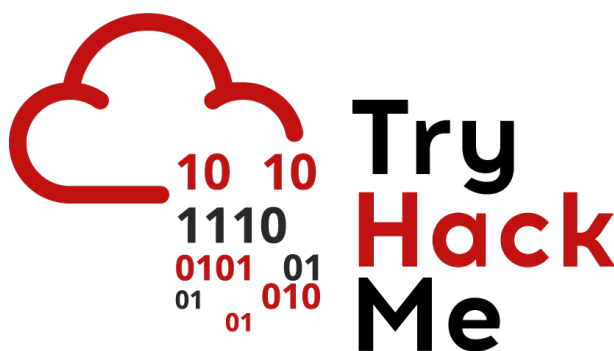


Writeup: Sala *Traffic Analysis Essentials*

Autor: Ismaeldevs

Plataforma: TryHackMe

4 de julio de 2025



Índice

1. Introducción	2
2. Sala	2
2.1. Tarea 1 – Introducción	2
2.2. Tarea 2 - Seguridad de la red y datos de red	2
2.3. Tarea 3 - Análisis de tráfico	3
2.4. Tarea 4 - Conclusión	8
3. Conclusión sobre la Sala	9

1. Introducción

En esta sala forma parte del módulo introductorio del camino de SOC Level 1 en TryHackMe y tiene como objetivo brindar una comprensión fundamental sobre el análisis de tráfico en redes. Aprenderemos los conceptos esenciales de seguridad en redes, los distintos tipos de datos que circulan por una red y cómo interpretarlos para detectar amenazas o comportamientos extraños.

2. Sala

2.1. Tarea 1 – Introducción

En esta primera tarea se define **Network Security** como el conjunto de prácticas para proteger datos, aplicaciones, dispositivos y sistemas en una red, asegurando disponibilidad, integridad, continuidad y confiabilidad.

Respuesta: **No requiere respuesta** (Hacemos clic en **Submit**).

2.2. Tarea 2 - Seguridad de la red y datos de red

Vamos a profundizar en dos temas esenciales los cuales son **Redes y Seguridad de datos** los cuales explica la autenticación y autorización como pilares del control de acceso. Además, conoceremos tres niveles de control de seguridad:

- **Físico**
- **Técnico**
- **Administrativo**

Por último, aprenderemos sobre dos enfoques principales que son **Control de Acceso** y el **Control de amenazas**.

Una vez que aprendemos sobre seguridad de la red y datos de red, procedemos a responder las siguientes preguntas.

Pregunta: Which Security Control Level covers contain creating security policies?

Respuesta: **Administrative**

Pregunta: Which Access Control element works with data metrics to manage data flow?

Respuesta: **Load Balancing**

Pregunta: Which technology helps correlate different tool outputs and data sources?

Respuesta: **SOAR**

2.3. Tarea 3 - Análisis de tráfico

Aprenderemos sobre qué es el **análisis de tráfico de red** (interceptar, registrar y examinar datos y patrones para identificar anomalías, problemas de rendimiento y amenazas). Sus beneficios claves e identifica como técnica fundamental en disciplinas como análisis de paquetes (Wireshark), monitoreo (Zeek), forense de red, detección de intrusiones y caza de amenazas. Se mencionan dos técnicas principales:

