

81Auditpol

Emilio Cabo Gomis

Sumario

Requisitos previos del ejercicio.....2

Ejecución del comando.....2

Requisitos previos del ejercicio

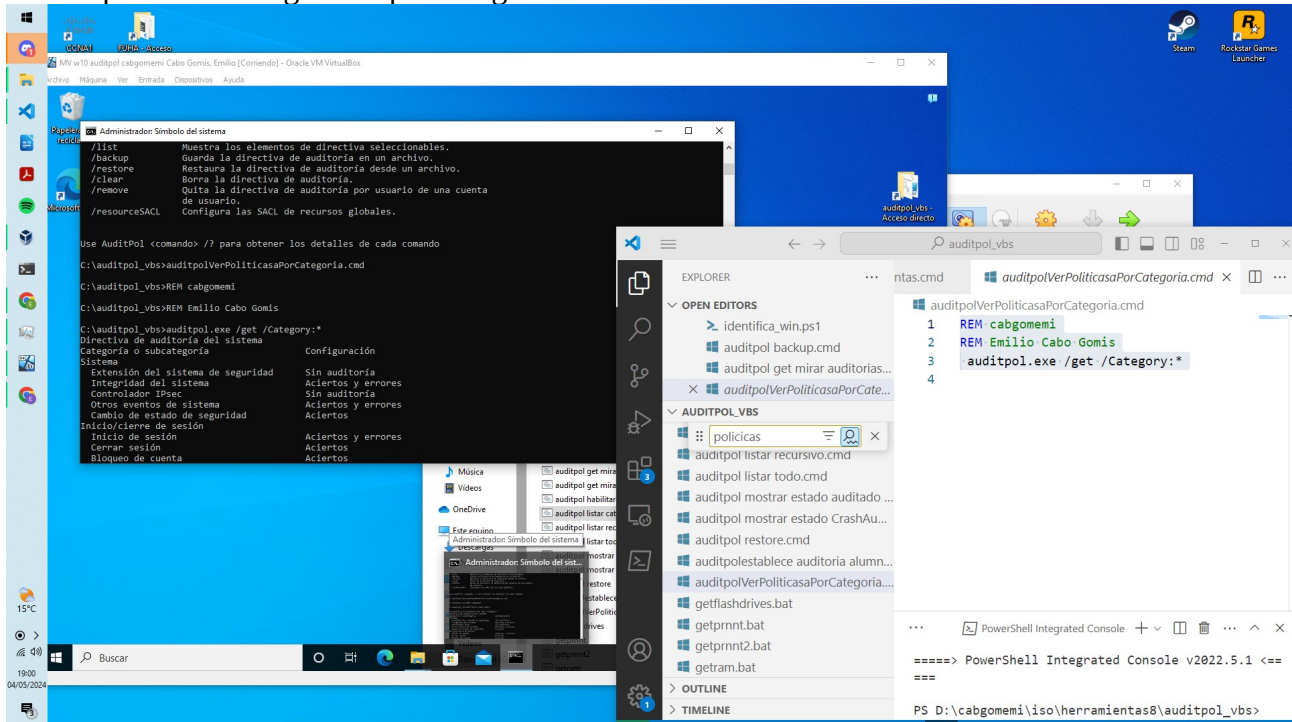
Iniciamos una máquina Windows 10.

Montamos la carpeta compartida en la que tenemos los scripts.

