SIEM IDS/IPS

Instituto Tecnológico de Cancún.

Kanxoc Ek Félix Gerardo.

Fundamentos de Telecomunicaciones.

Ismael Jiménez Sánchez.

Diciembre 2020.

SIEM, IDS/IPS.

Son un conjunto de herramientas se sirven o se encargan de mitigar o detectar ataques dentro de la red.

SIEM (Stands of security information and event management)

Es una herramienta, que nos sirve para reunir toda la información de seguridad y la gestión de eventos. Esto nos va a servir para poder hacer un análisis. Este nos permite tener la posibilidad de hacer un análisis en tiempo real de alertas de seguridad y esto se debe a que son generadas por distintos dispositivos que están en la red, estos pueden ser hardware y/o software.

En pocas palabras, SIEM es una herramienta que sirve para reunir toda la información y una vez que está reunida toda esa información, este se complementa con otros programas que servirán para analizar o detectar las diferentes amenazas.

IPS (Intrusion Prevention System)

Es una herramienta que nos ayudara a prevenir ataques o intrusiones dentro del sistema, si bien estas herramientas previenen los distintos tipos de intrusiones o ataques al sistema, esto no quiere decir que los desaparezca por completo, En estos sistemas hacen un análisis en tiempo real de toda la información de la red, ya sean conexiones o protocolos que se están utilizando dentro de la red, y verifican si las conexiones están bien o se está produciendo un incidente dentro de la red. IPS puede descartar paquetes y desconectar conexiones, además de lanzar un aviso o alarmas.

IDS (Intrusion Detection System)

Es una herramienta que nos sirve para hacer un monitoreo en tiempo real y de esa manera poder detectar accesos no autorizados o anomalías en una PC o dentro de una red. Estos emiten una alerta a los administradores de la red, por lo cual los administradores decidirán qué medidas utilizarán. Estos sistemas solo sirven para mandar alertas de intrusos o anomalías, esto quiere decir que estas herramientas no mitigan o tratan de mitigar la intrusión o anomalía.