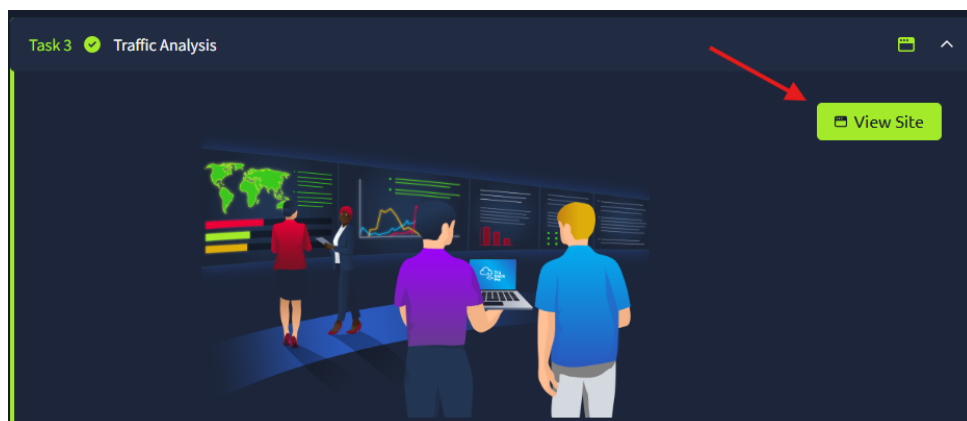
1. Flow Analysis

2. Packet Analysis

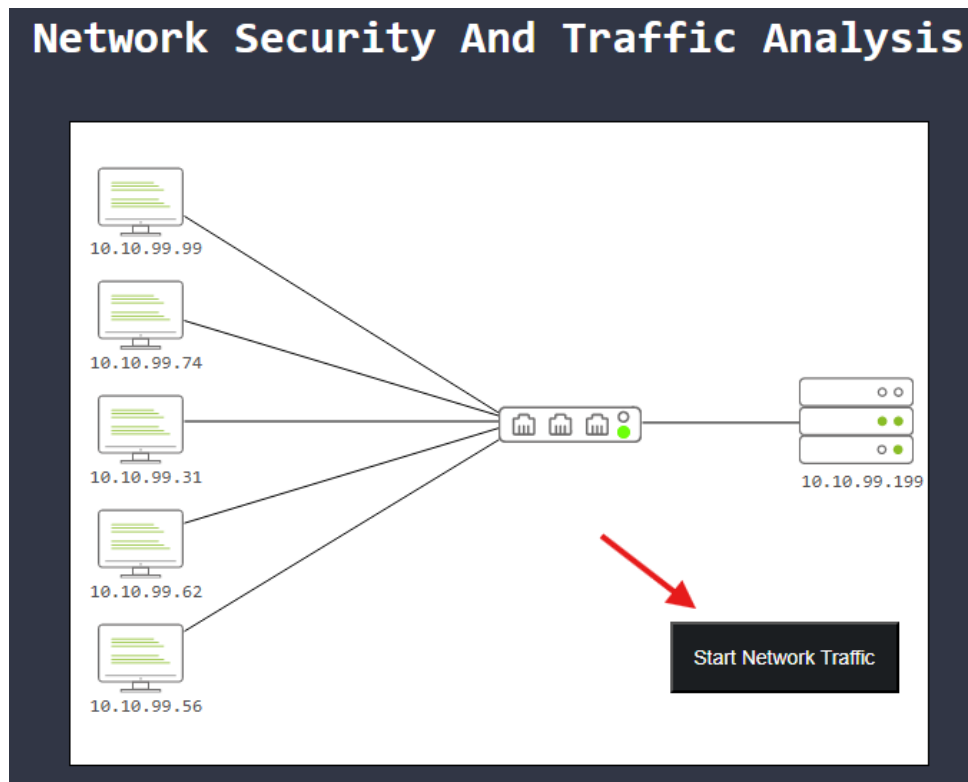
Después de entender el **análisis de tráfico**, procedemos a realizar una práctica para completar la tarea.

Level-1 is simulating the identification and filtering of malicious IP addresses.