Ejecución del comando

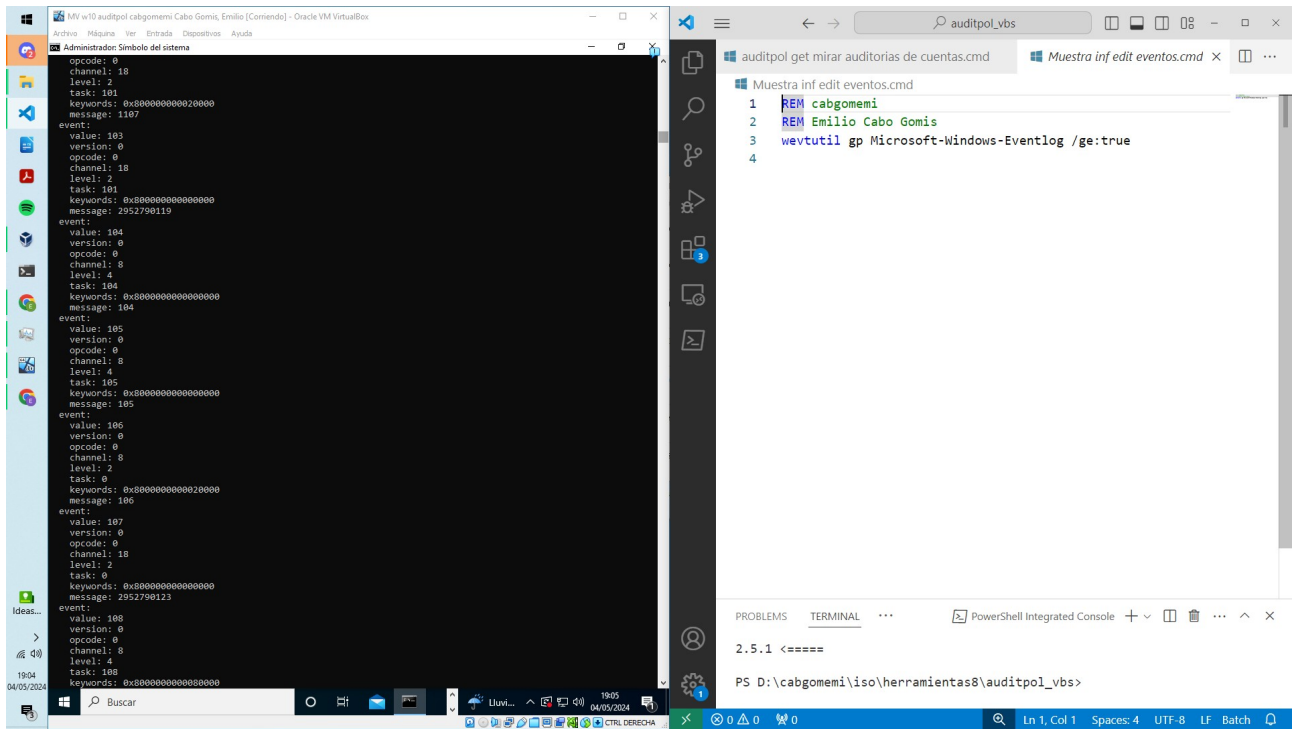
auditpolVerPoliticasaPorCategoria.cmd

Ver las políticas de seguridad por categoría.

