INSTITUTO TECNOLÓGICO DE CANCÚN

INGENIERÍA EN

SISTEMAS COMPUTACIONALES

FUNDAMENTOS DE TELECOMUNICACIONES

.

NOMBRE DEL ALUMNO:

COLLÍ CHEL WILLIAM BLADIMIR

HORARIO

LUNES A JUEVES

5:00 PM – 6:00 PM

PROFESOR

ISMAEL JIMENEZ SANCHEZ

¿Qué es el SIEM?

SIEM (información de seguridad y gestión de eventos), es una tecnología capaz de detectar rápidamente, responder y neutralizar las amenazas informáticas.

Un sistema SIEM puede permitir tener el control absoluto sobre la seguridad informática de la empresa. Al tener información y administración total sobre todos los eventos que suceden segundo a segundo, resulta más fácil detectar tendencias y centrarse en patrones fuera de lo común.

SEM: centraliza el almacenamiento y permite un análisis casi en tiempo real de lo que está sucediendo en la gestión de la seguridad, detectando patrones anormales de accesibilidad y dando mayor visibilidad a los sistemas de seguridad.

SIM: Mientas que si se recopila los datos a largo plazo en un repositorio central para luego analizarlo, proporcionando informes automatizados al personal de seguridad informática.

La importancia del sistema SIEM:

La importancia de estas soluciones está en la prevención de amenazas no relacionadas con vulnerabilidades del software, tales como malware, o la denegación del servicio (DoS).

¿Qué es el ids?

Sistema de detección de intrusos (o IDS de sus siglas en inglés Intrusion Detection System). Programa usado para detectar accesos no autorizados a una computadora o a una red.

Estos accesos pueden ser ataques de habilidosos hackers, o de Script Kiddies que usan herramientas automáticas.

El IDS suele tener sensores virtuales (por ejemplo, un sniffer de red) con los que el núcleo del IDS puede obtener datos externos (generalmente sobre el tráfico de red). El IDS detecta, gracias a dichos sensores, anomalías que pueden ser indicio de la presencia de ataques o falsas alarmas.

El funcionamiento de estas herramientas se basa en el análisis pormenorizado del tráfico de red, el cual al entrar al analizador es comparado con firmas de ataques conocidos, o comportamientos sospechosos, como puede ser el escaneo de puertos, paquetes malformados, etc. El IDS no sólo analiza qué tipo de tráfico es, sino que también revisa el contenido y su comportamiento.

HIDS (HostIDS): (Sistema de detección de intrusiones de red), que garantiza la seguridad dentro de la red, el principio de funcionamiento de un HIDS, depende del éxito de los intrusos, que generalmente dejaran rastros de sus actividades en el

equipo atacado, cuando intentan adueñarse del mismo, con propósito de llevar a cabo otras actividades.

NIDS (NetworkIDS): (Sistema de detección de intrusiones en el host), que garantiza la seguridad en el host, un IDS basado en red, detectando ataques a todo el segmento de la red. Su [[interfaz debe funcionar en modo promiscuo capturando así todo el tráfico de la red.

¿Qué es el ips?

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.

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:

IPS basado en anomalías:

IPS basado en políticas:

IPS basados en detección por *Honey Pot* (Pote de Miel):

IPS basado en host:

IPS basado en la red: