# INTRUSION DETECTION SYSTEM

Londero, Camila Soledad - Vargas, Maria Micaela

# Conceptos básicos

1. Intrusión
2. Detección de intrusos
3. Falso positivo/negativo
4. Firewall
5. Firmas / Bases de datos de firmas
6. Log

# ¿Qué son los IDS?

# Ventajas y desventajas

- Ver lo que está sucediendo en la red en tiempo real
- Reconocer modificación en los documentos
- Automatizar los patrones de búsqueda en los paquetes de datos enviados a través de la red.

- No están diseñadas para prevenir o detener los ataques que detectan.
- Falsos positivos
- Falsos negativos

# Características de un IDS

- Ligero
- Adaptable
- Confiable
- Robusto
- Reconocer un ataque

# Funcionamiento

## Monitoreo de datos

El monitor de datos tiene la tarea de recoger y hacer un primer filtro a los datos necesarios para filtrar intrusos.

## Análisis

Este debe editar y evaluar la información obtenida en tiempo real, de lo contrario no sería posible evitar los ataques a tiempo.

## Informe de resultados

Informa al administrador de la red si encontró un ataque o un comportamiento sospechoso del sistema

# Técnicas usadas por los IDS

1. Almacenamiento de paquetes bajo sospecha de ataque

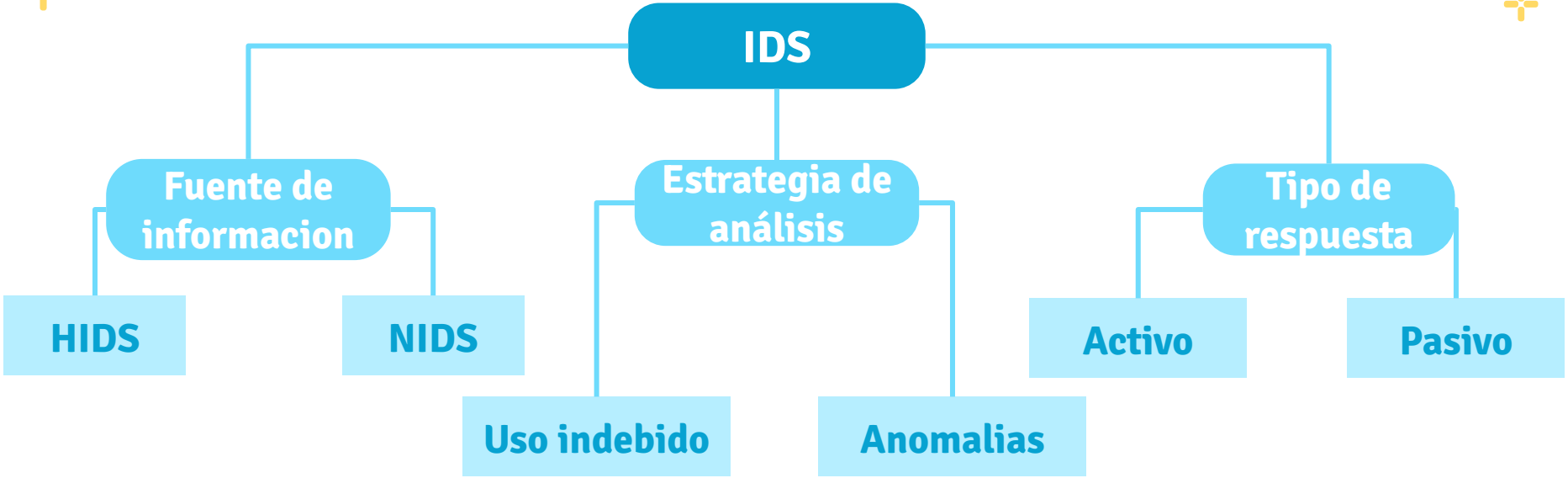
5. Registro de la intrusión en una base de datos

2. Verificación de la configuración de dispositivos externos

3. Envío de una señal de alerta

4. Alerta mediante correo electrónico

# Tipos de IDS

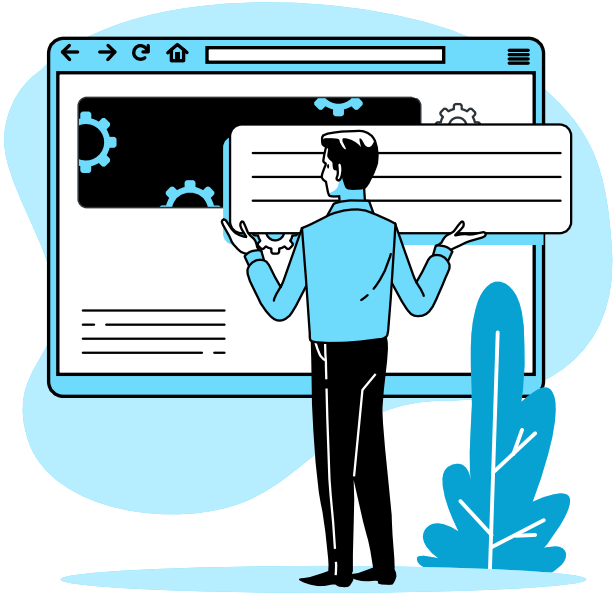

IDS
Fuente de informacion
Estrategia de análisis
Tipo de respuesta
HIDS
NIDS
Uso indebido
Anomalias
Activo
Pasivo

# Acciones a tomar ante una intrusión

Una vez que nuestro IDS detecta una intrusión, hay dos tipos de respuestas:

- Respuestas Activas
  - Contenemos el ataque
  - Eliminamos las posibles causas
  - Determinamos el alcance del ataque
  - Aseguramos la continuidad del servicio

- Respuestas Pasivas



# Ejemplos de IDS

Snort


OSSEC

Suricata


Security Onion

# Ejemplo de detecciones en IDS

# ¡Gracias!