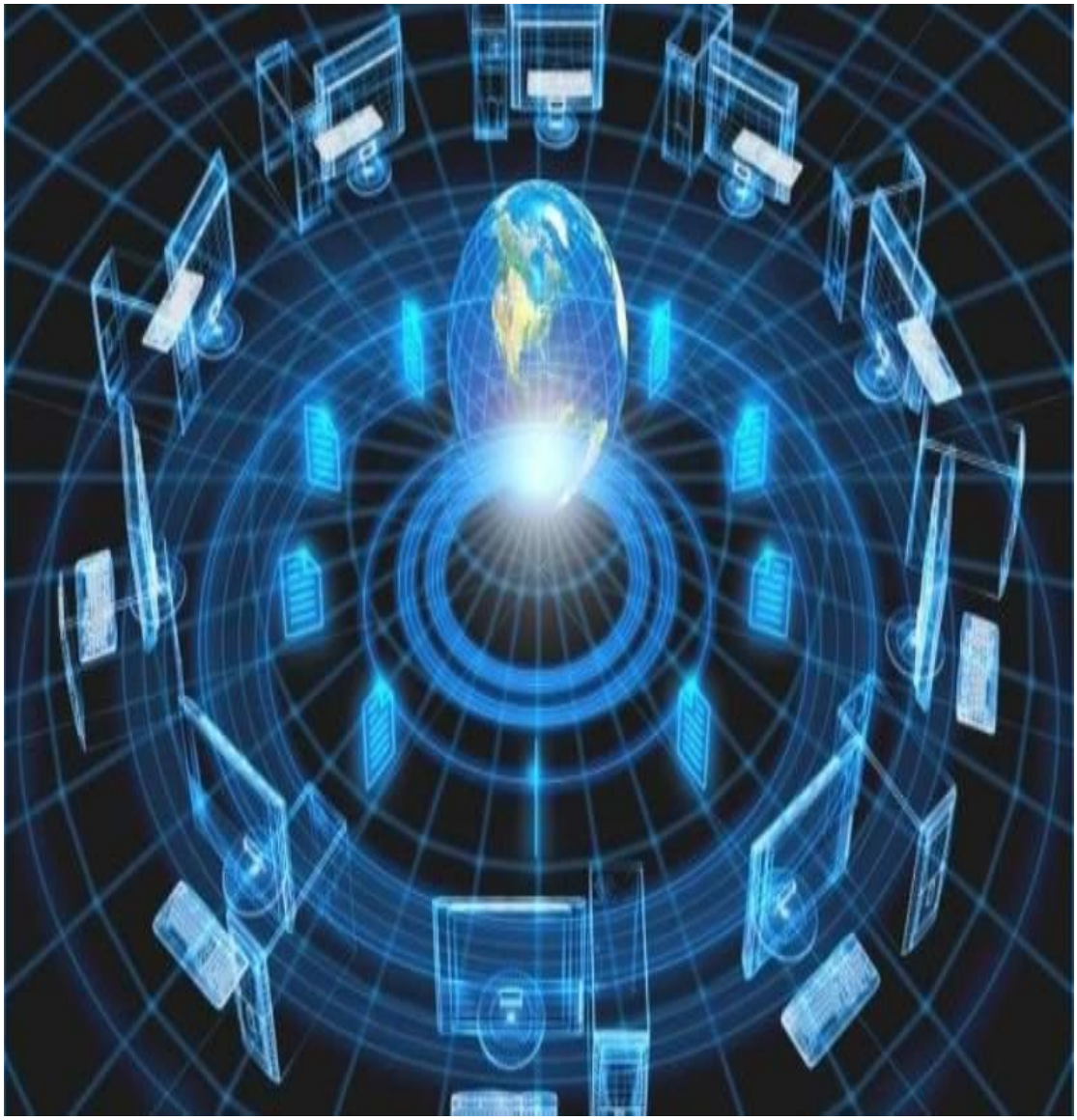

IDS /IPS

IBARRA SABIDO JOSE MARIA | **Fundamentos de Telecomunicaciones** | 03-12-2020

hace referencia a un mecanismo que, sigilosamente, escucha el tráfico en la red para detectar actividades anormales o sospechosas, y de este modo, reducir el riesgo de intrusión.

Existen dos claras familias importantes de IDS: el grupo N-IDS (Sistema de detección de intrusiones de red), que garantiza la seguridad dentro de la red, y el grupo H-IDS (Sistema de detección de intrusiones en el host), que garantiza la seguridad en el host.

