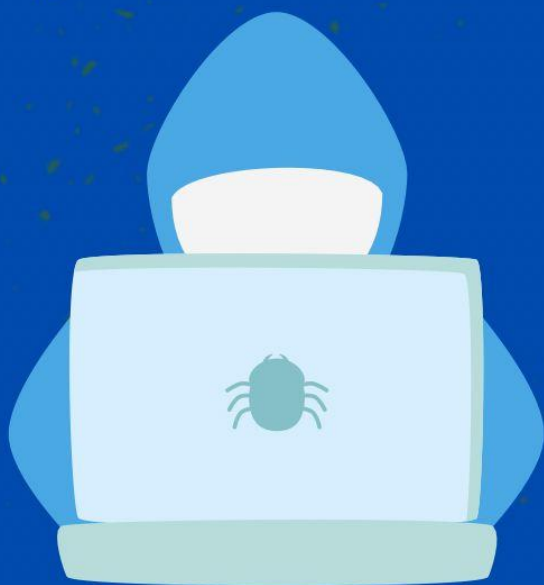


# Santalog8



ADRIÀ

# 1 CONTENIDO

---

2	Introducción .....	3
3	Objetivo.....	3
4	Plantemaiento .....	3
5	Logs .....	4
6	Obteniendo la flag.....	8

## 2 INTRODUCCIÓN

---

En el CTF SantaLogs de TheHackerLabs, tuve la oportunidad de poner a prueba mis conocimientos en ciberseguridad, enfocándome en el análisis forense digital y la investigación de registros de eventos (logs).

El reto se basaba en un escenario en el que Santa Claus había detectado actividad sospechosa en sus servidores, lo que ponía en peligro la entrega de regalos de Navidad. Mi objetivo era asumir el rol de analista de seguridad, investigar los incidentes y descubrir qué había sucedido mediante el análisis de logs y la identificación de posibles ataques.

## 3 OBJETIVO

---

Mi objetivo en esta máquina es poner en práctica y reforzar mis habilidades en ciberseguridad, centrándome en el análisis forense digital y la interpretación de logs. A lo largo del desafío, busco identificar posibles ataques, rastrear actividades sospechosas y comprender las técnicas utilizadas por los atacantes para comprometer los sistemas.

Para ello, analizaré registros de eventos, aplicaré metodologías forenses y utilizaré diversas herramientas de seguridad con el fin de recopilar evidencias, identificar patrones y extraer conclusiones que permitan resolver cada uno de los retos planteados.

## 4 PLANTEAMIENTO

---

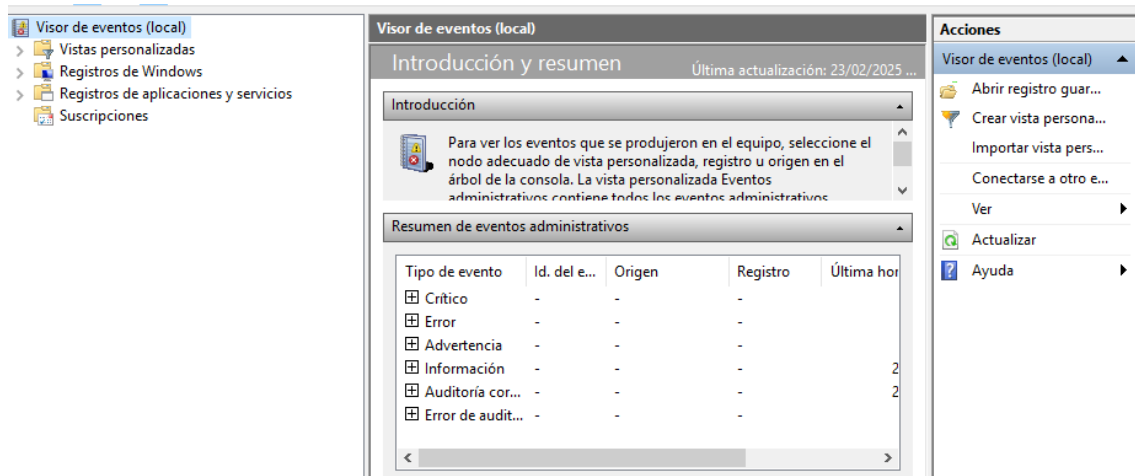
Dado que mi conocimiento es nulo en CTFs forenses, el primer camino que tomaré será analizar los registros de eventos disponibles. A través de la revisión de logs, intentaremos identificar actividades sospechosas, patrones anómalos o cualquier indicio de un posible ataque.

