Instituto Tecnológico de Cancún

Fundamentos de Telecomunicaciones

SIEM, IPS e IDS

Prof. Ismael Jiménez Sánchez

Alumno(a). Laury del Rosario Mex Martin

Ciclo 2020-B

Fecha de Entrega: 3 de Diciembre de 2020

IDS (Sistema de detección de intrusiones) es una herramienta que monitorizan el tráfico entrante y que ayuda a los administradores de redes a detectar accesos no autorizados a la red o a un ordenador, emite una alerta ante una actividad sospechosa, los accesos pueden ser ataques maliciosos realizado por usuarios o por herramientas automáticas. La alerta que emite son anticipatorias de esas posible ataques de intrusión, pero no van a tratar de detener la intrusión.

IPS (Sistema de prevención de intrusiones) es una herramienta para proteger la res u ordenadores de ataques y de intrusiones, hace un análisis en tiempo real de la red, las conexiones y protocolos, para determinar si hay una anomalía o comportamiento sospecho dentro de la red para que implemente políticas que se basan en el contenido del trafico que monitorio, lanza alarmas, puede descartar paquetes y hasta desconectar conexiones que pueden afectar en la red.

Existen proveedores que ofrecen ambos servicios por lo cual los llaman IPS/ISD, que se integran mayormente con Contrafuegos y UTM (Gestión Unificada de Amenazas) que lo que hacen es controlar la red en base a las reglas de protocolos.

SIEM (Sistema de gestión de eventos e información de seguridad) es una herramienta hibrida que engloba dos grandes conceptos SEM (Gestión de eventos de seguridad) este monitoriza el sistema en tiempo real y alerta al detectar anomalías o ataques y el SIM (Gestión de información de seguridad) que este almacena la información recolectada del SEM para analizar y llevar acabo reportes de los resultados del trafico monitoreado . Que en pocas palabras podemos decir que SIEM nos proporciona un análisis y recuperación de los eventos de seguridad.