Instituto Tecnológico de Cancún

Ingeniería en sistemas computacionales

Fundamentos de telecomunicación

“IDS/IPS”

Docente:

Ing. Ismael Jiménez Sánchez

Alumna:

Moen Ake Geraldy María

Las siglas IDS se corresponde con Sistema de Detección de Intrusiones, las siglas IPS se corresponde con Sistema de Prevención de Intrusiones. Es un conjunto de sistemas que se complementan para proveer de mayor seguridad a las redes de distintos tamaños. En especial, aquellas redes que requieren de un alto nivel de respuesta y servicio. Estos sistemas pueden aplicarse tanto a nivel de software o bien, a nivel hardware mediante equipos especializados. Se habla normalmente de IDS/IPS porque trabajan conjuntamente.

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.

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, 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.