Si no encuentro información concluyente en los registros iniciales, procederé a realizar una búsqueda más exhaustiva en fuentes externas, recurriendo a técnicas de

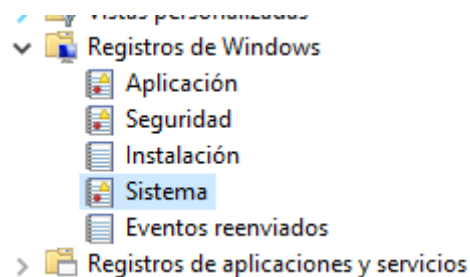
## 5 LOGS

Para empezar, así como nos dicen en el texto de entrada que nos viene dado en el PDF tenemos que mirar los logs para ver si podemos detectar alguna actividad maliciosa.

Para ello, buscaremos “Visor de eventos” y entraremos para ver los logs del sistema.



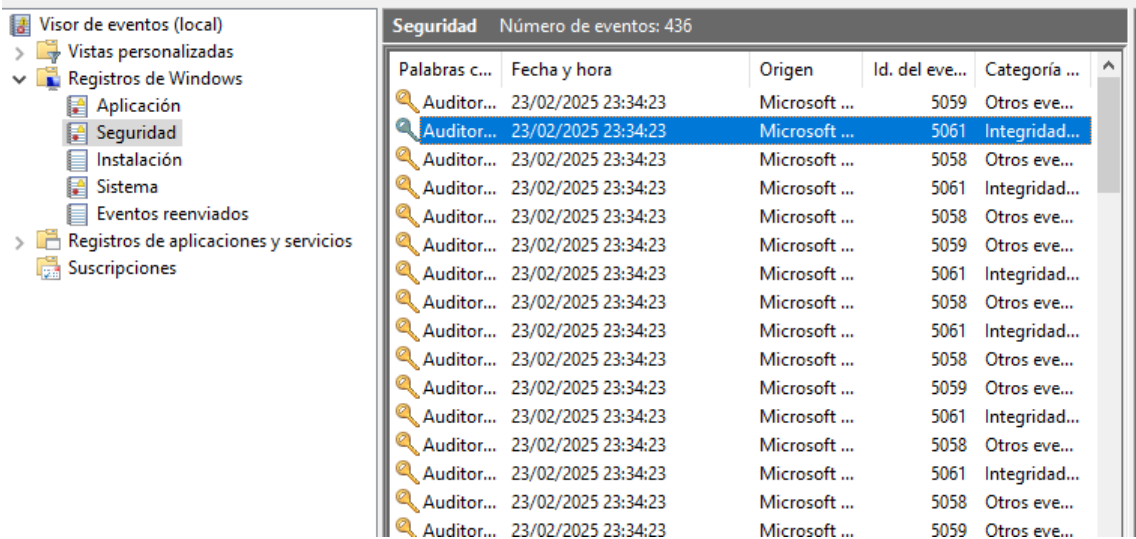
Si desplegamos el apartado de “Registros de Windows”, veremos los siguientes apartados:



1. Aplicación: Contiene eventos generados por aplicaciones y programas instalados en el sistema.
2. Seguridad: Contiene eventos relacionados con la seguridad del sistema, como intentos de inicio de sesión, cambios de permisos y actividades de auditoría.

3. Sistema: Contiene eventos generados por el sistema e incluye información sobre el inicio y apagado del sistema, fallos de hardware....

Una vez que sabemos esto vamos a mirar un poco por encima los logs que nos presenta la máquina.

