¿Qué es un sistema de prevención de intrusiones, IPS?

Ips en seguridad cibernética es una evolución, una mejora respecto al Ids, que ya vimos en una publicación anterior y hace parte por supuesto de un esquema de seguridad más fuerte y complejo para organizaciones medianas y grandes.

IPS es la abreviatura de «sistema de prevención de intrusiones». El software IPS e IDS son ramas del mismo árbol y utilizan tecnologías similares. La detección facilita la prevención, por lo que los IPS y los IDS deben funcionar en combinación para tener éxito.

¿Cómo se diferencian?

La diferencia clave entre estos sistemas de intrusión es que uno es activo y el otro es pasivo. Un monitor de intrusión típico que le avisa cuando algo es inusual o sospechoso puede denominarse IDS pasivo. Un sistema que detecta y actúa para prevenir daños y ataques posteriores se denominaría reactivo. Esto se debe a que reacciona a la intrusión en lugar de simplemente identificarla.

Un IPS o IDS reactivo no suele implementar las soluciones por sí mismo, sino que se comunica con las aplicaciones y los cortafuegos modificando su configuración. Un HIDS reactivo puede comunicarse con múltiples ayudas de red, con el objetivo de restaurar la configuración del dispositivo. Esto podría ser la configuración de SNMP, o aun de un administrador de

configuración instalado en el dispositivo.

Si se lanza un ataque al administrador, no se puede responder con un bloqueo automático del uso del administrador o alterando la contraseña del sistema. Esto se debe a que hacerlo bloquearía al usuario raíz de los servidores y la red.

Falsos positivos

Los usuarios de IDS a veces se quejan de que reciben una gran cantidad de falsos positivos cuando configuran el IDS por primera vez. Su IPS implementará una estrategia de defensa automáticamente, basada en la detección de condiciones y umbrales de alerta.

Si el IPS no está calibrado correctamente, esto puede causar caos y provocar que la actividad de su red auténtica se detenga por completo. Por tanto, no está de más enfatizar la calibración objetiva y pertinente de estos mecanismos, con graduación o umbrales tolerantes, que se revisen con regularidad y que gracias al feedback recibido, hagan el sistema más inteligente cada vez.

¿Cómo atenuar los errores?

Puede reducir la cantidad de falsos positivos y minimizar las interrupciones en la red implementando su IDS e IPS en etapas. Puede personalizar los disparadores, combinar condiciones de advertencia y crear alertas personalizadas. Al combinar las condiciones, se vuelven más complejas, lo que puede reducir la probabilidad de que se produzcan falsos positivos.

Sin embargo, es difícil erradicar los falsos positivos por completo sin correr el riesgo de que la actividad sospechosa se escape a través de sus defensas. Debe aspirar a lograr un equilibrio justo, sin comprometer su seguridad. Los procesos de detección y prevención de intrusiones deben poder interactuar con los firewalls de una manera ajustada, para

garantizar que los usuarios genuinos no estén bloqueados y la actividad de la red auténtica no se interrumpa.

Los IPS suelen registrar información relacionada con eventos observados, notificar a los administradores de seguridad sobre eventos observados importantes y generar informes. Muchos IPS también pueden responder a una amenaza detectada intentando evitar que tenga éxito. Utilizan diversas técnicas de respuesta, que implican que el IPS detenga el ataque en sí, cambie el entorno de seguridad o cambie el contenido del ataque.

Clasificación del sistema de prevención de intrusiones (IPS)

El sistema de prevención de intrusiones (IPS) se clasifica en 4 tipos:

Sistema de prevención de intrusiones basado en red (NIPS)

Monitorea toda la red en busca de tráfico sospechoso mediante el análisis de la actividad del protocolo.

Sistema inalámbrico de prevención de intrusiones (WIPS)

Monitorea una red inalámbrica en busca de tráfico sospechoso mediante el análisis de los protocolos de red inalámbrica.

Análisis del comportamiento de la red (NBA)

Examina el tráfico de la red para identificar amenazas que generan flujos de tráfico inusuales, como ataques distribuidos de denegación de servicio, formas específicas de malware y

violaciones de políticas.

Sistema de prevención de intrusiones basado en el host (HIPS)

Es un paquete de software incorporado que opera un solo host para actividades dudosas al escanear eventos que ocurren dentro de ese host.

El Hecho, la evidencia

No hay IPS sin IDS (Sistema de detección de intrusiones). IDS es el yang de IPS, como IPS es el yin de IDS. Dejando a un lado la poética, IDS es un dispositivo o incluso una pieza de software que monitorea activamente un sistema o red en busca de signos de violaciones de políticas o, lo que es relevante para este artículo, actividad maliciosa. Los datos recopilados por un IDS se pueden enviar a un SIEM (Sistema de gestión de eventos e información de seguridad).

¿Qué es un SIEM?

Los SIEM son la máquina de vapor proverbial de todo el esfuerzo de seguridad de la red: la información recopilada a nivel de SIEM se utilizará para crear informes procesables, reforzar la seguridad de la red, identificar brechas (de seguridad), minimizar el daño y, si corresponde, determinar el mejor curso de acción para erradicar el malware que pueda haber «excavado» en sus terminales.

IPS vs Firewall

Los IPS a veces se confunden con los firewalls, ya que ambos tienen algo que ver con la seguridad de la red. Por supuesto, no hace falta decir que los dos son diferentes, la principal diferencia entre los dos es la capacidad del IPS para detectar

amenazas tanto externas como internas.

Un IPS puede parecer más útil que un IDS simplemente porque «hace más», pero la **escucha pasiva del comportamiento de la red sigue siendo de vital importancia**.

Una gran cantidad de tráfico parece sospechoso pero, de hecho, es inocente, y si su herramienta siempre bloquea o reacciona automáticamente al tráfico, puede terminar con falsos positivos que interfieren con el tráfico normal de la red. En cualquier caso, debe configurar su IDS o IPS para minimizar los falsos positivos y negativos y garantizar la precisión con la mayor frecuencia posible.

¿Máquina o programas?

Los IPS pueden estar basados □□en hardware o software. Un honeypot es un gran ejemplo de IPS (e IDS) basado en hardware, sin embargo, un sistema de este tipo puede ser difícil y costoso de mantener. Por otro lado, los honeypots dominan el análisis de tráfico de red.

Método de detección del sistema de prevención de intrusiones (IPS)

Detección basada en firmas

El IDS basado en firmas opera paquetes en la red y los compara con patrones de ataque prediseñados y predeterminados conocidos como firmas.

Detección estadística basada en anomalías

Los IDS basado en anomalías supervisa el tráfico de la red y lo compara con una línea de base establecida. La línea de base identificará qué es normal para esa red y qué protocolos se utilizan. Sin embargo, puede generar una falsa alarma si las

líneas de base no se configuran de manera inteligente.

Detección de análisis de protocolo con estado

Este método IDS reconoce la divergencia de protocolos establecidos mediante la comparación de eventos observados con perfiles predefinidos de definiciones generalmente aceptadas de actividad no dañina.