Informe de Actividad del Honeypot

Este documento recoge la actividad registrada por el sistema honeypot conectado a Suricata. Se analizan los eventos detectados, las IPs más activas y los tipos de ataque observados.

Fecha de generación: 08/05/2025 18:27:55

# Resumen General

Total de eventos registrados: 32

IPs de origen únicas: 3

Tipos de eventos detectados:

* • dns: 8 eventos
* • alert: 21 eventos
* • http: 3 eventos

# Análisis por IP de Origen

## IP: unknown

Total de eventos: 20

Tipos de eventos:

* • alert: 20

Interpretación: La IP unknown ha generado múltiples eventos, lo que puede indicar una actividad automatizada como escaneo de puertos o pruebas de vulnerabilidades.

## IP: 192.168.86.35

Total de eventos: 8

Tipos de eventos:

* • dns: 8

Interpretación: La IP 192.168.86.35 ha generado múltiples eventos, lo que puede indicar una actividad automatizada como escaneo de puertos o pruebas de vulnerabilidades.

## IP: 127.0.0.1

Total de eventos: 4

Tipos de eventos:

* • alert: 1
* • http: 3

Interpretación: La IP 127.0.0.1 ha generado múltiples eventos, lo que puede indicar una actividad automatizada como escaneo de puertos o pruebas de vulnerabilidades.

# Eventos por Tipo

## DNS

Se han registrado 8 eventos de tipo dns.

Los eventos DNS pueden indicar intentos de reconocimiento de red o exfiltración de datos mediante dominios controlados por el atacante.

## ALERT

Se han registrado 21 eventos de tipo alert.

Este tipo de evento debe ser investigado según su naturaleza específica y frecuencia.

## HTTP

Se han registrado 3 eventos de tipo http.

Los eventos HTTP suelen estar relacionados con escaneos web, intentos de acceso a recursos inseguros o ejecución de comandos remotos.

# Conclusiones y Recomendaciones

Los datos obtenidos muestran actividad sospechosa en la red del honeypot. Se recomienda:

• Analizar las IPs con mayor número de eventos y considerarlas para listas de bloqueo.

• Monitorizar continuamente la red para detectar patrones de comportamiento repetitivo.

• Reforzar medidas de seguridad como firewalls o sistemas IDS adicionales.