INCIDENTES DE CIBERSEGURIDAD

Unidad 1. Actividad 2

10 DE OCTUBRE DE 2023

CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

¿Qué son las herramientas IDS/IPS? 2

Utilidad de las mismas en Incidentes de Ciberseguridad 2

Principales herramientas IDS/IPS encontradas y características 3

¿Qué son las herramientas IDS/IPS?

IDS

Un sistema de detección de intrusos (IDS) se refiere a una aplicación de software o dispositivo para supervisar la red informática, las aplicaciones o los sistemas de una organización en busca de infracciones de las políticas y actividades maliciosas.

Hay dos tipos principalmente de IDS:

- Sistema de detección de intrusiones en la red (**NIDS**): el NIDS supervisa el flujo de tráfico que entra y sale de los dispositivos, lo compara con ataques conocidos y señala las sospechas.

- Sistema de detección de intrusiones basado en el host (**HIDS**): Supervisa y ejecuta archivos importantes en dispositivos independientes (hosts) en busca de paquetes de datos entrantes y salientes y compara las instantáneas actuales con las tomadas anteriormente para comprobar si se han borrado o modificado.

IPS

Un sistema de prevención de intrusiones (IPS) se refiere a una aplicación o dispositivo de software de seguridad de red para identificar actividades y amenazas maliciosas y prevenirlas. Dado que funciona tanto para la detección como para la prevención, también se denomina sistema de detección y prevención de identidades (IDPS).

Hay 4 tipos principales de IPS:

- Sistema de prevención de intrusiones basado en la red (**NIPS**): Analiza los paquetes de datos de una red para encontrar vulnerabilidades y prevenirlas.

- Sistema de prevención de intrusiones basado en host (**HIPS**): Ayuda a proteger los sistemas informáticos sensibles analizando las actividades de los hosts para detectar actividades maliciosas y prevenirlas.

- Análisis del comportamiento de la red (**NBA**): Depende de la detección de intrusiones basada en anomalías

- Sistema de prevención de intrusiones inalámbricas (**WIPS**): Supervisa el espectro radioeléctrico para comprobar el acceso no autorizado y toma medidas para enfrentarse a él.

Utilidad de las mismas en Incidentes de Ciberseguridad

Mientras que los IDS se centran en la detección y alerta de incidentes de ciberseguridad, los IPS van un paso más allá al tomar medidas activas para prevenir o mitigar esos incidentes en tiempo real. Ambos desempeñan un papel importante en la protección de la seguridad informática de una organización.

Las principales utilidades son automatización, los ataques de malware, ataques de phishing, intrusión en la red, ataques de fuerza bruta y ataques de denegación de servicios

Principales herramientas IDS/IPS encontradas y características

Zeek

Ofrece protocolos de análisis en profundidad que permiten un análisis semántico de alto nivel en la capa de aplicación. Está orientado a redes de alto rendimiento y funciona eficazmente en todos los sitios. Además, proporciona un archivo de actividad de red de alto nivel y es altamente estadístico. Zeek está operativo en todo el mundo y es totalmente gratuito

Snort

Este IPS utiliza un conjunto de reglas para definir la actividad maliciosa en la red y encontrar paquetes para generar alertas para los usuarios. Monitor de tráfico en tiempo real, registro de paquetes, análisis de protocolo, huellas digitales del SO, puede instalarse en cualquier entorno de red, crea registros, fuente abierta y las reglas son fáciles de implementar.

Analizador EventLog de ManageEngine

Gestión de logs, auditoría de aplicaciones, auditoría de dispositivos de red, gestión de cumplimiento de TI, análisis de seguridad, análisis de amenazas y auditoría multiplataforma

Security Onion

Una distribución Linux abierta y accesible para la supervisión de la seguridad empresarial, la gestión de registros y la caza de amenazas. Sus principales características son la detección de amenazas avanzadas, la escalabilidad, la capacidad de personalización, la integración con otras herramientas, y su comunidad de usuarios y desarrolladores.

Suricata

Combina la detección de intrusiones, la prevención de intrusiones, la supervisión de la seguridad de la red y el procesamiento PCAP para identificar y detener rápidamente los ataques más sofisticados. Sus características principales son:

- Multi-threading (multiprocesamiento).

- Soporte GPU (Cuda).

- Estadísticas de Rendimiento.

- Detección de Protocolos automáticos.

- Fast IP Matching (Coincidencia rápida de direcciones IP).

- IP Reputation, GeoIP, IP list support (Soporte para reputación de direcciones IP, GeoIP y listas de direcciones IP).

- Graphic Cards Acceleration (Aceleración mediante tarjetas gráficas).

- Soporta Lua Scripting.

FireEye

Ofrece una detección de amenazas superior y se ha ganado una reputación concreta como proveedor de soluciones de seguridad. Ofrece un sistema integrado de inteligencia dinámica de amenazas y prevención de intrusiones (IPS). Combina el análisis de código, el aprendizaje automático, la emulación y la heurística en una única solución y mejora la eficacia de la detección junto con la inteligencia de primera línea. Protección contra malware completamente integrada con defensas antivirus (AV), aprendizaje automático, análisis de comportamiento, indicadores de riesgo (IOC) y visibilidad del endpoint. Triage Summary y Audit Viewer para una inspección y análisis exhaustivos de las amenazas