

DOCUMENTO DE PROFUNDIZACIÓN

Teoría de la Información y la Comunicación

Laboratorio de análisis de entropía en tráfico de red

Laboratorio de análisis de entropía en tráfico de red

Objetivo: Analizar cómo la variación en la distribución de direcciones IP puede indicar comportamientos anómalos.

Escenario

Un sistema IDS registra solicitudes HTTP provenientes de las siguientes direcciones IP:

IP	Frecuencia
192.168.1.10	500
192.168.1.11	480
192.168.1.12	20

Actividades

1. Calcule la probabilidad de cada IP.
2. Determine la entropía del sistema.
3. Analice qué ocurre si una sola IP genera el 90% de las solicitudes.
4. Interprete los resultados desde el punto de vista de seguridad.