**INSTITUTO TECNOLÓGICO DE CANCÚN**

**ALUMNO: GONGORA JIMENEZ FRANCISCO DAVID.**

**PROFESOR: ISMAEL JIMÉNEZ SÁNCHEZ.**

**MATERIA: FUNDAMENTOS DE TELECOMUNICACIONES.**

**U3 TAREA:**

**INVESTIGAR SOBRE SIEM E IDS/IPS**

**HORARIO: 5PM-6PM.**

**FECHA DE ENTREGA:**

**3 DE NOVIEMBRE DEL 2020**

# ÍNDICE

## Contenido

# ¿QUÉ ES SIEM?

SIEM significa Security Information and Event Management y es una combinación de dos conceptos: SIM (Security Information Management) y SEM (Security Event Management). Esta unión plantea un enfoque basado en software que permite obtener una visión completa de la seguridad informática. Un sistema SIEM considera en todo momento los requisitos específicos de la empresa, siempre que existan definiciones claras e individuales sobre qué procesos y eventos son relevantes para la seguridad, así como de qué manera y con qué prioridad es preciso reaccionar ante ellos.

**¿Cómo funciona un SIEM?**

El objetivo del Security Information and Event Management es poder responder con rapidez y precisión ante las amenazas. Con un SIEM, los responsables informáticos obtienen una poderosa herramienta que les permite actuar no solo cuando ya sea demasiado tarde, los sistemas SIEM tratan de visibilizar los ataques o las tendencias de ataque en tiempo real mediante la recopilación y el análisis de mensajes ordinarios, notificaciones de alarma y archivos de registro en un lugar centralizado.

**¿Cuándo se utiliza SIEM?**

Las empresas que tratan datos sensibles de clientes o que están supeditadas a operaciones de telecomunicaciones eficientes apuestan por sistemas de Security Information and Event Management precisamente por este motivo.

**Ejemplo práctico: intentos de acceso a VPN**

Los accesos remotos por VPN son comunes dentro de muchas redes de trabajo empresariales.

# ¿QUÉ ES UN SISTEMA DE DETECCIÓN DE INTRUSOS (IDS)?

Un Intrusion Detection System (IDS), en español sistema de detección de intrusos, es utilizado para detectar a tiempo ataques en contra de un sistema informático o de una red. El IDS software necesario se puede instalar en el sistema que está siendo supervisado o, también, en un dispositivo independiente. los sistemas de detección de intrusos supervisan y analizan las actividades de la red en búsqueda de tráfico inusual para informar al usuario

en caso de que lo haya, este tiene la oportunidad de responder a los ataques de acceso y de detener el ataque.

**Sistema de detección de intrusos basado en el host**

protege estructuras informáticas centralizadas, el sistema de detección se instalaba en el ordenador central a través del cual se ejecutaban los diferentes terminales conectados y, desde ese host, se controlaba el intercambio de archivos kernel, principalmente, estos se encargaban de filtrar el tráfico, o los datos cuya auditoría era relevante, y de enviar los resultados al servidor central que, a su vez, era responsable de la detección de los ataques.

**Intrusion Detection System basados en la red**

el acceso no autorizado desde Internet tiene lugar vía protocolos como TCP/IP o UDP (User Datagram Protocol), los sistemas basados en la red no comprueban los datos, sino los paquetes IP, también constituyeron una unidad central de monitoreo que no se limitaba a la protección de un solo sistema, sino que podía ver todo el tráfico de la red.

**¿Cómo funcionan los sistemas de reconocimiento modernos?**

Estos sistemas se caracterizan por un sistema de gestión central que recibe las informaciones necesarias tanto desde el software basado en la red como desde el software basado en el host. Hay tres componentes básicos involucrados en el proceso de reconocimiento:

**Monitoreo de datos**

El monitor de datos tiene la tarea de recoger y hacer un primer filtro a los datos necesarios para filtrar intrusos, incluye archivos log de sistemas informáticas y aplicaciones de seguridad como, por ejemplo, la capacidad de la CPU, el número de conexiones de red activas o la cantidad de intentos de inicio de sesión.

**Análisis**

El monitor de datos envía el flujo de datos recogidos y previamente filtrados al llamado analyzer (analizador). Este debe editar y evaluar la información obtenida en tiempo real, de lo contrario no sería posible evitar los ataques a tiempo, en caso de usos indebidos del **sistema (misuse detection)**, el analizador intenta detectar patrones de ataque conocidos, denominados firmas

(signature), en los datos obtenidos. Estos se almacenan en una base de datos independiente que es actualizada periódicamente.

**La detección de anomalías (anomaly detection)** se basa en un principio diferente: este método de análisis supone que el acceso no autorizado causa un comportamiento anormal en el sistema, el analizador se puede configurar de tal manera que encienda una alarma cuando la capacidad de la CPU o el tráfico a la página web sobrepase un cierto número.

**INFORME DE RESULTADOS**

**el Intrusion Detection System** informa al administrador de la red si encontró un ataque o un comportamiento sospechoso del sistema. Dependiendo del potencial de riesgo, existen diferentes posibilidades de notificarlo, por ejemplo, un sistema que necesita defenderse enviaría

- un correo electrónico que explique la naturaleza del ataque,
- una alarma local como una ventana emergente que active la consola de seguridad,
- un mensaje de alerta a un dispositivo móvil.

El grado de riesgo obtenido en la detección de anomalías se deriva del grado de desviación del valor estándar, mientras que el procedimiento de identificación de usos indebidos en el sistema

## ¿QUÉ ES UN Intruder prevention systems (IPS)?

Los Intrusion Prevention Systems (IPS) son sistemas de prevención de intrusos que van un paso más allá de los sistemas de detección de intrusos: una vez que han encontrado un posible ataque, no solo informan al administrador, sino que llevan a cabo medidas concretas e inmediatas. De esta forma evitan que transcurra un espacio de tiempo muy grande entre la detección y lucha contra el intruso, los IPS utilizan sensores basados en el host o en la red para registrar y evaluar datos del sistema y paquetes de red, un Intruder Prevention System es recomendable configúralo manualmente para evitar que los métodos de detección de anomalías clasifiquen acciones normales de los usuarios como una amenaza y las bloqueen. Algunos programas utilizados son:

**DenyHost: la respuesta simple a ataques de fuerza bruta**

La herramienta DenyHost, escrita en Python, permite establecer un Intrusion Prevention System basado en el host para conexiones SSH/SSHD que reconoce y detiene ataques de fuerza bruta, la aplicación es de código abierto comprueba las entradas en los registros de autenticación para identificar intentos fallidos de acceso a SSH.

**Snort: reglas flexibles para una red segura**

En 1998, el programador Martin Roesch publicó la herramienta de seguridad Snort, aunque únicamente para sistemas UNIX. Cisco Systems se ocupa, desde 2013, de su desarrollo y programación multiplataforma bajo la licencia GPL, proporciona las funciones necesarias para crear poderosos Intruder prevention systems basados en la red, comprueba el tráfico de la red en tiempo real y este compara los paquetes de datos entrantes y salientes con los patrones registrados, que en Snort se conocen como reglas (rules).