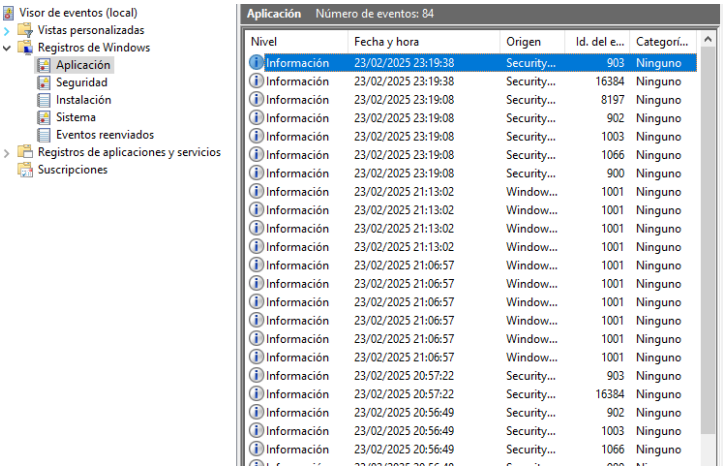


Visor de eventos (local)

- Vistas personalizadas
- Registros de Windows
  - Aplicación
  - Seguridad
  - Instalación
  - Sistema
  - Eventos reenviados
- Registros de aplicaciones y servicios
- Suscripciones

**Seguridad** Número de eventos: 436

Palabras c...	Fecha y hora	Origen	Id. del eve...	Categoría ...
Auditor...	23/02/2025 23:34:23	Microsoft ...	5059	Otros eve...
Auditor...	23/02/2025 23:34:23	Microsoft ...	5061	Integridad...
Auditor...	23/02/2025 23:34:23	Microsoft ...	5058	Otros eve...
Auditor...	23/02/2025 23:34:23	Microsoft ...	5061	Integridad...
Auditor...	23/02/2025 23:34:23	Microsoft ...	5058	Otros eve...
Auditor...	23/02/2025 23:34:23	Microsoft ...	5059	Otros eve...
Auditor...	23/02/2025 23:34:23	Microsoft ...	5061	Integridad...
Auditor...	23/02/2025 23:34:23	Microsoft ...	5058	Otros eve...
Auditor...	23/02/2025 23:34:23	Microsoft ...	5061	Integridad...
Auditor...	23/02/2025 23:34:23	Microsoft ...	5058	Otros eve...
Auditor...	23/02/2025 23:34:23	Microsoft ...	5059	Otros eve...
Auditor...	23/02/2025 23:34:23	Microsoft ...	5061	Integridad...
Auditor...	23/02/2025 23:34:23	Microsoft ...	5058	Otros eve...
Auditor...	23/02/2025 23:34:23	Microsoft ...	5059	Otros eve...
Auditor...	23/02/2025 23:34:23	Microsoft ...	5058	Otros eve...

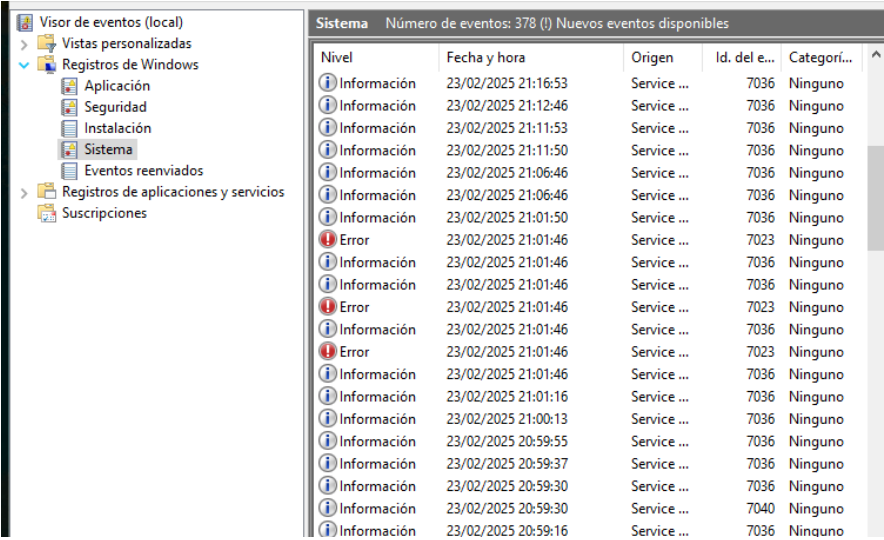


Visor de eventos (local)

