INSTITUTO TECNOLÓGICO DE CANCÚN

INGENIERÍA EN

SISTEMAS COMPUTACIONALES

FUNDAMENTOS DE TELECOMUNICACIONES

NOMBRE DEL ALUMNO:

CHAN BURGOS JOSE REYES

HORARIO

LUNES A JUEVES

5:00 PM – 6:00 PM

PROFESOR

ING. ISMAEL JIMENEZ SANCHEZ

IDS

Es un componente dentro del modelo de seguridad informática de una organización. Consiste en detectar actividades inapropiadas, incorrectas o anómalas, desde el exterior o interior de un dispositivo o una infraestructura de red.

El IDS se basa en la hipótesis de que el patrón de comportamiento de un intruso es diferente al de un usuario legítimo, lo que se emplea para su detección por análisis de estadísticas de uso.

El funcionamiento de un Sistema de Detección de Intrusos se basa en el análisis pormenorizado del tráfico de red o el uso de los dispositivos. Para la evaluación se compara la situación con firmas de ataques conocidos, o comportamientos sospechosos. Un IDS no solo analiza qué tipo de tráfico se emplea, sino también revisa su contenido y comportamiento; además, observa si ocurre un escaneo de puertos o la transmisión de paquetes de datos mal formados, entre otros aspectos.

TIPOS DE IDS

IDS basados en Red

IDS basados en Host o ab0nado de la red

IDS basado en Conocimiento

IDS basado en Comportamiento

IDS Activo

IDS Pasivo

IPS

Un IPS complementa una configuración de IDS mediante la inspección proactiva del tráfico entrante de un sistema para eliminar las solicitudes maliciosas. Una configuración típica de IPS utiliza firewalls de aplicaciones web y soluciones de filtrado de tráfico para proteger las aplicaciones.

Los Sistemas de Detección de Intrusos tienen como ventaja respecto de los firewalls tradicionales, el que toman decisiones de control de acceso basados en los contenidos del tráfico, en lugar de hacerlo basados en direcciones o puertos IP.

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.

Si bien es eficaz para bloquear los vectores de ataque conocidos, algunos sistemas IPS tienen limitaciones. Estos son comúnmente causados por una dependencia excesiva de reglas predefinidas, haciéndolos susceptibles a falsos positivos.