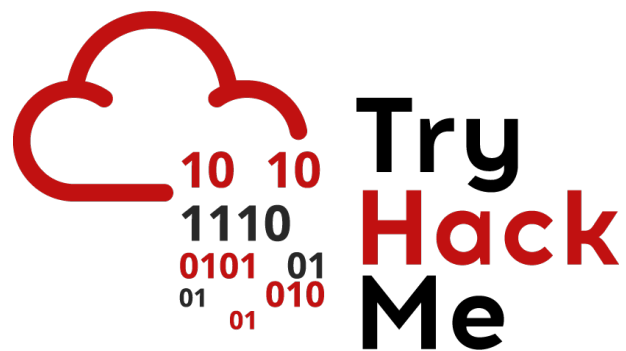


# Writeup: Sala *Intro to Endpoint Security*

Autor: Ismaeldevs

Plataforma: TryHackMe

4 de julio de 2025



## Índice

<b>1. Introducción</b>	<b>2</b>
<b>2. Sala</b>	<b>2</b>
2.1. Tarea 1 – Introducción . . . . .	2
2.2. Tarea 2 - Fundamentos de seguridad de endpoints . . . . .	2
2.3. Tarea 3 - Registro y monitoreo de endpoint . . . . .	2
2.4. Tarea 4 - Análisis de registros de endpoint . . . . .	3
2.5. Tarea 5 - Conclusión . . . . .	6
<b>3. Conclusión sobre la Sala</b>	<b>6</b>

# 1. Introducción

Esta sala logra proporcionar una comprensión básica pero esencial sobre la seguridad en endpoints dentro de entornos Windows. Aprenderemos a identificar procesos críticos del sistema, monitorizar actividad sospechosa, interpretar logs generados por el sistema operativo y herramientas de terceros, así como aplicar técnicas de análisis y respuesta ante incidentes.

## 2. Sala

### 2.1. Tarea 1 – Introducción

En esta primera tarea presenta las bases de la monitorización de seguridad en endpoints. Entenderemos que se repasarán herramientas, procesos y una metodología básica para identificar actividades maliciosas en dispositivos finales, preparando el terreno para el ejercicio final de investigación simulada.

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

### 2.2. Tarea 2 - Fundamentos de seguridad de endpoints

Aprenderemos sobre cómo funciona internamente Windows, identificando procesos críticos (como wininit.exe, services.exe, svchost.exe, lsass.exe, etc).

También se presentan herramientas como **Sysinternals**, en especial **TCPView** (para monitorear conexiones de red) y **Process Explorer** (para inspeccionar procesos, DLLs, handles, servicios, etc).

Ahora, procederemos a responder las siguientes preguntas.

**Pregunta:** What is the normal parent process of services.exe?

**Respuesta:** **wininit.exe**

**Pregunta:** What is the name of the network utility tool introduced in this task?

**Respuesta:** **TCPView**

### 2.3. Tarea 3 - Registro y monitoreo de endpoint

Profundizaremos en la recopilación de datos desde endpoints. Vamos a aprender sobre el funcionamiento de los **Windows Event Logs** (.evtx) y las formas de acceder a ellos (Event Viewer, wevtutil.exe, Get-WinEvent).

Luego conoceremos **Sysmon** (para registro detallado de eventos de seguridad) y herramientas como **OSQuery** (para consultar estado del sistema con SQL). Además, se menciona **Wazuh** como solución EDR/SIEM que centraliza y analiza logs de endpoints.

Una vez que entendemos los registros y monitoreo de endpoint, pasamos a responder las siguientes preguntas.

