INSTITUTO TECNOLÓGICO DE CANCÚN

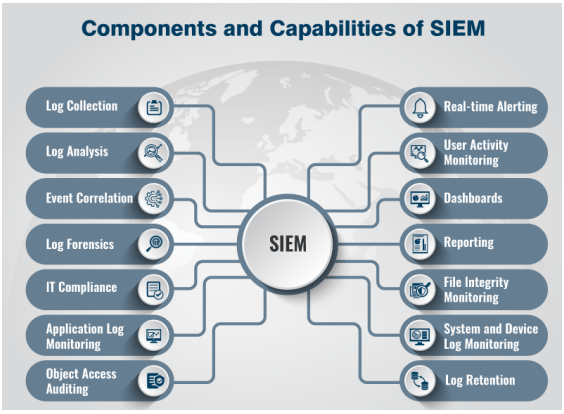
ESPECTRO ELECTROMAGNETICO

MIGUEL ÁNGEL OY CASTRO

DICIEMBRE 3 2020

PROFESOR: ISMAEL JIMÉNEZ SÁNCHEZ

FUNDAMENTOS DE TELECOMUNICACIONES



Qué es un IDS?

Un IDS (Intrusion Detection System) es un software de seguridad cuya función es detectar accesos no autorizados en un sistema o una red de ordenadores, y en base a ello, generar algún tipo de alerta o log para que posteriormente pueda ser gestionado por el administrador de sistemas correspondiente.

A diferencia de un IPS (Intrusion Prevention System), el IDS no actúa ante un posible ataque, simplemente alerta del mismo. Podríamos decir que el IPS es en base, la misma idea, pero que, al detectar una intrusión, ejerce alguna función determinada en base al tipo de ataque, para prevenir que este llegue a ser efectuado o mitigarlo en caso de que ya se haya materializado.

Tipos de IDS (en base a su radio de actuación)

HIDS (HostIDS) – Monitorea el tráfico entrante y saliente de un host específico. Sólo actúa en el host en el que está corriendo (recomendado para servidores web).

NIDS (NetworkIDS) – Captura todo el tráfico de la red y detecta tráfico inusual (están constituidos por un sniffer).


BRO – Bro es open source (políticas especializadas).

SNORT – Snort es también gratis y open source y se caracteriza por ser bastante ligero (preprocesadores).

SURICATA – Suricata es gratis, open source, robusto y rápido (procesamiento multi-threaded)