Instituto Tecnológico de Cancún

Ingeniería en Sistemas Computacionales

Fundamentos de Telecomunicaciones

Tarea: Investigación IDS-IPS

Docente: Ing. Ismael Jiménez Sánchez

Alumno: Uc Uc César Enrique

## Detección de intrusos (IDS)

Un IDS es un dispositivo de hardware o una aplicación de software que utiliza firmas de intrusión conocidas para detectar y analizar el tráfico de red entrante y saliente en busca de actividades anormales.

Esto se hace a través de:

- Comparaciones de archivos del sistema contra firmas de malware.
- Procesos de escaneo que detectan signos de patrones maliciosos.
- Monitoreo del comportamiento del usuario para detectar intenciones maliciosas.
- Monitoreo de configuraciones y configuraciones del sistema.
- Monitoreo del tráfico de red entrante y saliente de los dispositivos

Al detectar una violación de la política de seguridad, un virus o un error de configuración, un IDS puede expulsar a un usuario infractor de la red y enviar una alerta al personal de seguridad.

A pesar de sus beneficios, incluido el análisis en profundidad del tráfico de red y la detección de ataques, un IDS tiene inconvenientes inherentes. Debido a que utiliza firmas de intrusión previamente conocidas para localizar ataques, las amenazas recientemente descubiertas 0 Day, pueden permanecer sin ser detectadas.

Además, un IDS solo detecta ataques continuos, no ataques entrantes. Para bloquearlos, se requiere un sistema de prevención de intrusiones.

## Prevención de intrusiones (IPS)

Un IPS complementa una configuración de IDS mediante la inspección proactiva del tráfico entrante de un sistema para eliminar las solicitudes maliciosas. Una configuración típica de IPS utiliza firewalls de aplicaciones web y soluciones de filtrado de tráfico para proteger las aplicaciones.

Un IPS evita ataques al descartar paquetes maliciosos, bloquear IP's ofensivas y alertar al personal de seguridad de posibles amenazas. Este sistema generalmente usa una base de datos preexistente para el reconocimiento de firmas y puede programarse para reconocer ataques basados en el tráfico y anomalías de comportamiento.

Si bien es eficaz para bloquear los vectores de ataque conocidos, algunos sistemas IPS tienen limitaciones. Estos son comúnmente causados por una dependencia excesiva de reglas predefinidas, haciéndolos susceptibles a falsos positivos.