**Pregunta:** Where do the Windows Event logs (.evtx files) typically reside?

**Respuesta:** **C:32**

**Pregunta:** Provide the command used to enter OSQuery CLI.

**Respuesta:** **osqueryi**

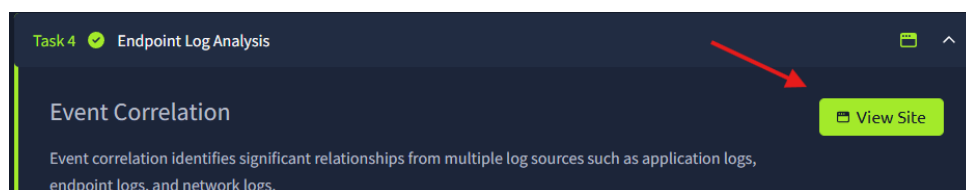
**Pregunta:** What does EDR mean? Provide the answer in lowercase.

**Respuesta:** **endpoint detection and response**

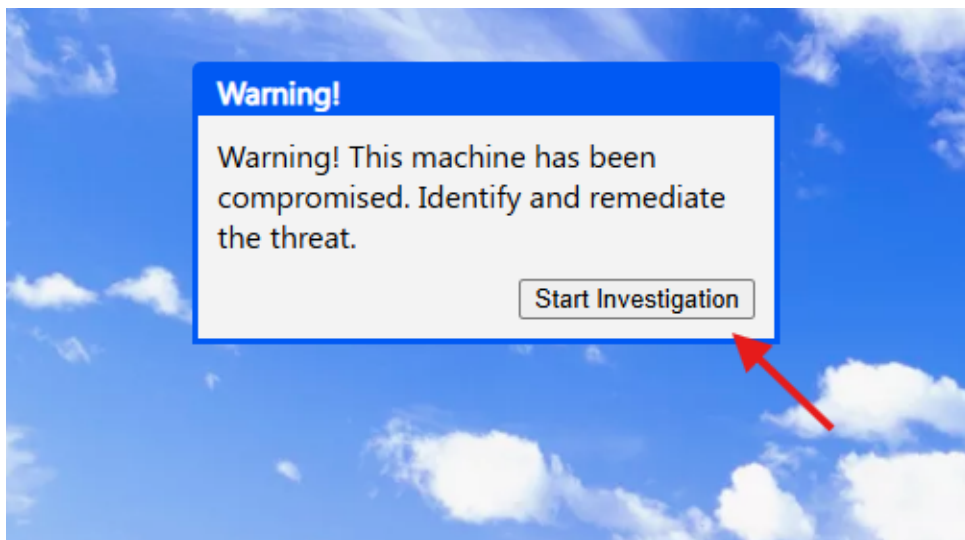
## 2.4. Tarea 4 - Análisis de registros de endpoint

Vamos a aprender las metodologías para analizar registros como **baselining** (definir comportamiento normal de procesos, conexiones y usuarios) y **event correlation** (vincular registros de distintas fuentes).

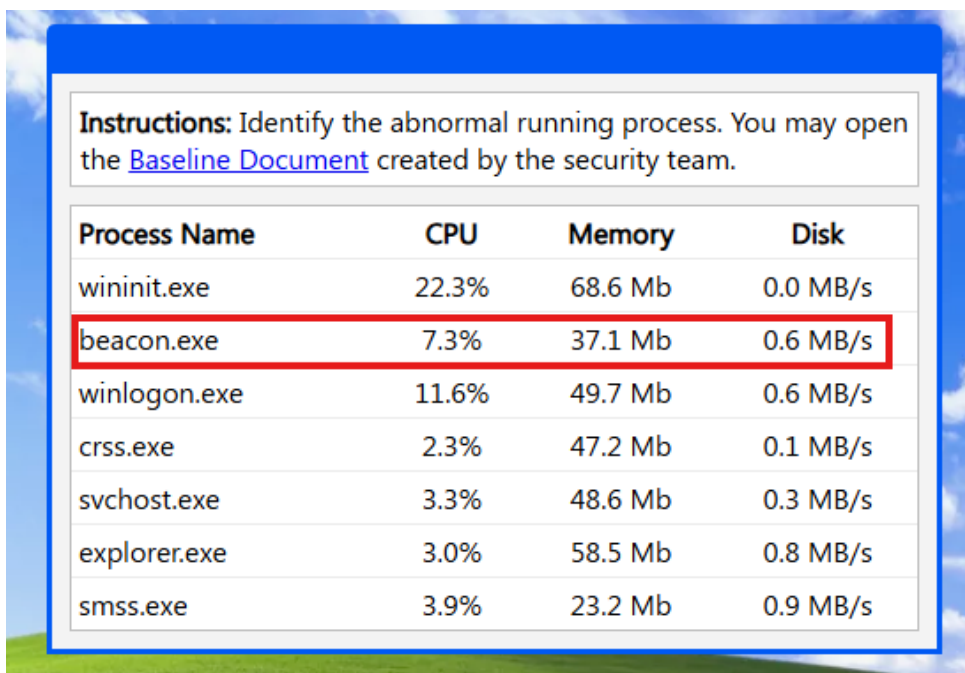
Para completar esta tarea debemos completar un laboratorio, para ello, desplegaremos el sitio que se encuentra en el lado superior de la tarea y haremos clic en **View Site**



