



ANÁLISIS FORENSE

Unidad 4. Actividad 2



15 DE ABRIL DE 2023
CARLOS DÍAZ MONTES
ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

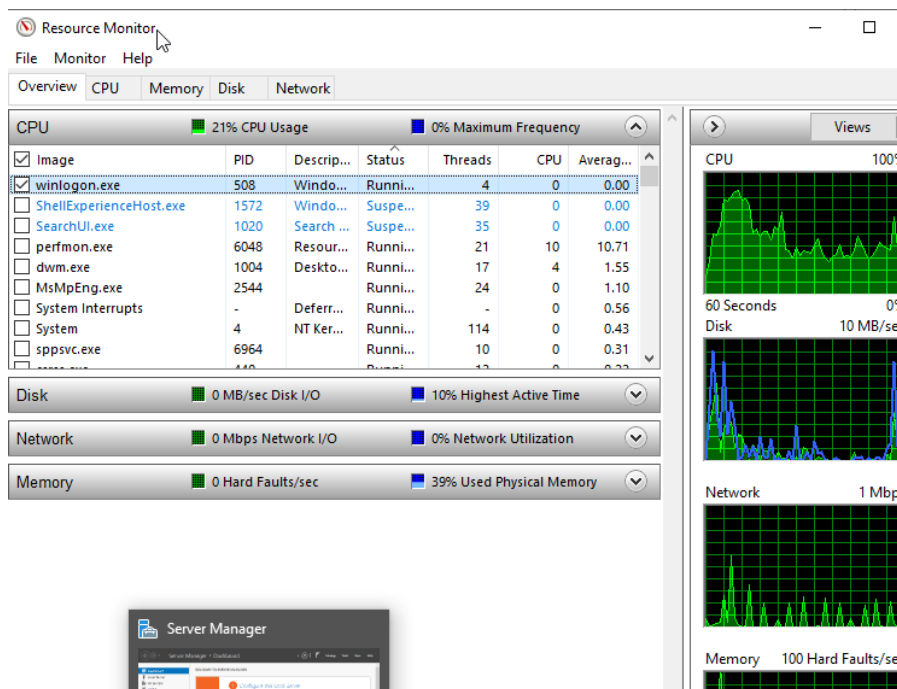
RELACION DE EJERCICIOS T04-R01-Ejercicio 1 ¡Error! Marcador no definido.

Ejercicio 1 (2 puntos) Análisis de Google Drive ¡Error! Marcador no definido.

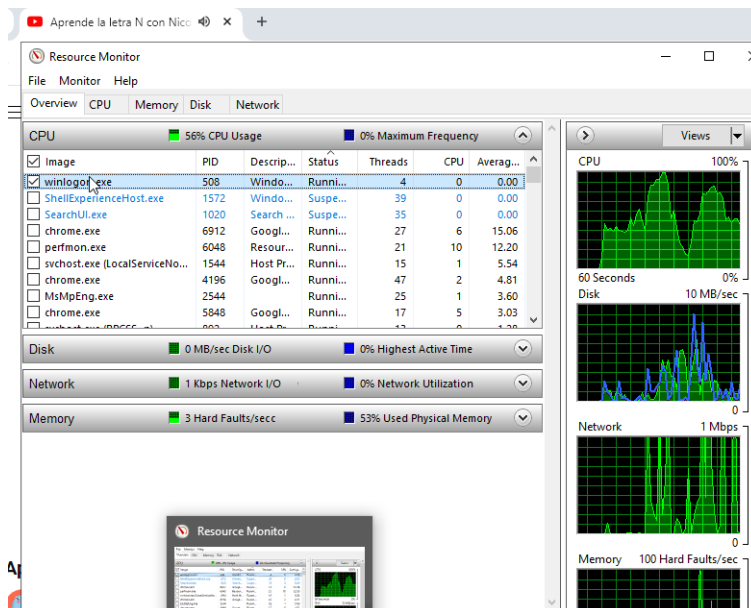
Monitor de un sistema de Windows server

Ejercicio 2 (2 puntos) Monitorizacion de windows server

Monitor de rendimiento de Windows Server antes del video:

