Caso de Estudio: Mini SOC Casero con Suricata, Zeek y EveBox

Autores: Ubernel Hernandez y Bug Hunter GPT

1. Arquitectura General del Mini SOC

Este proyecto se centró en la construcción de un **Mini SOC (Security Operations Center)** funcional utilizando herramientas *open-source* de grado profesional. La solución fue desplegada en una **máquina Linux endurecida**, configurada para la captura y el análisis de **tráfico real de la red** donde se alojaba.

---

2. Componentes Clave Utilizados

Componente	Función Principal
Suricata (IDS)	Motor de **Detección de Intrusiones** basado en reglas, análisis de protocolos y generación de eventos en formato JSON.
Zeek (NSM)	Motor de **Análisis de Comportamiento** y registro profundo de red (logs detallados de DNS, HTTP, SSL, conexiones, etc.).
EveBox (SIEM Ligero)	Plataforma de visualización estilo SIEM (Security Information and Event Management) para la **monitorización de eventos en tiempo real**.
Python + IA	Script de automatización para el **análisis de eventos y generación de Informes Ejecutivos** potenciados por Inteligencia Artificial.

3. Procedimiento de Instalación

Se detallan los comandos clave para el despliegue de los principales componentes:

Instalación de Suricata

```
sudo apt update && sudo apt upgrade -y
sudo apt install -y suricata
sudo suricata-update
suricata --version
```

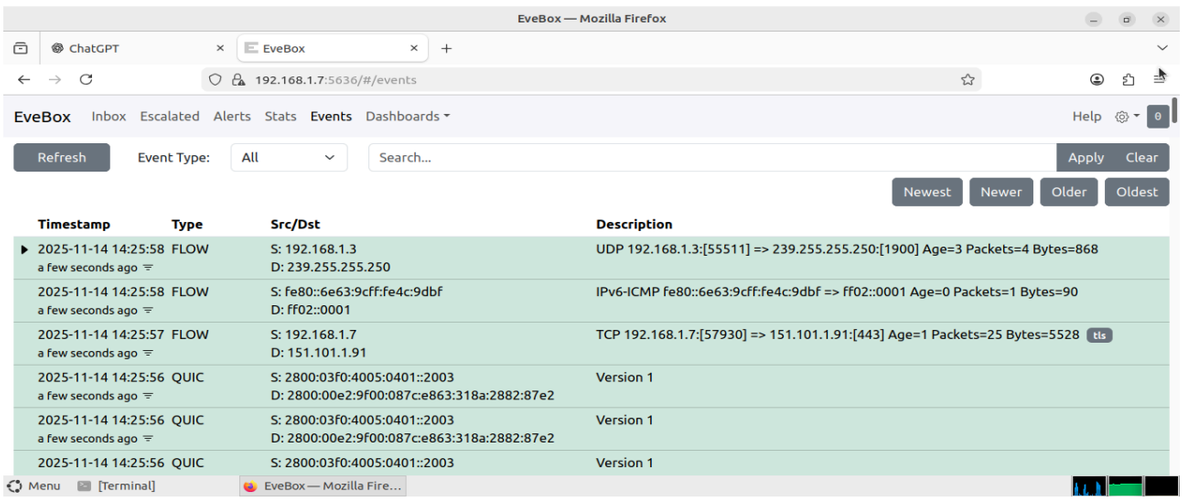
Instalación de Zeek

```
sudo apt install -y zeek
zeek --version
sudo zeek -i enp0s3 # Nota: La interfaz real de captura puede variar.
```

Instalación y Configuración de EveBox

wget https://evebox.org/files/evebox-latest-amd64.deb
sudo dpkg -i evebox-latest-amd64.deb
sudo evebox server -D -e /var/log/suricata/eve.json

Punto de Verificación: La configuración permite que la **Interfaz de EveBox** cargue y muestre los eventos generados por Suricata y Zeek en tiempo real.



---

4. Automatización con Inteligencia Artificial (IA)

Se implementó un script en **Python** diseñado para automatizar la labor del analista. Este script realiza:

1. Análisis del archivo de eventos (`eve.json`).
2. Resumen de la actividad de red e identificación de patrones de tráfico.
3. Generación de un **Informe Ejecutivo** mediante IA, que luego se reinserta como un evento dentro del SOC para su trazabilidad.

Ejemplo de Informe Ejecutivo Generado por IA

> **Informe Ejecutivo: Análisis Diario de Tráfico de Red**
>
> **Fecha del Análisis:** 13 de noviembre de 2025 **Analista:** OpenAI-SOC **Nivel de Severidad:** 1 (Bajo) **Tipo de Evento:** Análisis Diario SOC
>
> ## Resumen Ejecutivo de Tráfico de Red
>
> **A. Análisis de Tráfico:**
>
> - **Top IPs Activas (Anonimizadas):** Identificación de *hosts* internos con mayor volumen de conexiones (Ej: Host-Local-1 con 6136 conexiones).
> - **Tipos de Eventos Detectados:** DNS (11426 eventos), Flujo (4758 eventos), Estadísticas (4014 eventos).
>
> **B. Alertas Críticas Detectadas:**
>
> - **Ataque de Respuesta de ID (`GPL ATTACK_RESPONSE id check returned root`): Alerta de Máxima Prioridad** que sugiere un posible compromiso de sistema con la obtención de **privilegios de *root***. Requiere investigación inmediata.
> - **Actividad Relacionada con GNU/Linux APT:** Alertas recurrentes sobre el *User-Agent* de gestión de paquetes, indicando posible escaneo avanzado o intento de explotación de vulnerabilidades.

C. Prioridades de Riesgo y Recomendaciones:

- **Riesgo Crítico:** Investigar urgentemente la alerta `GPL ATTACK_RESPONSE` para verificar el acceso no autorizado.
- **Riesgo Alto:** Monitoreo intensivo de las IPs involucradas y **Verificación de Integridad de Sistemas** afectados por las alertas de GNU/Linux APT.

---

5. Resolución del Desafío Técnico

El mayor desafío del proyecto fue la **determinación precisa de la interfaz de red** que capturaba el tráfico real dentro del entorno de virtualización.

Problema a Resolver: Las configuraciones híbridas de VirtualBox (Bridge + NAT) y la coexistencia de múltiples interfaces (ej. `enp0s3`, `br0`, tráfico IPv6) dificultaban la identificación de la fuente de tráfico de la red física.

Solución Implementada: Se ejecutaron **análisis directos con `tcpdump` en cada interfaz** para verificar, en tiempo real, el flujo de paquetes entrantes y salientes. Una vez que se identificó y confirmó la interfaz correcta (**`br0`** en este caso), se configuró permanentemente en Suricata y Zeek, lo que permitió la captura de tráfico real y la visualización estable de eventos en EveBox.

---

6. Resultado Final del Proyecto

El Mini SOC desarrollado es una prueba de concepto que ofrece:

- **Detección de Intrusiones en Tiempo Real.**
- **Análisis de Comportamiento de Red Profundo.**
- **Visualización Avanzada de Eventos** mediante EveBox.
- **Generación Automatizada de Reportes Ejecutivos** asistida por IA.