¿Qué es un sistema de detección de intrusiones, IDS?

La seguridad web siempre está en boca de todos y hasta hace pocas semanas el eje de nuestro diálogo en el blog eran los firewalls, ahora vamos a dar una mirada diferente, complementaria si se quiere.

Lo que significa, funciones

Un sistema de detección de intrusiones (IDS) es una tecnología de seguridad de red construida originalmente para detectar vulnerabilidades contra una aplicación, computadora o servidor de destino.

Algunos IDS son capaces de responder a una intrusión detectada tras su descubrimiento. Se trata de un sistema que monitorea el tráfico de la red en busca de actividad sospechosa y emite alertas cuando se descubre dicha actividad. Es una aplicación de software que escanea una red o un sistema en busca de actividad dañina o incumplimiento de políticas.

Central

Cualquier empresa maliciosa o infracción normalmente se informa a un administrador o se recopila de forma centralizada mediante un sistema de gestión de eventos e información de seguridad (SIEM).

Un sistema SIEM integra salidas de múltiples fuentes y utiliza técnicas de filtrado de alarmas para diferenciar la actividad maliciosa de las falsas alarmas. Aunque los sistemas de

detección de intrusos monitorean las redes en busca de actividad potencialmente maliciosa, también están expuestos a falsas alarmas.

Comprobaciones

Por lo tanto, las organizaciones deben ajustar sus productos IDS cuando los instalan por primera vez. Significa configurar correctamente los sistemas de detección de intrusos para reconocer cómo se ve el tráfico normal en la red en comparación con la actividad maliciosa.

Los sistemas de prevención de intrusiones también monitorean los paquetes de red que ingresan al sistema para verificar las actividades maliciosas involucradas en él e inmediatamente envían las notificaciones de advertencia. Un IDS solo necesita detectar amenazas y, como tal, se coloca fuera de banda en la infraestructura de red, lo que significa que no se encuentra en la verdadera ruta de comunicación en tiempo real entre el remitente y el receptor de información. Más bien, las soluciones IDS a menudo aprovecharán un puerto TAP o SPAN para analizar una copia del flujo de tráfico en línea (y así garantizar que IDS no afecte el rendimiento de la red en línea).

TAP

Los TAP de red son un dispositivo de hardware especialmente diseñado, que se ubica en un segmento de red, entre dos dispositivos (enrutador, conmutador o firewall), y le permite acceder y monitorear el tráfico de la red. Los TAP transmiten los flujos de datos de envío y recepción simultáneamente en canales dedicados separados, lo que garantiza que todos los datos lleguen al dispositivo de monitoreo o seguridad en tiempo real.

Port Mirroring

También conocido como SPAN (Switch Port Analyzer), son puertos designados en un dispositivo de red (conmutador), que están programados para enviar una copia de los paquetes de red vistos en un puerto (o una VLAN completa) a otro puerto, donde los paquetes puede ser analizado.

Una vez que se han identificado las amenazas potenciales, el software de detección de intrusos envía notificaciones para alertarlo. El último software de IDS analizará e identificará proactivamente patrones indicativos de una variedad de tipos de ciberataques. Una solución eficaz debería poder descubrir cualquier amenaza antes de que se infiltre por completo en el sistema.

Más allá de los cortafuegos

Los firewalls y los programas anti-malware son solo una pequeña parte de un enfoque integral de seguridad. Cuando una red crece y los dispositivos nuevos o desconocidos entran y salen regularmente, necesita un software de detección de intrusos. Este software debe capturar instantáneas de todo su

sistema, utilizando el conocimiento de posibles intrusiones para prevenirlas de manera proactiva.

El software del sistema de detección de intrusiones generalmente se combina con componentes diseñados para proteger los sistemas de información como parte de una solución de seguridad más amplia. Una solución de seguridad completa también contará con medidas de control de acceso de autenticación y autorización como parte de su defensa contra intrusiones. Si bien esta es la función y el propósito básicos del software de detección de intrusos, no todos los programas son iguales.

Algunas le permiten implementar reglas, que luego el programa usa para informar y ejecutar ciertas acciones y tareas, mientras que otras no. Las opciones de IDS de código abierto también están disponibles, que pueden diferir significativamente del software de código cerrado, por lo que es importante comprender los matices de un sistema de detección de intrusiones de red de código abierto antes de elegirlo.

¿Qué hace un sistema de detección de intrusos?

Los sistemas de detección de intrusiones utilizan dos métodos: detección basada en firmas, que toma la actividad de los datos y la compara con una firma o patrón en la base de datos de firmas.

La detección basada en firmas tiene una restricción por la cual se ignora una nueva actividad maliciosa que no está en la base de datos. El otro método de detección es la detección estadística basada en anomalías o basada en el comportamiento, que, a diferencia de la basada en firmas, detecta cualquier anomalía y emite alertas; por tanto, detecta nuevos tipos de ataques. Se lo conoce como un sistema experto, ya que aprende

cuál es el comportamiento normal en el sistema.

IDS frente a sistemas de prevención de intrusiones frente a firewalls

Un IDS es un sistema de detección de intrusos , no un sistema diseñado para responder a un ataque . Un IDS puede ser parte de una herramienta de seguridad más grande con respuestas y remedios, pero el IDS en sí es simplemente un sistema de monitoreo.

Leer también: ¿Cuales son las diferencias entre un firewall y un antivirus? ; ¿Me conviene un firewall físico o uno lógico? ¿Hardware o software? ; ¿Qué es un Firewall como servicio, FWaaS? Ventajas