Fundamentos de telecomunicaciones

Arturo alexander felipe lopez
Diciembre 2020
Profesor: ING. Ismael Jiménez Sánchez

Instituto tecnológico de Cancún
Ing. En sistemas computacionales
Investigación IDS/IPS

IDS/IPS

La detección de intrusiones es el proceso de monitorear los eventos que ocurren en su red y analizarlos en busca de signos de posibles incidentes, violaciones o amenazas inminentes a sus políticas de seguridad. La prevención de intrusiones es el proceso de realizar la detección de intrusiones y luego detener los incidentes detectados. Estas medidas de seguridad están disponibles como sistemas de detección de intrusos (IDS) y sistemas de prevención de intrusiones (IPS), que se vuelven parte de su red para detectar y detener posibles incidentes.

-¿Qué se puede hacer con IDS / IPS?

Los sistemas de detección de intrusiones (IDS) y los sistemas de prevención de intrusiones (IPS) vigilan constantemente su red, identificando posibles incidentes y registrando información sobre ellos, deteniendo los incidentes e informándolos a los administradores de seguridad. Además, algunas redes utilizan IDS / IPS para identificar problemas con las políticas de seguridad y disuadir a las personas de violar las políticas de seguridad. Los IDS / IPS se han convertido en una adición necesaria a la infraestructura de seguridad de la mayoría de las organizaciones, precisamente porque pueden detener a los atacantes mientras recopilan información sobre su red.

-¿Cómo funciona IDS?

Las tres metodologías de detección de IDS se utilizan normalmente para detectar incidentes.

*La detección basada en firmas compara las firmas con los eventos observados para identificar posibles incidentes. Este es el método de detección más simple porque compara solo la unidad de actividad actual (como un paquete o una entrada de registro, con una lista de firmas) mediante operaciones de comparación de cadenas.

*La detección basada en anomalías compara las definiciones de lo que se considera actividad normal con los eventos observados para identificar desviaciones significativas. Este método de detección puede ser muy eficaz para detectar amenazas previamente desconocidas.

*Stateful Protocol Analysis compara perfiles predeterminados de definiciones generalmente aceptadas para la actividad de protocolo benigna para cada estado de protocolo con eventos observados con el fin de identificar desviaciones.