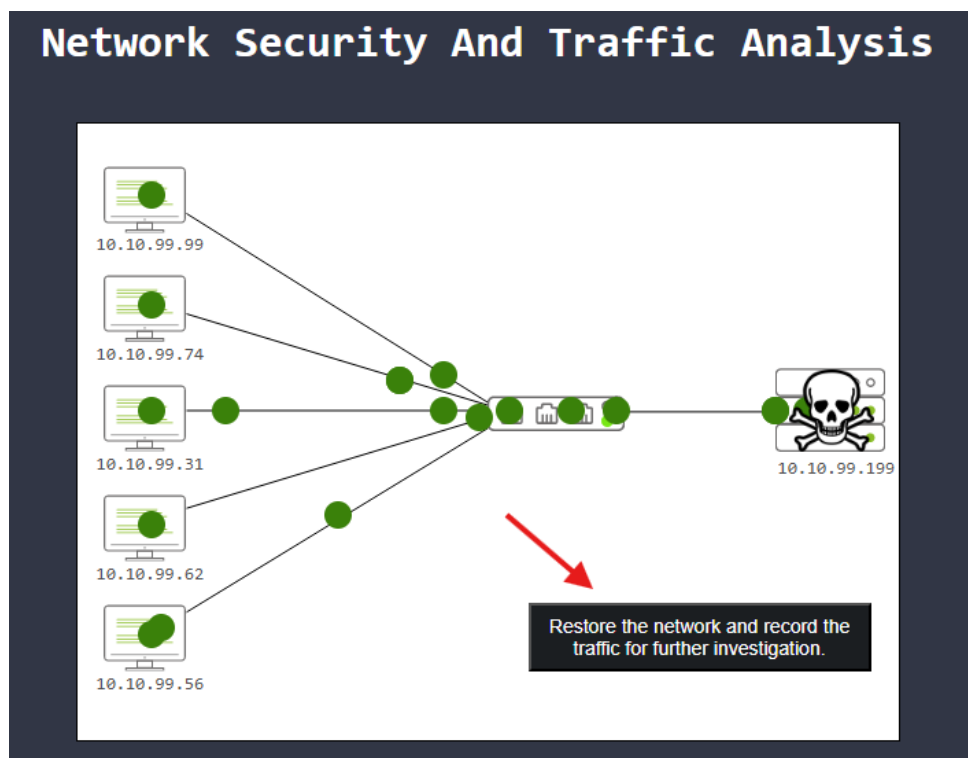
Antes de comenzar, debemos desplegar el sitio haciendo clic en **View Site** que se encuentra en el lado superior de la tarea.



Una vez en el sitio, haremos clic en **Start Network Traffic** para empezar con el tráfico de red.

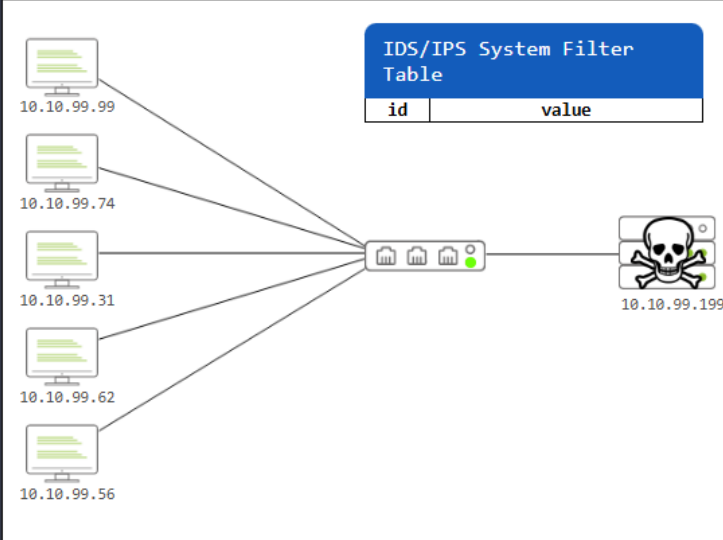


Ahora, vamos a restaurar la red y registrar el tráfico para una investigación posterior, para ello, haremos clic en **Restore the network and record the traffic for further investigation**



Ahora debemos analizar los datos registrados e ingresar dos IP sospechosas para que el Firewall las filtre de la red.

Network Security And Traffic Analysis



IDS/IPS System Filter Table

id	value

Instructions
 Analyse the data below and enter **2 IP addresses** for the firewall to filter.

