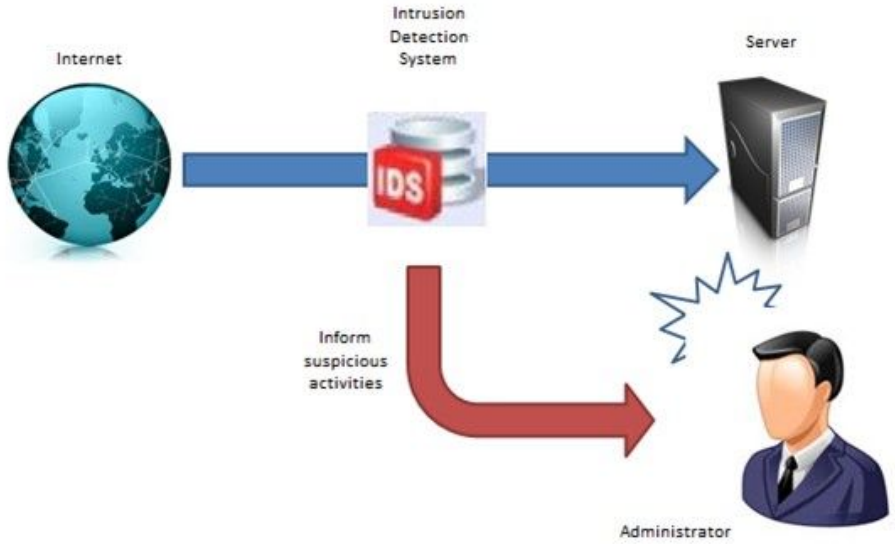
Network based IDS analyzing all incoming traffic outside the Perimeter network

TIPOS DE IDS

Clasificados por su tipo de respuesta:

-Pasivos

-Activos



¿Por qué instalar un IDS?

- Para una mejora en la prevención contra los ataques informáticos
- Por detectar las acciones previas a un ataque
- Para recolectar información acerca del ataque producido

SURICATA

Hablemos de Suricata....

Suricata es un Sistema de Detección de Intrusos de código abierto. El proyecto empezó a finales de 2009 y sigue en marcha. Es un IDS del tipo NIDS.
El motor de suricata analiza el tráfico en tiempo real, también incorpora IPS y procesamiento de paquetes offline.

Características de Suricata

- Multi-Threaded Processing
- Automatic Protocol Detection
- Performance Statistics
- HTTP Log Module
- Fast Log Module

¿Cómo funciona?