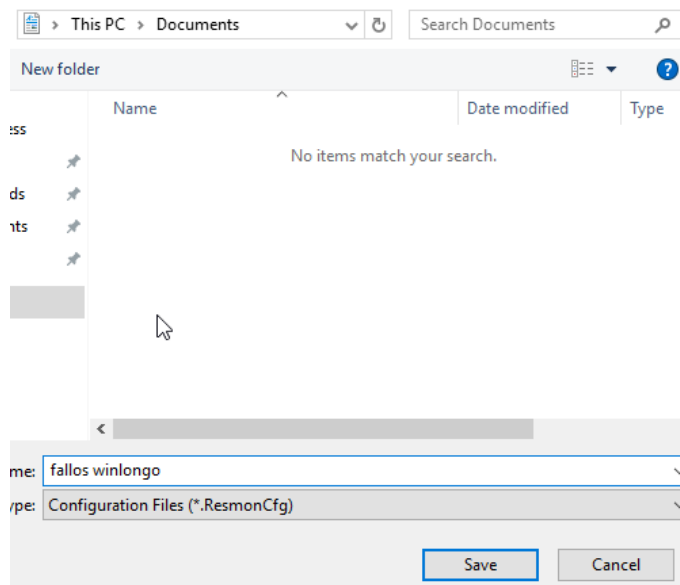


Ahora con el video puesto:



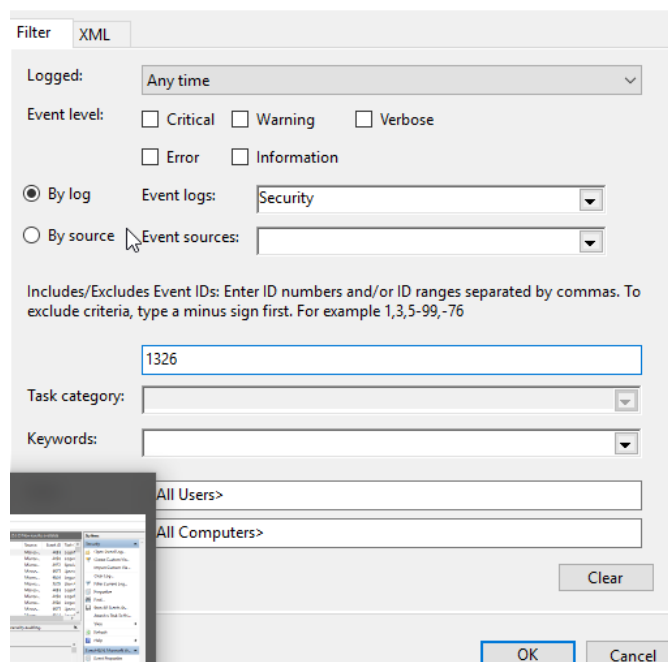
Como vemos ha aumentado el nivel de cpu, entre otras cosas.

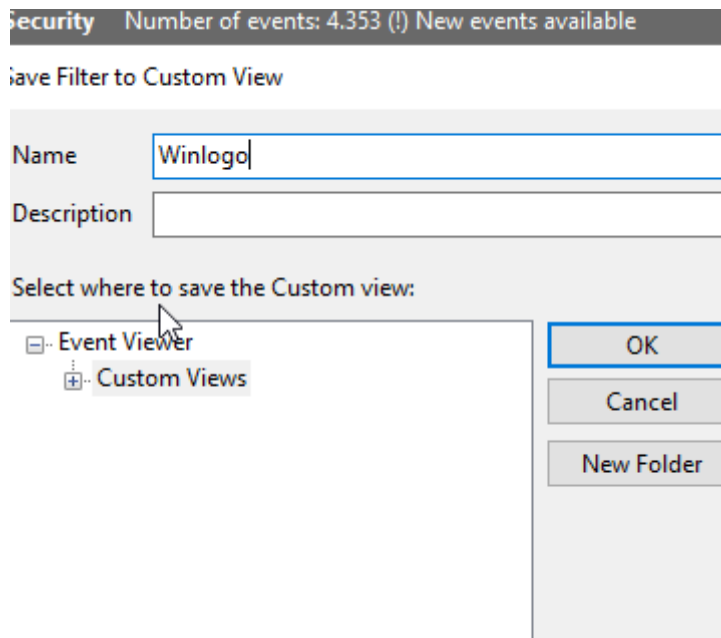
Guardamos los procesos:



