Seguridad de Redes

Transcribed on July 31, 2025 at 5:05 PM by Minutes AI

Speaker 1 (00:01)

Bienvenidos a esta nueva sesión.

En esta sesión vamos a tratar el tema de la monitorización, detección y prevención de intrusiones en nuestra arquitectura.

Un Sistema de Detección de Intrusiones o IDS es una herramienta de seguridad diseñada para monitorizar y analizar el tráfico de red en busca de actividades maliciosas o anómalas que puedan indicar un intento de intrusión en un sistema o red informática.

Su principal objetivo es identificar y alertar sobre posibles amenazas de seguridad como intentos de acceso no autorizado, ataques de malware, anomalías de tráfico, entre otros muchos más.

Los IDS se pueden implementar en forma de software o de hardware y pueden operar en tiempo real o de forma periódica dependiendo de las necesidades y requisitos de seguridad de nuestra empresa u organización.

Los IDS al detectar y alertar sobre actividades sospechosas, permiten a los equipos de seguridad responder rápidamente a posibles intrusos y tomar medidas para mitigar los riesgos en seguridad.

Además, los IDS se integran con otros sistemas de seguridad como los cortafuegos y también los IPS que veremos luego, para proporcionar un defensa integral contra una gran amplia gama de amenazas.

Un Sistema de Detección de Intrusos en Red o NIDS es una herramienta de seguridad diseñada para monitorizar y analizar también el tráfico de red.

A diferencia de un IDS que puede monitorizar solo un dispositivo o una red local, un ENERIS o un NITS examina el tráfico en toda la red, lo que le hace especialmente efectivo para detectar amenazas que atraviesan múltip punto de acceso y este funciona escaneando el tráfico de red en busca de patrones conocidos de actividad maliciosa, como intentos de intrusión, exploits o algún tipo de comportamiento sospechoso.

Cuando detecta una actividad anómala, el niche genera alertas que son enviadas al equipo de seguridad para su revisión y acción.

En definitiva, la diferencia entre un NITS y un IDS tradicional radica en su alcance de monitorización.

Mientras un IDS se centra en la seguridad de un solo dispositivo, supervisa y analiza el tráfico de toda la red.

Un Sistema de Detección de Intrusiones en el host o un HIDS es una herramienta también de seguridad diseñada para monitorizar y analizar la actividad de un dispositivo individual, como un servidor, una estación de trabajo.

A diferencia de los sistemas de detección de intrusiones en la red como son los NITS que se enfocan en la red y también en diferencia con los IDS, que también pueden monitorizar la red de un sistema específico.

Los HIDS operan a nivel de host y examinan eventos y actividades locales, como cambios en archivos, intentos de autenticación o actividades de diferentes procesos.

La ventaja del HIDS es que puede detectar amenazas que no pueden ser visibles desde el punto de vista de la red, como ataques dirigidos a vulnerabilidades específicas de aplicaciones o malware que intentan evadir la detección a un nivel de red.

Un sistema de prevención de intrusiones IPS es una herramienta de seguridad diseñada para identificar y bloquear activamente las amenazas y actividades maliciosas en una red.

A diferencia de los sistemas de detección de intrusiones o IDS, que solamente detectan y notifican sobre posibles intrusiones, un IPS tiene la capacidad adicional de tomar medidas automáticas para prevenir o mitigar activamente las amenazas detectadas.

Utiliza muchas técnicas, como la inspección de paquetes, el análisis de protocolos y firmas de amenazas.

También examina el tráfico de red para buscar patrones de comportamiento sospechoso y malicioso.

Cuando detecta una amenaza, el IPS puede tomar medidas inmediatas como bloquear el tráfico, rechazar conexiones o generar alertas para notificar a los administradores.

Un sistema de prevención de intrusiones basados en la red ¿Que es el NIPS?

NIPS es una herramienta de seguridad que está diseñada para proteger una red completa y lo que hace es monitorizar y analizar el tráfico de la red en busca de actividades maliciosas o anómalas.

A diferencia de los sistemas de prevención de intrusiones basados en el host, como los HEAPS, que se centran en la protección de sistemas individuales, un NIPS opera a nivel de red y puede examinar todo el tráfico que atraviesa la infraestructura de red de una organización, y esto lo hace utilizando técnicas como la inspección profunda de paquetes, el análisis de comportamiento, la detección de firmas, etc.

Y el NIPS también puede identificar y bloquear activamente las amenazas en tiempo real.

Un sistema de prevención de intrusiones en el host o HIPS es una herramienta de seguridad que protege un sistema informático individual monitorizando y analizando la actividad del dispositivo localmente.

En este caso, el HEAPS se centra en la protección de un host, como un servidor o una estación de trabajo, y también utiliza técnicas como inspección de archivos, control de acceso, monitorización, etc.

La diferencia con los HIDS es también que pueden tomar algún tipo de acción cuando se detecta algún tipo de amenaza.

También es importante mencionar que es un Sistema de Gestión de Información y Eventos de Seguridad o SIEM, que es una solución también de seguridad informática que está diseñada para proporcionar una visión integral y centralizada de cómo está la seguridad en una organización y para ello integra múltiples fuentes de datos de seguridad como registro de eventos, alertas de seguridad, registro de sistemas, dispositivos de red, etc.

El SIEM permite la recopilación, correlación y el análisis en tiempo real de esta información para poder detectar y responder a amenazas potenciales.

Además de la detección de amenazas, el SIEM también facilita la generación de informes, también facilita la monitorización, etc.

En otras palabras, un SIEM es una plataforma unificada para la supervisión proactiva y la gestión de eventos de seguridad, lo que ayuda a organizaciones a identificar y mitigar eficazmente los riesgos de seguridad en toda la infraestructura de IT.

Aquí puedes ver una tabla que incluye ejemplos de diferentes tipos de sistemas de prevención y detección de intrusiones, tanto a nivel de host de leer como de sistemas de gestión de información de eventos como los SIEM.

Podemos ver como en IDS muy conocido Snort, que veremos más adelante también en un vídeo explicativo, tenemos para Niche, tenemos Suricata, para IPS, tenemos el Cisco Firepower, para el HIDS el OSS SEC, bueno hay varios, por ejemplo en los SIEM aparece Splunk que es muy muy conocido, etc.

Estos son solo algunos de los que podemos encontrar, pero hay una gran variedad de herramientas tanto de pago como de código libre o open source.

La implementación de dispositivos de seguridad como los sistemas de detección de intrusos, los IDs, los NIDS, que son los sistemas de detección de intrusos en la red, los sistemas de prevención de intrusión como los IPS, etc.

Desempeñan un papel fundamental en la protección y el fortalecimiento de una seguridad de una infraestructura de red de datos.

Estos dispositivos trabajan en conjunto para detectar y prevenir intrusiones tanto internas como externas, identificando comportamientos maliciosos, anomalías en el tráfico y ataques en tiempo real.

También esto es importante, proporcionan una visión integral de la actividad de la red, permitiendo a los equipos de ciberseguridad anticiparse a posibles amenazas, tomar medidas proactivas y responder de manera eficiente ante incidentes de seguridad, lo que al final contribuye a salvaguardar la confidencialidad, la integridad y la disponibilidad de los datos de los sistemas de una empresa u organización.

Llegamos al final de la sesión.

Os esperamos en el siguiente vídeo.

What not to them.