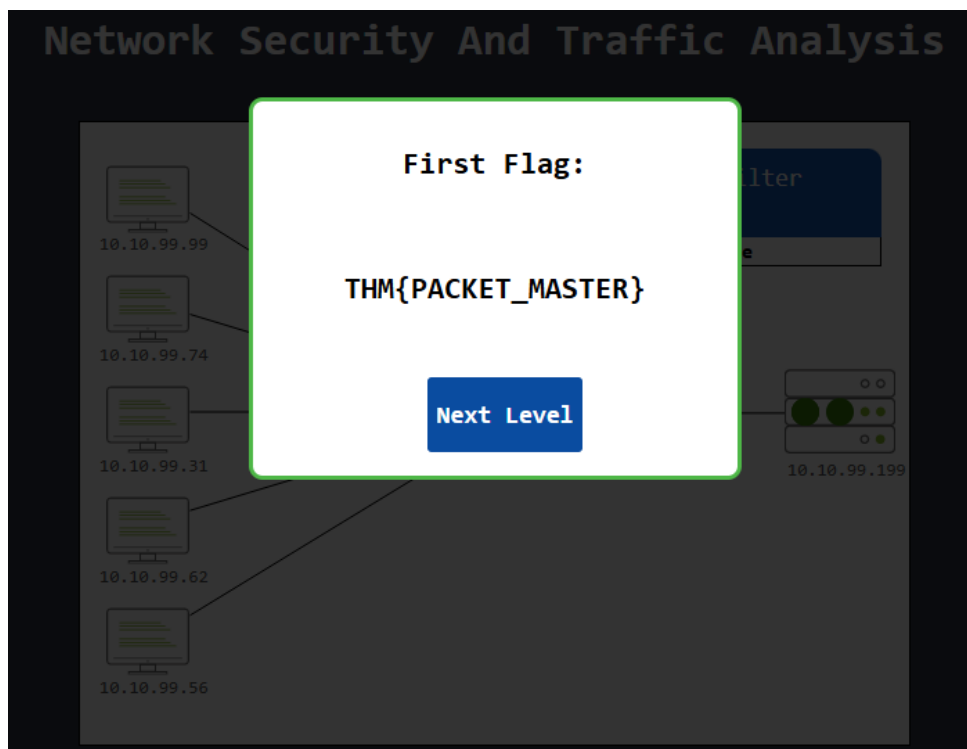
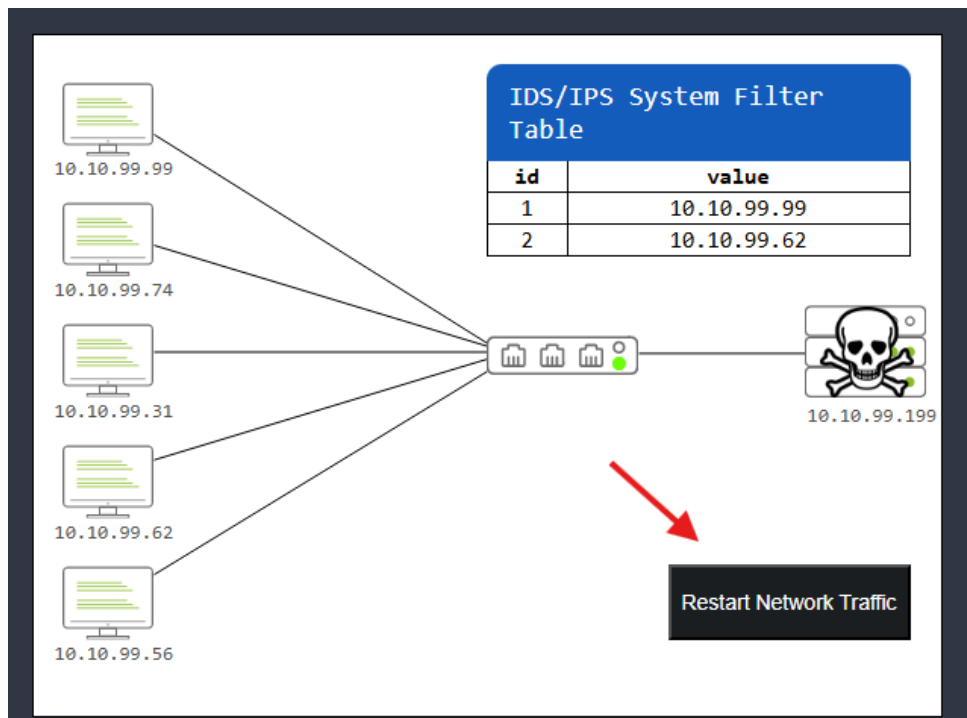
Traffic Analyser	
1	10.10.99.199:2999 10.10.99.99:4444
2	10.10.99.29:59635 10.10.99.199:445
3	10.10.99.62:13698 10.10.99.199:7777
4	10.10.99.99:35987 10.10.99.199:21
5	10.10.99.31:18695 10.10.99.199:3689
6	10.10.99.74:63587 10.10.99.199:2222
7	10.10.99.56:45986 10.10.99.199:8080
8	10.10.99.16:24985 10.10.99.199:3306

