Fundamentos del análisis de tráfico

La seguridad de red es un conjunto de operaciones para proteger datos, aplicaciones, dispositivos y sistemas conectados a la red. Se considera uno de los subdominios más importantes de la ciberseguridad. Se centra en el diseño, la operación y la gestión de la arquitectura/infraestructura del sistema para garantizar la accesibilidad, integridad, continuidad y fiabilidad de la red. El análisis de tráfico (a menudo denominado análisis de tráfico de red) es un subdominio de la seguridad de red y su principal objetivo es investigar los datos de la red para identificar problemas y anomalías.
En esta sala se abordarán los fundamentos de la seguridad de red y el análisis de tráfico, y se presentarán los conceptos esenciales de estas disciplinas para ayudarle a iniciarse en el análisis de tráfico/paquetes. Le recomendamos completar el módulo " Fundamentos de red " antes de comenzar a trabajar en esta sala.

Tarea 1: Introducción
P: Lea la tarea anterior.
R: No se necesita respuesta

Tarea 2: Seguridad de la red y datos de red
P1: ¿Qué nivel de control de seguridad cubre la creación de políticas de seguridad?
R1: Administrative / Administrativo

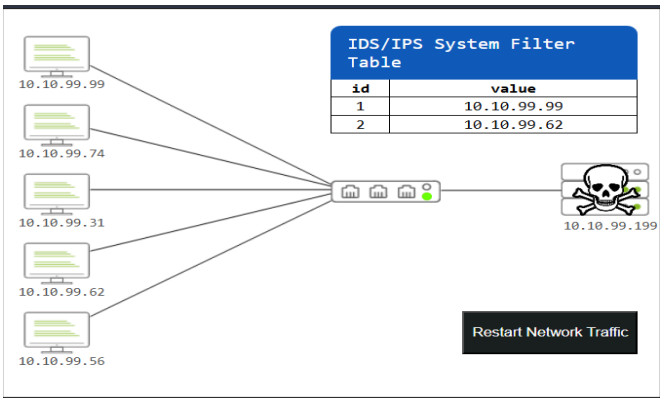
P2: ¿Qué elemento de control de acceso trabaja con métricas de datos para gestionar el flujo de datos?
R2: Load Balancing / Balanceo de Carga

P3: ¿Qué tecnología ayuda a correlacionar diferentes salidas de herramientas y fuentes de datos?
R3: SOAR

Tarea 3: Análisis de tráfico

P1: **El nivel 1** simula la identificación y el filtrado de direcciones IP maliciosas.

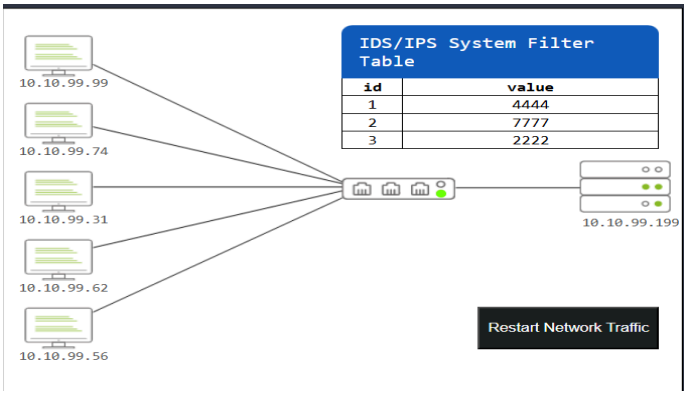
¿Qué es la bandera?



R1: THM{PACKET_MASTER}

P2: El nivel 2 simula la identificación y el filtrado de direcciones IP y puertos maliciosas.

¿Qué es la bandera?



R2: THM{DETECTION_MASTER}

Tarea 4: Conclusión

¡Felicitaciones! Acabas de completar la sección "Fundamentos del Análisis de Tráfico".

En esta sala cubrimos los fundamentos de los conceptos de seguridad de red y análisis de tráfico:

- Operaciones de seguridad de red
- Análisis del tráfico de red

Ahora, está listo para completar el módulo **"Seguridad de red y análisis de tráfico" .**

P: Lea la tarea anterior.
R: No se necesita respuesta

💼**LinkedIn:**https://www.linkedin.com/in/mateo-rodr%C3%ADguez-suar-202695249/
💻 **GitHub:** https://github.com/MaateoSuar