

Análisis forense

Unidad 4. Actividad 2



15 de ABRIL de 2023

Carlos DÍAZ MONTES

ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

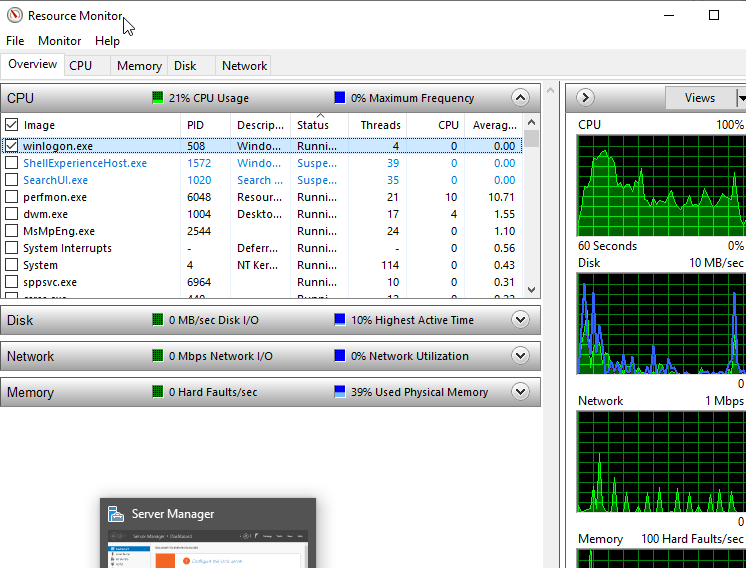
[RELACION DE EJERCICIOS T04-R01-Ejercicio 1 **¡Error! Marcador no definido.**](#_Toc163578451)

[Ejercicio 1 (2 puntos) Análisis de Google Drive **¡Error! Marcador no definido.**](#_Toc163578452)

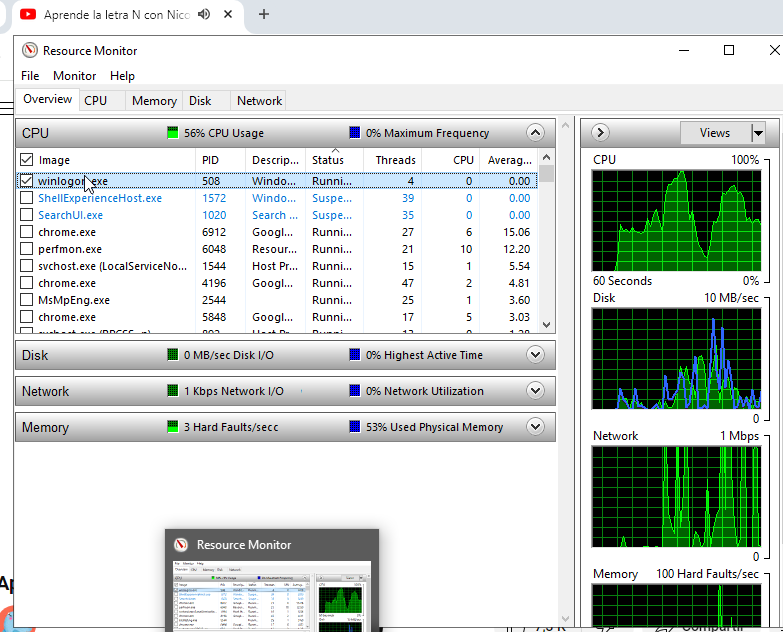
# Monitor de un sistema de Windows server

**Ejercicio 2 (2 puntos) Monitorizacion de windows server**

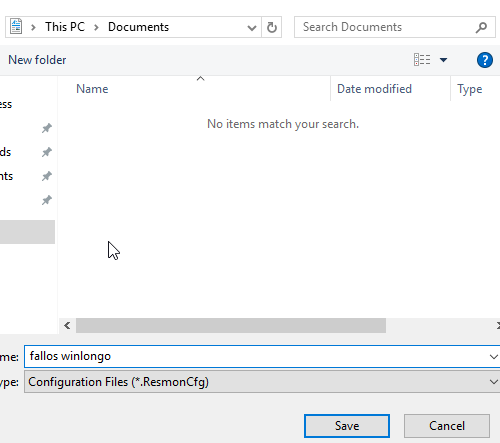
Monitor de rendimiento de Windows Server antes del video:



Ahora con el video puesto:

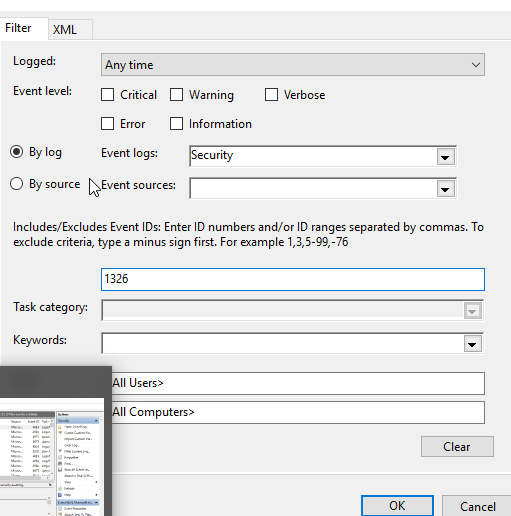


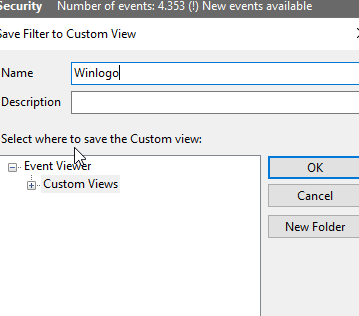
Como vemos ha aumentado el nivel de cpu, entre otras cosas.

Guardamos los procesos:  


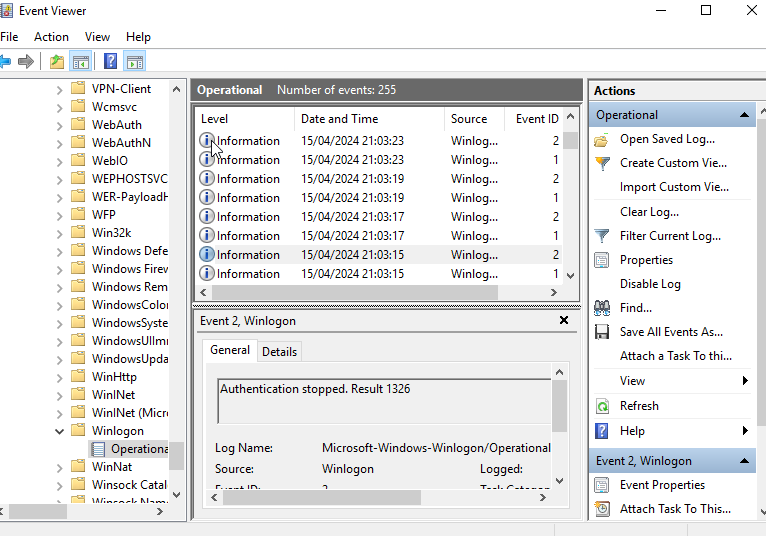
**Sal del sistema, haz tres intentos de entrar fallidos, vuelve a entrar en el sistema y aplica la vista personalizada que has creado. Entrega una captura de pantalla donde figuran los tres intentos fallidos de Winlogon.**

Creamos el filtro:



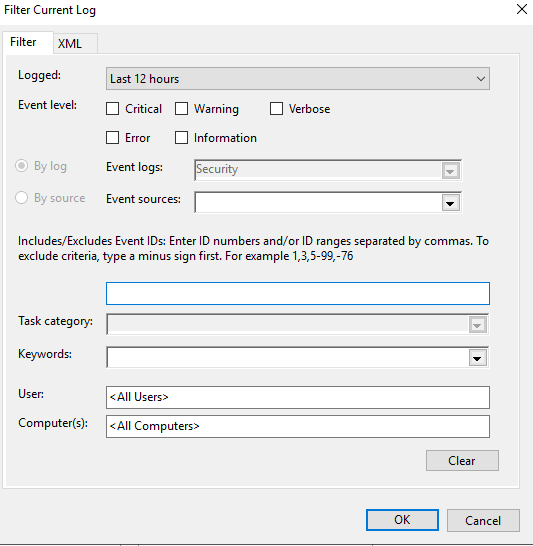


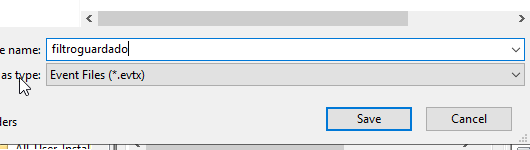
Ahora ponemos 3 veces mal la contraseña y miramos el log creado anteriormente:



**Crea un filtro donde se vea únicamente los sucesos de las últimas 12 horas para todos los niveles de eventos del log Seguridad y Sistema. Entrega capturas de pantalla donde se vean las acciones que hemos realizado en ese tiempo, con los detalles, explicando que indican.**

Nos creamos el filtro donde ponemos las ultimas 12 horas:



Guardamos el filtro:  


Ahora