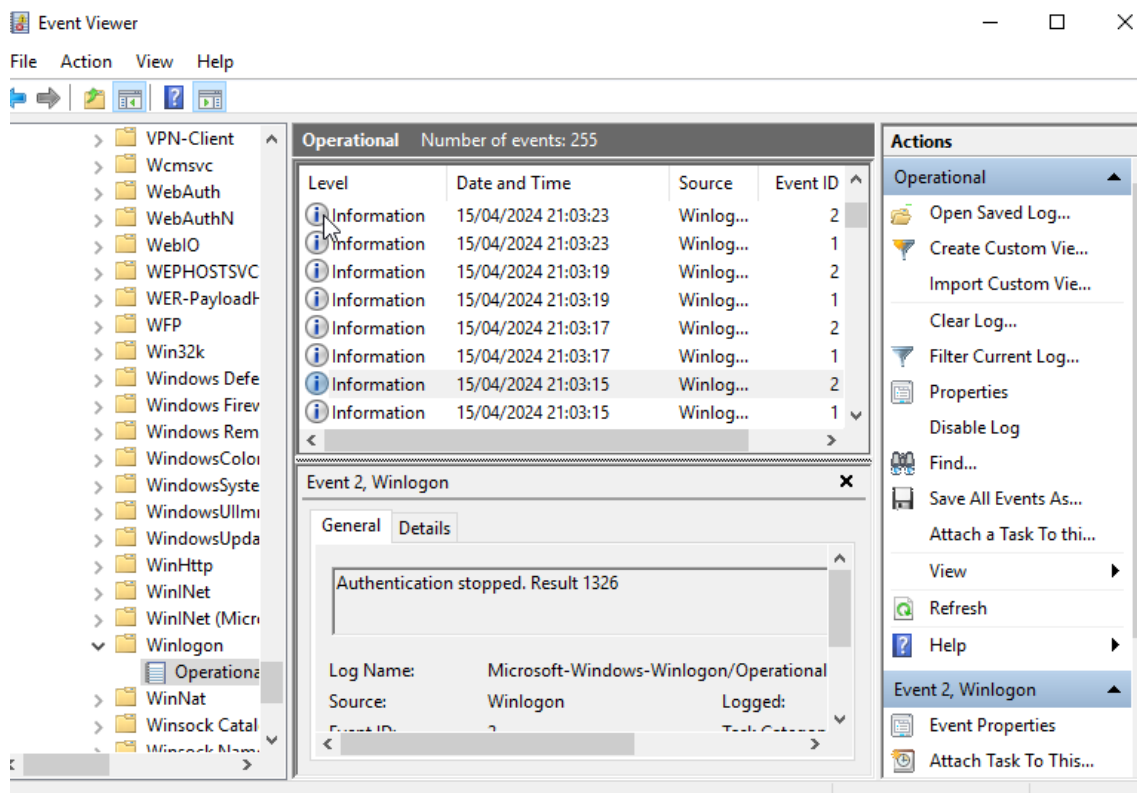
Sal del sistema, haz tres intentos de entrar fallidos, vuelve a entrar en el sistema y aplica la vista personalizada que has creado. Entrega una captura de pantalla donde figuran los tres intentos fallidos de Winlogon.

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:

Filter Current Log

Filter XML

Logged: Last 12 hours

Event level: ☐ Critical ☐ Warning ☐ Verbose
☐ Error ☐ Information

☒ By log Event logs: Security

☐ By source Event sources:

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

Task category:

Keywords:

User: <All Users>

Computer(s): <All Computers>

Clear

OK Cancel

Guardamos el filtro:

Filter name: filtroguardado

File type: Event Files (*.evtx)

Save Cancel

Ahora

filtroguardado Number of events: 4.523

| Level | Date and Time | Source | Event ID |
|-------------|---------------------|-----------|----------|
| Information | 15/04/2024 21:14:15 | Micros... | 4634 |
| Information | 15/04/2024 21:14:09 | Micros... | 4634 |
| Information | 15/04/2024 21:14:09 | Micros... | 4624 |
| Information | 15/04/2024 21:14:09 | Micros... | 4672 |
| Information | 15/04/2024 21:14:04 | Micros... | 4624 |
| Information | 15/04/2024 21:14:04 | Micros... | 4672 |
| Information | 15/04/2024 21:13:29 | Micros... | 4672 |
| Information | 15/04/2024 21:13:29 | Micros... | 4624 |

Event 4634, Microsoft Windows security auditing.

General Details