**PRÁCTICA N° 4**

Implementación de snort para IDS

1. **OBJETIVOS**
   1. Entender los conceptos básicos de IDS y cómo funcionan.
   2. Aprender a instalar y configurar Snort en un dispositivo con sistema operativo Linux.
   3. Crear y probar reglas personalizadas en Snort para detectar tráfico.
   4. Ejecutar Snort en modos IDS para evaluar su funcionalidad.
2. **MARCO TEÓRICO**
   1. **Snort**

Snort es una herramienta de código abierto para la detección y prevención de intrusiones (IDS/IPS) que permite monitorear y analizar el tráfico de red en tiempo real, contribuyendo a identificar y prevenir posibles vulnerabilidades de seguridad. Creada en 1998 por Martin Roesch, se ha consolidado como una de las soluciones IDS/IPS más utilizadas y eficaces hasta la fecha. Esta herramienta está diseñada para vigilar las redes en busca de actividades inusuales y alertar a los administradores de sistemas, permitiéndoles tomar medidas preventivas. Snort compara el tráfico de la red con un conjunto de reglas predefinidas para identificar patrones o comportamientos sospechosos que podrían ser indicativos de intrusiones o intentos de ataque. Además, ofrece la capacidad de bloquear activamente el tráfico malicioso antes de que alcance su destino, lo que la convierte en una solución poderosa para prevenir intrusiones.

Snort puede operar en tres modos principales:

* **Modo sniffer:** Este modo permite capturar y mostrar los paquetes de red en tiempo real directamente en la consola.
* **Modo registrador de paquetes:** En este modo, Snort almacena los paquetes capturados en el disco para su análisis posterior, facilitando la revisión detallada de actividades en la red.
* **Modo sistema de detección de intrusiones en red (NIDS):** Para este modo, Snort monitorea activamente el tráfico de la red y lo analiza utilizando un conjunto de reglas personalizables. En función de los resultados del análisis, puede tomar acciones específicas basadas en las actividades detectadas.

1. **TRABAJO PREPARATORIO**
   1. Consultar que es antivirus, su funcionamiento, y las principales clases de amenazas como virus, malware, etc.
   2. Explicar la diferencia entre IDS (Sistema de Detección de Intrusos) e IPS (Sistema de Prevención de Intrusos).
   3. Consultar que es snort, para que sirve, arquitectura y sus componentes claves.
   4. Investigar herramientas de Linux para la gestión de paquetes como apt y yum.
2. **EQUIPO Y MATERIALES**

* Oracle VM Virtual Box o VMWare Player.
* Máquina virtual con distribución Ubuntu/Debian que actúe como dispositivo Linux.
* Internet.

1. **PROCEDIMIENTO**

**Instalación de prerrequisitos**

* Primero se instalan las siguientes dependencias necesarias para ejecutar snort sin complicaciones con el comando sudo apt install build-essential libpcap-dev libpcre3-dev libnet1-dev zlib1g-dev luajit hwloc libdumbnet-dev bison flex liblzma-dev openssl libssl-dev pkg-config libhwloc-dev cmake cpputest libsqlite3-dev uuid-dev libcmocka-dev libnetfilter-queue-dev libmnl-dev autotools-dev libluajit-5.1-dev libunwind-dev libfl-dev -y.
* Después es necesario instalar DAQ, que es una biblioteca de obtención de datos para la salida y entrada de datos. Para ello se ejecutan los siguientes comandos:

git clone https://github.com/snort3/libdaq.git

cd libdaq

./bootstrap

./configure

make

sudo make install

* Por último, se instala la herramienta TCMalloc la cual se usa para administrar la memoria y agilizar en rendimiento de CPU. Para ellos, se usan los siguientes comandos.

cd ../

wget https://github.com/gperftools/gperftools/releases/download/gperftools-2.9.1/gperftools-2.9.1.tar.gz

tar xzf gperftools-2.9.1.tar.gz

cd gperftools-2.9.1/

./configure

make

sudo make install

**Descarga e instalación de snort3**

* Para descargar última versión de snort desde su sitio oficial con los siguientes comandos:

cd..

wget https://github.com/snort3/snort3/archive/refs/heads/master.zip

unzip master.zip

cd snort3-master

./configure\_cmake.sh --prefix=/usr/local --enable-tcmalloc

* Para instalar snort3 es necesario moverse al directorio snort3-master/build y luego ejecutar los comandos make, sudo make install.

A screenshot of a computer program

Description automatically generated

* Por último, se actualizan las bibliotecas con el comando sudo ldconfig y se verifica que este corriendo correctamente con el comando snort -V.

**Configuración de Snort**

* Para configurar snort, primero se crea los directorios necesarios para reglas y logs. Además, se dan los permisos adecuados con los siguientes comandos:

sudo mkdir /usr/local/etc/rules

sudo mkdir /usr/local/etc/so\_rules/

sudo mkdir /usr/local/etc/lists/

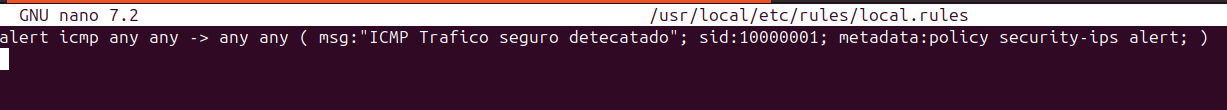
sudo touch /usr/local/etc/rules/local.rules

sudo touch /usr/local/etc/lists/default.blocklist

sudo mkdir /var/log/snort

* Después se crea una regla básica para detectar tráfico ICMP de la siguiente forma, con el comando sudo nano /usr/local/etc/rules/local.rules.

alert icmp any any -> any any ( msg:"ICMP Traffic Detected"; sid:10000001; metadata:policy security-ips alert; )



* Luego se configura el archivo snort.lua con el comando sudo nano /usr/local/etc/snort/snort.lua y se edita de la siguiente forma:

A screenshot of a computer program

Description automatically generatedA screenshot of a computer

Description automatically generated

* La línea include = RULE\_PATH .. "/local.rules", la cual se la configura para se tome la o las reglas creadas dentro del archivo local.rules.
* Se inicia snort y se carga el archivo local.rules con el siguiente comando snort -c /usr/local/etc/snort/snort.lua -R /usr/local/etc/rules/local.rules. De este modo se debe mostrar al final, el mensaje de la figura 2.52. para que no exista errores.

A black background with white text

Description automatically generated

1. **INFORME**
   1. Documentar las configuraciones aplicadas.
   2. Presentar las capturas de pantalla, con la debida explicación de los resultados mostrados. Además, indicar el impacto en la seguridad.
   3. Crear reglas de tal forma que los resultados sean ¨Trafico seguro¨ y ¨Trafico inseguro¨ para dos dispositivos específicos.
2. **REFERENCIAS**

**[1] "How to Install & Configure Snort on Ubuntu Linux?" Zenarmor. https://www.zenarmor.com/docs/linux-tutorials/how-to-install-and-configure-snort-on-ubuntu-linux#2---install-dependencies (accessed Jan 12. 2025).**

**[2] "Cómo Instalar y Configurar el Sistema de Detección de Intrusos Snort 3 en Ubuntu 22.04" Shapehost. https://shape.host/resources/como-instalar-y-configurar-el-sistema-de-deteccion-de-intrusos-snort-3-en-ubuntu-22-04 (accessed Jan 12. 2025).**