INSTITUTO TECNOLOGICO DE CANCÚN

INGENIERIA EN SISTEMAS COMPUTACIONALES

FUNDAMENTOS DE TELECOMUICACIONES

INVESTIGAR IDS/IPS

Peraza Soberanis Gabriel Alfredo

Sistemas de detección y prevención IDS e IPS: ¿Para qué sirven?

Sirven como herramientas que se usan para monitorizar y detectar intrusiones en los equipos o en la red de la empresa son diferentes entre sí.

IDS

IDS *(Intrusion Detection System)* o Sistema de Detección de Intrusiones: es una aplicación usada para detectar accesos no autorizados a un ordenador o a una red, es decir, son sistemas que monitorizan el tráfico entrante y lo cotejan con una base de datos actualizada de firmas de ataque conocidas. Ante cualquier actividad sospechosa, emiten una alerta a los administradores del sistema quienes han de tomar las medidas oportunas. Estos accesos pueden ser ataques esporádicos realizados por usuarios malintencionados o repetidos cada cierto tiempo, lanzados con herramientas automáticas. Estos sistemas sólo detectan los accesos sospechosos emitiendo alertas anticipatorias de posibles intrusiones, pero no tratan de mitigar la intrusión. Su actuación es reactiva.

IPS

IPS *(Intrusion Prevention System)* o Sistema de Prevención de Intrusiones: es un software que se utiliza para proteger a los sistemas de ataques e intrusiones. Su actuación es preventiva. Estos sistemas llevan a cabo un análisis en tiempo real de las conexiones y los protocolos para determinar si se está produciendo o se va a producir un incidente, defensa frente a múltiples ataques, como intrusiones, ataques de fuerza bruta, infecciones por malware o modificaciones del sistema de archivos, entre otros identificando ataques según patrones, anomalías o comportamientos sospechosos y permitiendo el control de acceso a la red, implementando políticas que se basan en el contenido del tráfico monitorizado, es decir, el IPS además de lanzar alarmas, puede descartar paquetes y desconectar conexiones. Y aumento de la eficiencia y la seguridad de la prevención de intrusiones o ataques a la red.

Muchos proveedores ofrecen productos mixtos, llamándolos IPS/IDS, integrándose frecuentemente con cortafuegos y UTM (en inglés Unified Threat Management o Gestión Unificada de Amenazas) que controlan el acceso en función de reglas sobre protocolos y sobre el destino u origen del tráfico.

En resumen

La principal ventaja de un **sistema IDS** es que permite **ver lo que está sucediendo en la red en tiempo real** en base a la información recopilada, reconocer modificaciones en los documentos y automatizar los patrones de búsqueda en los paquetes de datos enviados a través de la red. Su principal desventaja es qué estas

herramientas, sobre todo en el caso de las de tipo pasivo, no es están diseñadas para prevenir o detener los ataques que detecten.

El IPS es un software que se utiliza para **proteger a los sistemas de ataques** e intrusiones. Su actuación es preventiva. Estos sistemas llevan a cabo un análisis en tiempo real de las conexiones y los protocolos para determinar si se está produciendo o se va a producir un incidente, identificando ataques según patrones, anomalías o comportamientos sospechosos y permitiendo el control de acceso a la red, implementando políticas que **se basan en el contenido del tráfico monitorizado**, es decir, el IPS además de lanzar alarmas, puede descartar paquetes y desconectar conexiones.