**ANEXO IV**

**Práctica 4: Implementación de snort para IDS.**

**Trabajo preparatorio**

* **Explicar la diferencia entre IDS (Sistema de Detección de Intrusos) e IPS (Sistema de Prevención de Intrusos).**

Un IDS es una herramienta pasiva que supervisa y analiza el tráfico de red o las actividades del sistema para identificar comportamientos anómalos o no autorizados. Su propósito principal es detectar posibles amenazas y notificar a los administradores de seguridad, pero no actúa directamente para detenerlas. Esto permite a los expertos evaluar la situación y decidir cómo proceder. [50]

Por otro lado, un IPS es una solución activa que no solo identifica actividades maliciosas, sino que también toma medidas para bloquearlas automáticamente en tiempo real. Se implementa directamente en el flujo de tráfico de la red, permitiéndole interceptar y responder de inmediato a las amenazas, como eliminar paquetes maliciosos o bloquear direcciones IP sospechosas, sin necesidad de intervención manual. [50]

* **Consultar que es snort, para que sirve, arquitectura y sus componentes claves.**

Snort es un sistema de detección de intrusos en red (NIDS) de código abierto, creado en 1998 por Martin Roesch y actualmente gestionado por Cisco Systems. Esta herramienta es capaz de analizar el tráfico de red en tiempo real para detectar actividades sospechosas o maliciosas. Además, ofrece funcionalidades tanto para la detección de intrusiones (IDS) como para la prevención de intrusiones (IPS). [51]

Snort se utiliza para:

* Monitoreo de Tráfico en Tiempo Real: Inspecciona los paquetes de red en tiempo real, facilitando la detección de comportamientos inusuales o anómalos. [52]
* Detección de Intrusiones: Identifica intentos de acceso no autorizado, ataques de denegación de servicio (DoS), escaneos de puertos y otras actividades maliciosas en la red. [52]
* Prevención de Intrusiones: Además de detectar amenazas, Snort puede configurarse para bloquear o mitigar ataques en tiempo real, funcionando como un Sistema de Prevención de Intrusiones (IPS). [52]
* Registro de Paquetes: Guarda registros detallados del tráfico de red, útiles para análisis forense, auditorías de seguridad y revisión de incidentes. [52]

Los componentes claves de snort son los siguientes:

* Decodificador de paquetes: Se encarga de interpretar los paquetes entrantes, desglosándolos en sus componentes básicos para facilitar su análisis detallado. [53]
* Preprocesadores: Realizan análisis adicionales como la normalización de datos, detección y gestión de fragmentación de paquetes, y el reensamblado de flujos de datos. Estas tareas preparan la información para que el motor de detección trabaje de manera efectiva. [53]
* Motor de detección: Analiza el tráfico utilizando un conjunto de reglas definidas, buscando patrones que puedan indicar actividades maliciosas o no autorizadas. [53]
* Módulos de salida: Controlan cómo se registran y presentan las alertas generadas. Esto incluye opciones como guardar en archivos de registro, enviar a bases de datos o mostrar en tiempo real, según las necesidades del usuario. [53]
* **Investigar herramientas de Linux para la gestión de paquetes como apt y yum.**

**APT (Advanced Package Tool)**

APT es el sistema de gestión de paquetes estándar para distribuciones basadas en Debian, como Debian, Ubuntu y Linux Mint. Su principal función es simplificar la instalación, actualización y administración de software al resolver automáticamente las dependencias y manejar las versiones de los paquetes instalados. [54]

**YUM (Yellowdog Updater, Modified):**

YUM es el gestor de paquetes para distribuciones basadas en RPM, como CentOS, RHEL (Red Hat Enterprise Linux) y versiones anteriores de Fedora. Permite instalar, actualizar y eliminar software de manera sencilla, resolviendo automáticamente las dependencias entre los paquetes para garantizar una gestión eficiente del sistema. [54]