SIEM, IDS e IPS

UNIDAD III

FECHA: 03 – Dic – 2020

Wilmer Rodríguez Jiménez

Fundamentos de telecomunicaciones

Prof:Ismael Jimenez Sanchez

Periodo Ago – Dic

SIEM

El Security Information and Event Management seria como una parte dentro de la seguridad informática, aquí es donde los productos y servicios de software combinan Security Information Management (SIM) y security information management (SIM)). Que basicamente hacen el análisis en tiempo real de las alertas de seguridad generadas por aplicaciones y hardware de red.

También podríamos tomar como ejemplo de regla personalizada la posiblilidad de autenticación de usuarios, ataques detectados e infecciones detectadas

IDS

Un Intrusion Detection System (IDS), que en si significa sistema de detección de intrusos, es utilizado para detectar a tiempo ataques en contra de un sistema informático o de una red asi que el IDS software que es necesario se puede instalar en el sistema que está siendo supervisado o en un dispositivo entiendo que muchos proveedores distribuyen soluciones IDS preconfiguradas de con un cierto costo por otra parte 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 encuentre asi se logra que este tenga la oportunidad de responder a los ataques de acceso y de detener el ataque.

Para ello podemos tener en cuenta que hay 2 tipos de IDS:

HIDS (Host Intrusion Detections System).
Busca detectar anomalías que indican un riesgo potencial, revisando las actividades en la máquina que en este caso sería nuestro host.

NIDS (Network Instrusion Detection System).
El NIDS lo que lo hace diferente del HIDS sería que el NIDS da cobertura a toda una red para detectar actividad sospechosa relizando un análisis del tráfico de red.

IPS

Entiendo que sirven para la prevención de accesos a partir de la identificación y bloqueo de un tipo de patrones específicos de ataque en su transito por la red, para esta funcionalidad se denominan IPS (Intrusion Prevention System) y están específicamente diseñados para prestar de manera dedicada este tipo de funciones con una base amplia de firmas y algunas detecciones basadas en métodos relacionados con comportamiento.

NIPS.
Análisis para una red.
WIPS.
Análisis dentro una red inalámbrica.
NBA.
Analiza los comportamientos que hay dentro de la red uno de los importantes sería la denegación de servicios.
HIPS.
Análisis de red dedicado para un host.