- Vistas personalizadas
- Registros de Windows
  - Aplicación
  - Seguridad
  - Instalación
  - Sistema
  - Eventos reenviados
- Registros de aplicaciones y servicios
- Suscripciones

**Aplicación** Número de eventos: 84

Nivel	Fecha y hora	Origen	Id. del e...	Categori...
Información	23/02/2025 23:19:38	Security...	903	Ninguno
Información	23/02/2025 23:19:38	Security...	16384	Ninguno
Información	23/02/2025 23:19:08	Security...	8197	Ninguno
Información	23/02/2025 23:19:08	Security...	902	Ninguno
Información	23/02/2025 23:19:08	Security...	1003	Ninguno
Información	23/02/2025 23:19:08	Security...	1066	Ninguno
Información	23/02/2025 23:19:08	Security...	900	Ninguno
Información	23/02/2025 21:13:02	Window...	1001	Ninguno
Información	23/02/2025 21:13:02	Window...	1001	Ninguno
Información	23/02/2025 21:13:02	Window...	1001	Ninguno
Información	23/02/2025 21:13:02	Window...	1001	Ninguno
Información	23/02/2025 21:06:57	Window...	1001	Ninguno
Información	23/02/2025 21:06:57	Window...	1001	Ninguno
Información	23/02/2025 21:06:57	Window...	1001	Ninguno
Información	23/02/2025 21:06:57	Window...	1001	Ninguno
Información	23/02/2025 21:06:57	Window...	1001	Ninguno
Información	23/02/2025 21:06:57	Window...	1001	Ninguno
Información	23/02/2025 20:57:22	Security...	903	Ninguno
Información	23/02/2025 20:57:22	Security...	16384	Ninguno
Información	23/02/2025 20:56:49	Security...	902	Ninguno
Información	23/02/2025 20:56:49	Security...	1003	Ninguno
Información	23/02/2025 20:56:49	Security...	1066	Ninguno



Visor de eventos (local)

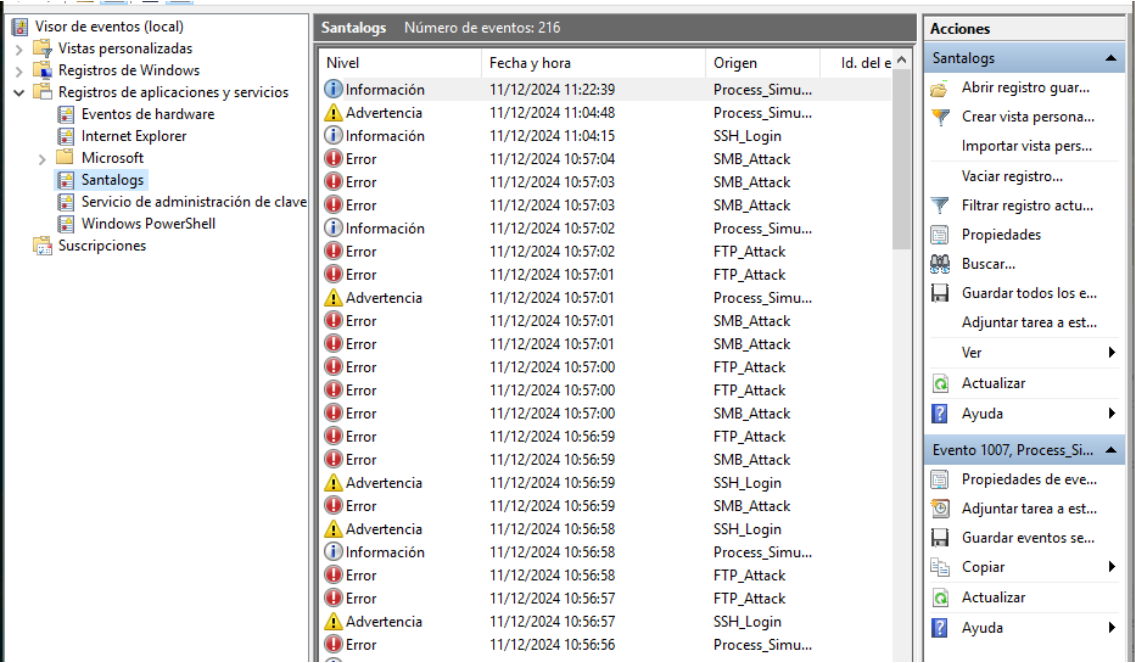
- Vistas personalizadas
- Registros de Windows
  - Aplicación
  - Seguridad
  - Instalación
  - Sistema
  - Eventos reenviados
- Registros de aplicaciones y servicios
- Suscripciones