Ahora, realizaremos los pasos correspondientes para completar el laboratorio. Comenzaremos haciendo clic en **Start Investigation**.



Una vez hecho eso, se nos abra una ventana con múltiples procesos y debemos seleccionar el proceso sospechoso.

A window with a blue border and a white background. It contains a table of running processes. The table has four columns: Process Name, CPU, Memory, and Disk. The row for 'beacon.exe' is highlighted with a red border. Above the table, there is a text box with instructions: "Instructions: Identify the abnormal running process. You may open the [Baseline Document](#) created by the security team." The background of the image is a blue sky with white clouds.

Process Name	CPU	Memory	Disk
wininit.exe	22.3%	68.6 Mb	0.0 MB/s
beacon.exe	7.3%	37.1 Mb	0.6 MB/s
winlogon.exe	11.6%	49.7 Mb	0.6 MB/s
crss.exe	2.3%	47.2 Mb	0.1 MB/s
svchost.exe	3.3%	48.6 Mb	0.3 MB/s
explorer.exe	3.0%	58.5 Mb	0.8 MB/s
smss.exe	3.9%	23.2 Mb	0.9 MB/s

Una vez que identificamos el proceso malicioso, pasaremos a la siguiente etapa donde debemos determinar el tráfico de red malicioso.

**Notes**

Malicious process:  
beacon.exe

**Instruction:** Based on the identified malicious process, determine the malicious network traffic. You may refer to your notes.

Process Name	Process ID	Remote Address	Remote Port
svchost.exe	2031	time.windows.com	443
svchost.exe	1023	52.242.211.89	443
beacon.exe	6823	59.23.48.195	4444

Posterior a eso, pasaremos a un siguiente escenario donde debemos ingresar la IP maliciosa en el buscador para buscar todas las máquinas afectadas.

**Notes**

Malicious process:  
beacon.exe

Malicious IP Address:  
59.23.48.195

**Instruction:** Find all machines affected using the discovered IP address and eradicate the threat.

Search:

**Notes**

Malicious process:  
beacon.exe

Malicious IP Address:  
59.23.48.195

**Instruction:** Find all machines affected using the discovered IP address and eradicate the threat.

Search:

Ahora que encontramos las máquinas afectadas, simplemente haremos clic en la acción de **Remediate** y finalizaremos la práctica una vez hecho eso.