IDS/IPS System	
1	10.10.99.16 Corporate Policy Violation
2	10.10.99.29 P2P Usage
3	10.10.99.31 Social Media Usage
4	10.10.99.99 Multiple Login Attempts
5	10.10.99.74 Suspicious ARP Behaviour
6	10.10.99.62 Bad Traffic
7	10.10.99.56 Protocol Other
8	10.10.99.99 Metasploit Traffic

1. **10.10.99.99**

2. **10.10.99.62**

Después que agregamos las IP sospechosas para que las filtre el Firewall, podemos hacer clic en **Restart Network Traffic**



Respuesta: **THM{PACKET_MASTER}**

Hemos logrado conseguir la primera flag, ahora debemos conseguir la segunda para completar la tarea.

Level-2 is simulating the identification and filtering of malicious IP and Port addresses.

Para lograr completar esta segunda fase, debemos ingresar 3 puertos para bloquear y evitar que el servidor se vea comprometido. Para ello, analizaremos los registros del tráfico de red.

The screenshot displays the 'SALA' room interface. At the top, a diagram shows five client machines (IPs: 10.10.99.99, 10.10.99.74, 10.10.99.31, 10.10.99.62, 10.10.99.56) connected to a central switch, which is then connected to a server (IP: 10.10.99.199). An 'IDS/IPS System Filter Table' is shown with columns 'id' and 'value'.

Below the diagram, an 'Instructions' box states: "This time instead of IP addresses select **3 destination ports** to block to stop the server getting compromised."

The 'Traffic Analyser' table shows the following data:

	Source IP:Port	Destination IP:Port
1	10.10.99.199:2999	10.10.99.99:4444
2	10.10.99.29:59635	10.10.99.199:445
3	10.10.99.62:13698	10.10.99.199:7777
4	10.10.99.99:35987	10.10.99.199:21
5	10.10.99.31:18695	10.10.99.199:3689
6	10.10.99.74:63587	10.10.99.199:2222
7	10.10.99.56:45986	10.10.99.199:8080
8	10.10.99.16:24985	10.10.99.199:3306