**Sistema** Número de eventos: 378 (!) Nuevos eventos disponibles

Nivel	Fecha y hora	Origen	Id. del e...	Categori...
Información	23/02/2025 21:16:53	Service ...	7036	Ninguno
Información	23/02/2025 21:12:46	Service ...	7036	Ninguno
Información	23/02/2025 21:11:53	Service ...	7036	Ninguno
Información	23/02/2025 21:11:50	Service ...	7036	Ninguno
Información	23/02/2025 21:06:46	Service ...	7036	Ninguno
Información	23/02/2025 21:06:46	Service ...	7036	Ninguno
Información	23/02/2025 21:01:50	Service ...	7036	Ninguno
Error	23/02/2025 21:01:46	Service ...	7023	Ninguno
Información	23/02/2025 21:01:46	Service ...	7036	Ninguno
Información	23/02/2025 21:01:46	Service ...	7036	Ninguno
Error	23/02/2025 21:01:46	Service ...	7023	Ninguno
Información	23/02/2025 21:01:46	Service ...	7036	Ninguno
Error	23/02/2025 21:01:46	Service ...	7023	Ninguno
Información	23/02/2025 21:01:46	Service ...	7036	Ninguno
Información	23/02/2025 21:01:16	Service ...	7036	Ninguno
Información	23/02/2025 21:00:13	Service ...	902	Ninguno
Información	23/02/2025 20:59:55	Service ...	7036	Ninguno
Información	23/02/2025 20:59:37	Service ...	7036	Ninguno
Información	23/02/2025 20:59:30	Service ...	7036	Ninguno
Información	23/02/2025 20:59:30	Service ...	7040	Ninguno
Información	23/02/2025 20:59:16	Service ...	7036	Ninguno

Como podemos ver, en general hay logs que no nos aportan mucha información, algún error que otro, pero nada de información.

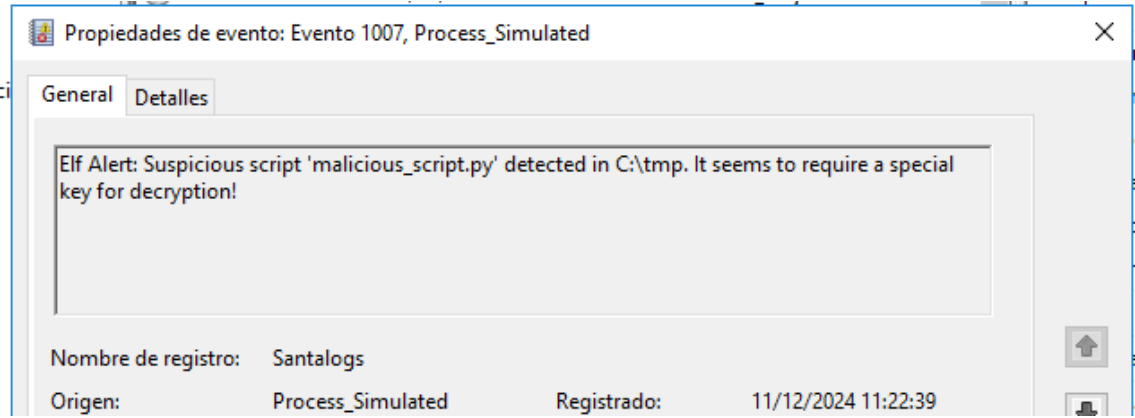
Sin embargo, si miramos el apartado “Registros de aplicaciones y servicios” y dentro de este el de “Santalogs”, veremos una serie de logs mucho más interesantes.