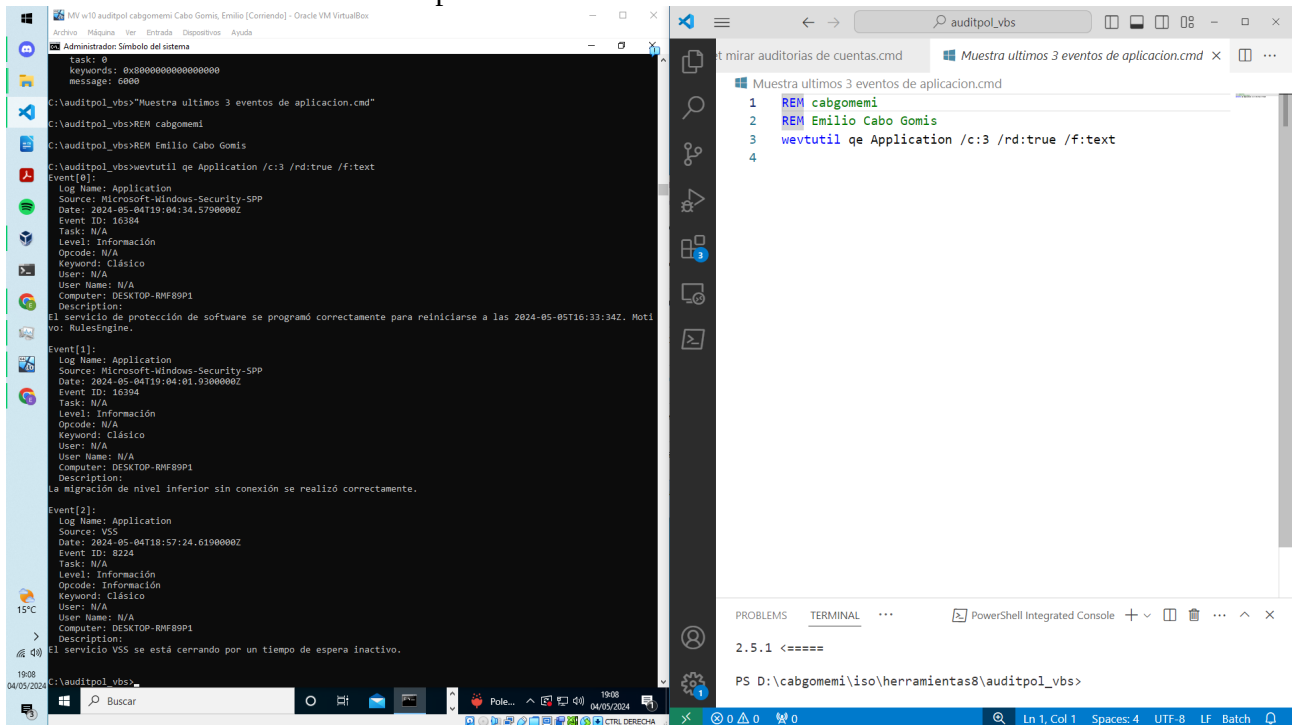


Muestra inf edit eventos

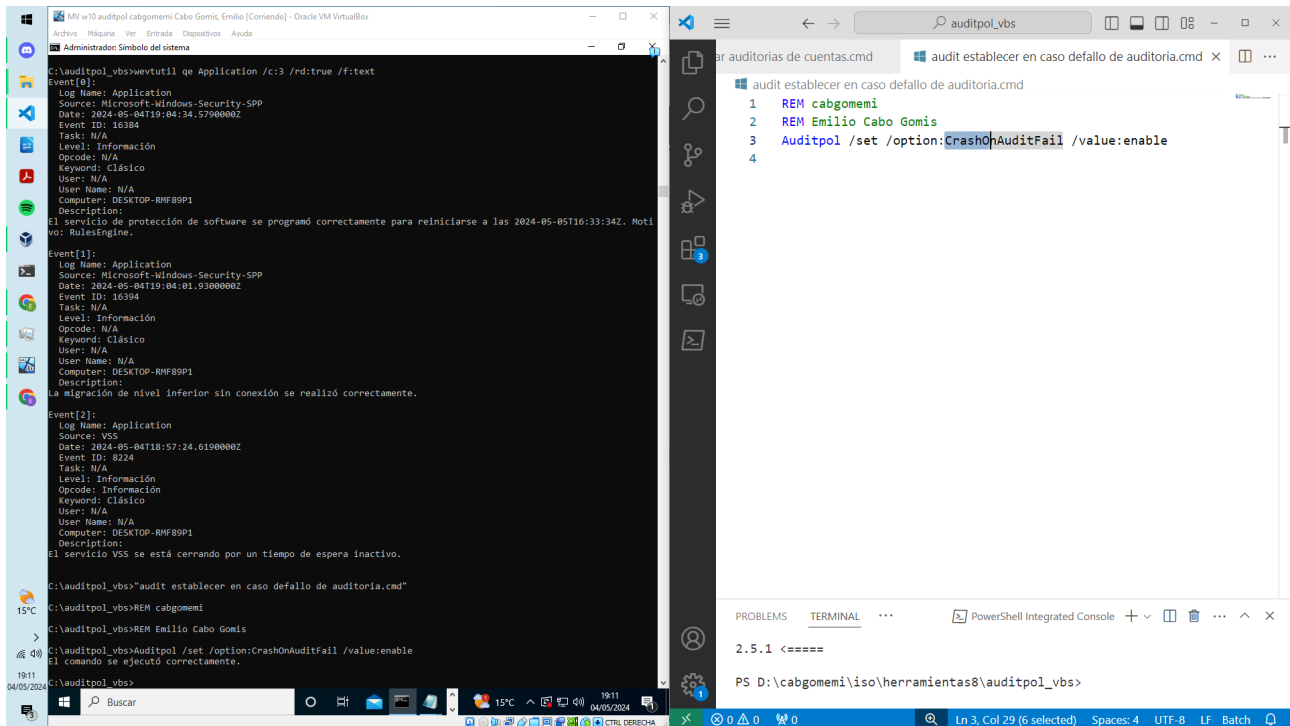
Muestra el event log