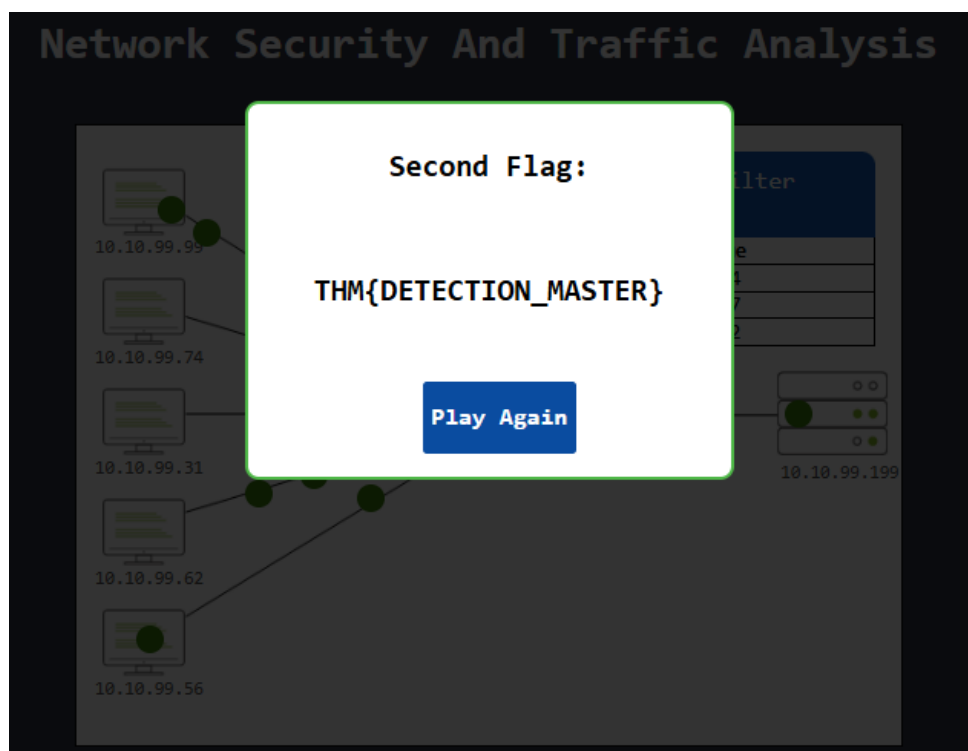
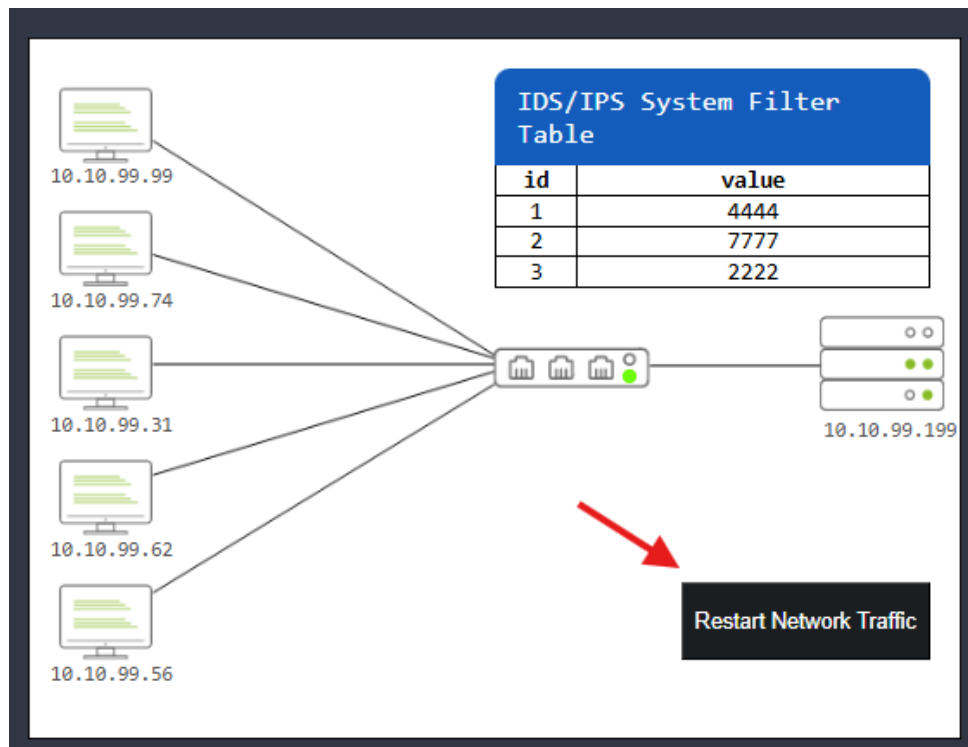
The 'IDS/IPS System' table shows the following data:

	IP Address	Event Description
1	10.10.99.16	Corporate Policy Violation
2	10.10.99.29	P2P Usage
3	10.10.99.31	Social Media Usage
4	10.10.99.99	Multiple Login Attempts
5	10.10.99.74	Suspicious ARP Behaviour
6	10.10.99.62	Bad Traffic
7	10.10.99.56	Protocol Other
8	10.10.99.99	Metasploit Traffic

At the bottom, there is a text input field labeled 'Enter Suspicious Port Here' and a blue button labeled 'Add To Filter'.

1. 4444
2. 7777
3. 2222

Una vez que agregamos los puertos correspondientes, haremos clic en **Restart Network Traffic**



Respuesta: **THM{DETECTION_MASTER}**

2.4. Tarea 4 - Conclusión

En esta última tarea resume lo aprendido sobre fundamentos de **operaciones de seguridad en redes y análisis de tráfico**.

Respuesta: **No requiere respuesta** (Hacemos clic en **Submit**).

3. Conclusión sobre la Sala

Una vez que finalizamos, hemos logrado comprender los diferentes niveles de control de seguridad, los enfoques para gestionar amenazas, y las técnicas empleadas para observar y analizar el comportamiento de los datos en tránsito.