Nombre de la Materia:
Fundamentos de Telecomunicaciones Aula

Nombre de la Licenciatura:
Ing. Sistemas Computacionales.

Nombre del Alumno(a):

Pool Ramírez Miguel Ángel

Nombre de la Tarea:

Sistema de Detección de Intrusos (IDS) / Sistema de Prevención de Intrusos (IPS)

Unidad #3

Nombre de la Unidad: Modulación

Nombre del Profesor(a):

Ing. Ismael Jiménez Sánchez

Fecha: 03/12/20

Introducción

La detección y prevención de intrusiones son dos términos generales que describen las prácticas de seguridad de las aplicaciones utilizadas para mitigar ataques y bloquear nuevas amenazas.

La primera es una medida reactiva que identifica la de detección de intrusos. Capaz de detectar el malware existente como troyanos, puertas traseras, rootkits) y detectar ataques de ingeniería social como, man in the middle, phishing que manipulan a los usuarios para el robo de credenciales e información confidencial.

La segunda es una medida de seguridad proactiva que utiliza un sistema de prevención de intrusiones para bloquear ataques preventivos de aplicaciones. Esto incluye inclusiones en archivos remotos que facilitan las inyecciones de malware e inyecciones de SQL, utilizadas para acceder a las bases de datos de una empresa.

¿Qué es un sistema de detección de intrusos (IDS)?

Un IDS es un dispositivo de hardware o una aplicación de software que utiliza firmas de intrusión conocidas para detectar y analizar el tráfico de red entrante y saliente en busca de actividades anormales.

Esto se hace a través de:

- Comparaciones de archivos del sistema contra firmas de malware.
- Procesos de escaneo que detectan signos de patrones maliciosos.
- Monitoreo del comportamiento del usuario para detectar intenciones maliciosas.
- Monitoreo de configuraciones y configuraciones del sistema.
- Monitoreo del tráfico de red entrante y saliente de los dispositivos

Al detectar una violación de la política de seguridad, un virus o un error de configuración, un IDS puede expulsar a un usuario infractor de la red y enviar una alerta al personal de seguridad.

A pesar de sus beneficios, incluido el análisis en profundidad del tráfico de red y la detección de ataques, un IDS tiene inconvenientes inherentes. Debido a que utiliza firmas de intrusión previamente conocidas para localizar ataques, las amenazas recientemente descubiertas 0 Day, pueden permanecer sin ser detectadas.

Además, un IDS solo detecta ataques continuos, no ataques entrantes. Para bloquearlos, se requiere un sistema de prevención de intrusiones.

¿Qué es un sistema de prevención de intrusiones (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.

Un IPS evita ataques al descartar paquetes maliciosos, bloquear IP's ofensivas y alertar al personal de seguridad de posibles amenazas. Este sistema generalmente usa una base de datos preexistente para el reconocimiento de firmas y puede programarse para reconocer ataques basados en el tráfico y anomalías de comportamiento.

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.

Referencias.

- Ciberseguridad Industrial by Logitek . (Jul 8, 2020). IDS vs IPS ¿Cuál es la diferencia?. Dic 3, 2020, de Logitek Sitio web: https://www.ciberseguridadlogitek.com/ids-vs-ips-cual-es-la-diferencia/