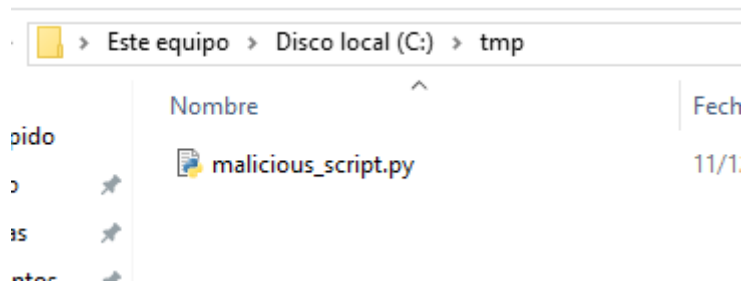
Nivel	Fecha y hora	Origen	Id. del e
Información	11/12/2024 11:22:39	Process_Simu...	
Advertencia	11/12/2024 11:04:48	Process_Simu...	
Información	11/12/2024 11:04:15	SSH_Login	
Error	11/12/2024 10:57:04	SMB_Attack	
Error	11/12/2024 10:57:03	SMB_Attack	
Error	11/12/2024 10:57:03	SMB_Attack	
Información	11/12/2024 10:57:02	Process_Simu...	
Error	11/12/2024 10:57:02	FTP_Attack	
Error	11/12/2024 10:57:01	FTP_Attack	
Advertencia	11/12/2024 10:57:01	Process_Simu...	
Error	11/12/2024 10:57:01	SMB_Attack	
Error	11/12/2024 10:57:01	SMB_Attack	
Error	11/12/2024 10:57:00	FTP_Attack	
Error	11/12/2024 10:57:00	FTP_Attack	
Error	11/12/2024 10:57:00	SMB_Attack	
Error	11/12/2024 10:56:59	FTP_Attack	
Error	11/12/2024 10:56:59	SMB_Attack	
Advertencia	11/12/2024 10:56:59	SSH_Login	
Error	11/12/2024 10:56:59	SMB_Attack	
Advertencia	11/12/2024 10:56:58	SSH_Login	
Información	11/12/2024 10:56:58	Process_Simu...	
Error	11/12/2024 10:56:58	FTP_Attack	
Error	11/12/2024 10:56:57	FTP_Attack	
Advertencia	11/12/2024 10:56:57	SSH_Login	
Error	11/12/2024 10:56:56	Process_Simu...	

Como se ve, hay varios errores y advertencias con nombres de origen como: SMB\_ATTACK, FTP\_ATTACK, SSH\_LOGIN. Por ende, vamos a ir mirando los primeros logs para ver si nos brinda algún tipo de información.

Si miramos la información del primero, nos encontramos con el siguiente mensaje:



Aquí nos indica que en el directorio tmp/ tenemos un archivo .py que por lo visto es un archivo malicioso, vamos a movernos a ese directorio y vamos a comprobarlo.



En efecto, hay un script .py con el nombre de “malicious\_script.py”. Además, en el mensaje anterior nos decía que necesitamos una key especial para desencriptar los datos y reiniciar el sistema para que todo vuelva a la normalidad. Seguimos investigando.

Sin ir mucho más lejos, al 3 log investigado, obtenemos el siguiente mensaje:



La llave de acceso es la **FTP25\_SMB192.168.1.101** . Ahora que tenemos esta clave, vamos a introducirla en el script .py que hemos encontrado antes.



## 6 OBTENIENDO LA FLAG

Abrimos la PowerShell y nos movemos al directorio tmp/ para ejecutar el script

```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. Todos los derechos reservados.

PS C:\Users\Administrador> cd C:\tmp\
PS C:\tmp> dir

Directorio: C:\tmp

Mode                LastWriteTime         Length Name
----                -
-a----           11/12/2024   11:27             447 malicious_script.py

PS C:\tmp>
```

Si lo ejecutamos e introducimos la contraseña, obtendremos la siguiente flag:

```
PS C:\tmp> .\malicious_script.py
Introduce la clave AES:

[+] Mensaje desencriptado: FLAG: oscar_feliz_navidad
PS C:\tmp> _
```

Ya hemos obtenido la flag y restablecido el sistema, como bien nos pedían en el mensaje que hemos leído al inicio.