Un N-IDS necesita un hardware exclusivo. Esta forma un sistema que puede verificar paquetes de información que viajan por una o más líneas de la red para descubrir si se ha producido alguna actividad maliciosa o anormal. El N-IDS pone uno o más de los adaptadores de red exclusivos del sistema en modo promiscuo. Este es una especie de modo "invisible" en el que no tienen dirección IP. Tampoco tienen una serie de protocolos asignados. Es común encontrar diversos IDS en diferentes partes de la red. Por lo general, se colocan sondas fuera de la red para estudiar los posibles ataques, así como también se colocan sondas internas para analizar solicitudes que hayan pasado a través del firewall o que se han realizado desde dentro. Los sistemas de detección de intrusos suelen formar parte de otros sistemas o software de seguridad, junto con la intención de proteger los sistemas de información.

La seguridad IDS funciona en combinación con medidas de autenticación y control de acceso de autorización, como una doble línea de defensa contra la intrusión. Los firewalls y el software antivirus o de malware generalmente se configuran en cada dispositivo individual en una red, pero a medida que las empresas crecen, entran y salen dispositivos más desconocidos o nuevos, como teléfonos celulares y USB. Los firewalls y el software antimalware por sí solo no son suficientes para proteger una red completa de ataques. Actúan como una pequeña parte de todo un sistema de seguridad.

El uso de un IDS completo como parte de tu sistema de seguridad es vital y está destinado a aplicarse en toda tu red de diferentes maneras. Un IDS puede capturar instantáneas de todo tu sistema y luego usar la inteligencia recopilada de patrones preestablecidos para determinar cuándo se produce un ataque o proporcionar información y análisis sobre cómo ocurrió un ataque.

Esencialmente, hay varios componentes para la preparación de intrusiones:

conocimiento de intrusiones potenciales,

prevención de intrusiones potenciales,

conocimiento de intrusiones activas y pasadas, y

respuesta a la intrusión.

Si bien puede parecer «demasiado tarde» una vez que ya ha ocurrido un ataque, saber qué intrusiones han sucedido o se han intentado en el pasado puede ser una herramienta vital para prevenir futuros ataques. Conocer el alcance de la intrusión de un ataque también es importante para determinar su respuesta y responsabilidades ante las partes interesadas que dependen de la seguridad de sus sistemas.

En la actualidad, el desarrollo de las estrategias de seguridades para los dispositivos y las redes de comunicación, ha influido en el surgimiento de un nuevo tipo de defensa: los IPS o Sistemas de Prevención de Intrusiones, que en buena medida pueden interpretarse como una evolución de los tradicionales IDS o Sistemas de Detección de Intrusiones.

Un Sistema de Prevención de Intrusos es un dispositivo de seguridad, fundamentalmente para redes, que se encarga de monitorear actividades a nivel de la capa 3 (red) y/o a nivel de la capa 7 (aplicación) del Modelo OSI, con el fin de identificar comportamientos maliciosos, sospechosos e indebidos, a fin de reaccionar ante ellos en tiempo real mediante una acción de contingencia.

El IPS fue creado con la intensión de ser una alternativa complementaria a otras herramientas de seguridad en redes, tales como un firewall o un IDS, por lo que muchas de sus características son heredadas de estos dos elementos, complementadas con un comportamiento proactivo ante ataques y amenazas.

Los Sistemas de Detección de Intrusos tienen como ventaja respecto de los firewalls tradicionales, el que toman decisiones de control de acceso basados en los contenidos del tráfico, en lugar de hacerlo basados en direcciones o puertos IP.

El contraste entre un IPS y un IDS radica en que este último es reactivo, pues alerta ante la detección de un posible intruso, mientras que el primero es proactivo, pues establece políticas de seguridad para proteger el equipo o la red de un posible ataque.

Clasificación de acuerdo al método de detección:

IPS basado en firmas o signaturas: cuentan con una base de datos de “firmas”, en la cual se reflejan patrones conocidos de ataques a la seguridad de un dispositivo o una red. Esta información se adhiere al dispositivo que realizará la detección para que así, mediante una búsqueda de coincidencias, se pueda establecer si existe o no un posible ataque y reaccionar en consecuencia.

IPS basado en anomalías: también conocido como basado en “perfil”, esta funcionalidad intenta identificar un comportamiento diferente que se desvíe de lo que, de alguna forma, se ha predefinido como una “actuación normal” de un dispositivo o una red. Para garantizar este comportamiento se hace uso de un potente análisis estadístico de indicadores de tráfico.

IPS basado en políticas: se requiere que se declaren muy específicamente las políticas de seguridad. El IPS reconoce el tráfico definido por el perfil establecido, permitiendo o descartando paquetes de datos, por lo que su manera de actuar ocurre de forma muy similar al funcionamiento de un firewall.

IPS basados en detección por Honey Pot (Pote de Miel): funciona usando un equipo configurado para que, a primera vista, parezca ser vulnerable e interesante para un ataque, de forma tal, que al ocurrir estos, se deja evidencia de la forma de actuar, con lo cual posteriormente se pueden implementar políticas de seguridad.