**Notes**

Malicious process:  
beacon.exe

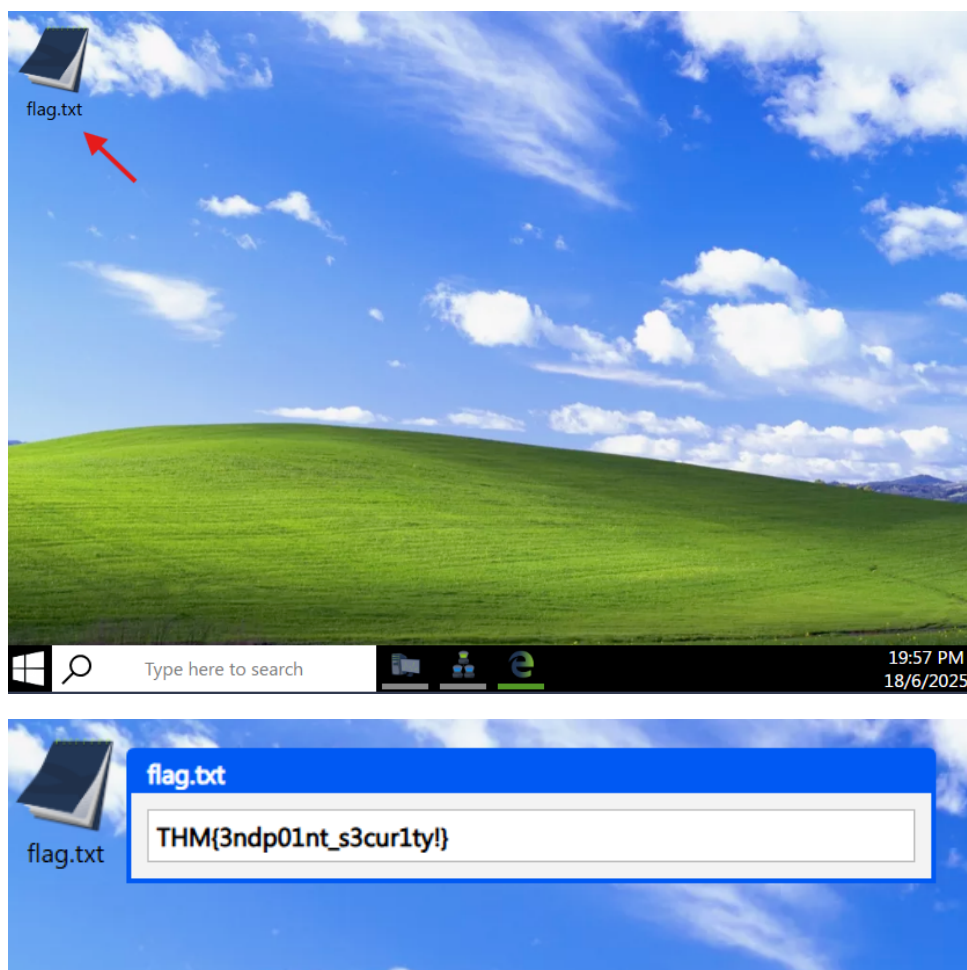
Malicious IP Address:  
59.23.48.195

**Instruction:** Find all machines affected using the discovered IP address and eradicate the threat.

Search:

Computer Name	Remote IP Address	Action
WKSTN-1	59.23.48.195	<input type="button" value="Remediate"/>
WKSTN-2	59.23.48.195	<input type="button" value="Remediate"/>
WKSTN-3	59.23.48.195	<input type="button" value="Remediate"/>
WKSTN-4	59.23.48.195	<input type="button" value="Remediate"/>

Por último, aparecerá un bloc de notas llamado **flag.txt** la cual haremos clic para visualizar la flag que necesitamos para finalizar la tarea.



Respuesta: **THM{3ndp01nt\_s3cur1ty!}**

## 2.5. Tarea 5 - Conclusión

Está última tarea es un resumen de los aprendizajes claves como la importancia de una línea base, el uso de correlación de eventos para reconstruir ataques, documentar artefactos relevantes y remediar sistemas afectados.

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

## 3. Conclusión sobre la Sala

Una vez que finalizamos hemos logrado obtener una visión clara sobre cómo funcionan los procesos fundamentales de Windows y cómo pueden ser utilizados tanto para operar el sistema como para detectar actividad maliciosa. Se exploran herramientas clave como **Sysinternals**, **Sysmon** y **OSQuery** para la observación detallada del

sistema, y se practica el análisis de logs reales mediante técnicas como el baselining y la correlación de eventos.