

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: 14/05/2025 11:12:53

Resumen General

Total de eventos registrados: 375

IPs de origen únicas: 1

Tipos de eventos detectados:

- dns: 186 eventos
- http: 189 eventos

Análisis por IP de Origen

IP: 192.168.86.28

Total de eventos: 375

Tipos de eventos:

- dns: 186
- http: 189

Interpretación: La IP 192.168.86.28 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 186 eventos de tipo dns.

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

HTTP

Se han registrado 189 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.