Instituto Tecnológico De Cancún

Fundamentos de Telecomunicaciones

Tarea: Investigar Sobre SIEM e IDS/IPS

Ingeniería En Sistemas Computacionales

Alumno: Pérez Ovalle Alan

Docente: Ing. Ismael Jiménez Sánchez

Horario 05:00 Pm – 06:00 Pm

IDS, IPS y SIEM, ¿qué son?

Aunque las tres herramientas se usan para monitorizar y detectar intrusiones en los equipos o en la red de la empresa son diferentes entre sí. A continuación, os describimos cada una de ellas.

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, 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.

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.

SIEM

SIEM (Security Information and Event Management) o sistema de gestión de eventos e información de seguridad: es una solución híbrida centralizada que engloba la gestión de información de seguridad (Security Information Management) y la gestión de eventos (Security Event Manager). La tecnología SIEM proporciona un análisis en tiempo real de las alertas de seguridad generadas por los distintos dispositivos hardware y software de la red. Recoge los registros de actividad (logs) de los distintos sistemas, los relaciona y detecta eventos de seguridad, es decir, actividades sospechosas o inesperadas que pueden suponer el inicio de un incidente, descartando los resultados anómalos, también conocidos como falsos positivos y generando respuestas acordes en base a los informes y evaluaciones que registra, es decir, es una herramienta en la que se centraliza la información y se integra con otras herramientas de detección de amenazas.

Ventajas y desventajas de cada herramienta

IDS

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, además son vulnerables a los ataques DDoS que pueden provocar la inoperatividad de la herramienta.

IPS

Las ventajas de un IPS son:

- escalabilidad al gestionar multitud de dispositivos conectados a la misma red;

- protección preventiva al comprobarse de forma automatizada comportamientos anómalos mediante el uso de reglas prefijadas;
- fácil instalación, configuración y administración al estar disponibles multitud de configuraciones predefinidas y centralizar en un punto su gestión, aunque puede ser contraproducente para su escalabilidad;
- defensa frente a múltiples ataques, como intrusiones, ataques de fuerza bruta, infecciones por malware o modificaciones del sistema de archivos, entre otros;
- aumento de la eficiencia y la seguridad de la prevención de intrusiones o ataques a la red.

Entre sus desventajas, destacan los efectos adversos que pueden producirse en el caso de que se detecte un falso positivo, si por ejemplo se ejecuta una política de aislamiento de las máquinas de la red o en el caso de que se reciban ataques de tipo DDoS o DoS que pueden provocar su inutilización.

SIEM

Entre las ventajas de contar con un SIEM destacan la centralización de la información y eventos, es decir, se proporciona un punto de referencia común. La centralización permite automatizar tareas, con su consiguiente ahorro de tiempo y costes, el seguimiento de los eventos para detectar anomalías de seguridad o la visualización de datos históricos a lo largo del tiempo. Además, los sistemas SIEM muestran al administrador la existencia de vulnerabilidades, así como si están siendo aprovechadas en los ataques.

Entre sus desventajas en el caso de que se encargue de su mantenimiento un departamento de la empresa destacan sus altos costes de implantación, una curva de aprendizaje larga al tener que formar personal propio para esta tarea y una integración limitada con el resto del sistema. En el caso de que se externalice esta tarea se experimenta una pérdida de control de la información generada o un acceso limitado a determinada información y una fatiga por la alta recepción de notificaciones. Estos aspectos pueden gestionarse con el proveedor del servicio a través de los acuerdos de nivel de servicios o ANS.