Materia:

Fundamentos de telecomunicaciones

IDS - IPS

Profesor:

Ismael Jiménez Sánchez

Alumno:

Ángel Eduardo Hernández Pimentel

03 De diciembre del 2020

El IDS es un sistema de detección de intrusos, como su nombre en inglés lo dice “Intrusion Detection System”, se utiliza para detectar accesos no permitidos a una red.

El IDS posee sensores que les permite obtener datos, de manera que cuando el IDS detecta el tráfico puede identificar por intermedio de anomalías o comportamientos extraños si se trata de un ataque o un falso positivo. El modo de funcionamiento del IDS es analizar a nivel muy profundo todo el tráfico de red, en el momento que dicho tráfico pasa se con firmas de ataques ya reconocidos, así como también se controlan los comportamientos extraños como el escaneo de puertos, por ejemplo. Este equipo debe funcionar junto con un Firewall debido a que el IDS no tiene la funcionalidad de bloquear un ataque.

Tipos de IDS:

HIDS: busca datos que hayan dejado los atacantes en un equipo cuando intentan tomar control del mismo, con toda la información que consiguen saca sus conclusiones.

NIDS: IDS de red, detecta ataques a nivel de toda la red. Debe ver todo el tráfico que entra a la red.

IPS (Intrusion Prevention System)

Controla el acceso de usuarios ilegítimos adicionando la posibilidad de bloquear los ataques, no simplemente de monitorearlos. Tiene varias opciones para implementarlo, Hardware, software o combinación de ambas. Los IPS se categorizan según el modo en el que detectan el tráfico malicioso:

- Basado en firmas: compara el tráfico con firmas de ataques conocidos, debe tener la lista de firmas actualizada.

- Basado en políticas: se definen políticas de seguridad estrictas, si el tráfico está permitido el IPS permite el tráfico, si no lo está lo bloquea.

- Basado en anomalías: este método es el que más falsos positivos genera debido a que es muy difícil que es lo normal o estándar. En este modo encontramos dos opciones:

- Detección estadística de Anormalidades: analiza todo el tráfico durante un tiempo determinado, luego de este tiempo crea una línea de lo que es “normal o estándar”. Luego de terminado este período si el comportamiento varía mucho en comparación a la regla creada, se toma como una posibilidad de ataque.

- Detección no Estadística de Anormalidades: en esta opción el Administrador define la línea de lo que es lo “normal o estándar” que va a ser la base para la comparación del tráfico.

En resumen, el IPS agrega la posibilidad de bloquear ataques y además protege de forma proactiva la red, mientras que el IDS no permite bloquear y protege de forma reactiva la red.