Muestra últimos tres eventos de aplicación.

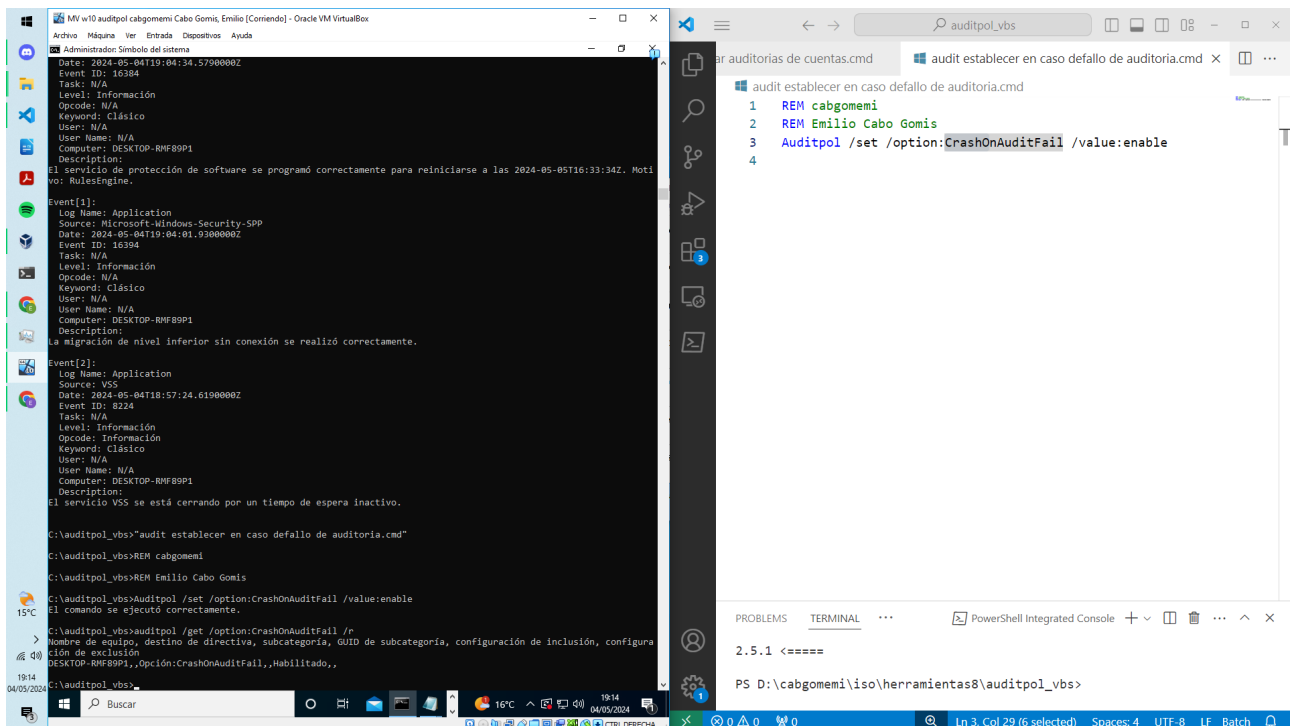


Establecer el crash on audit fail



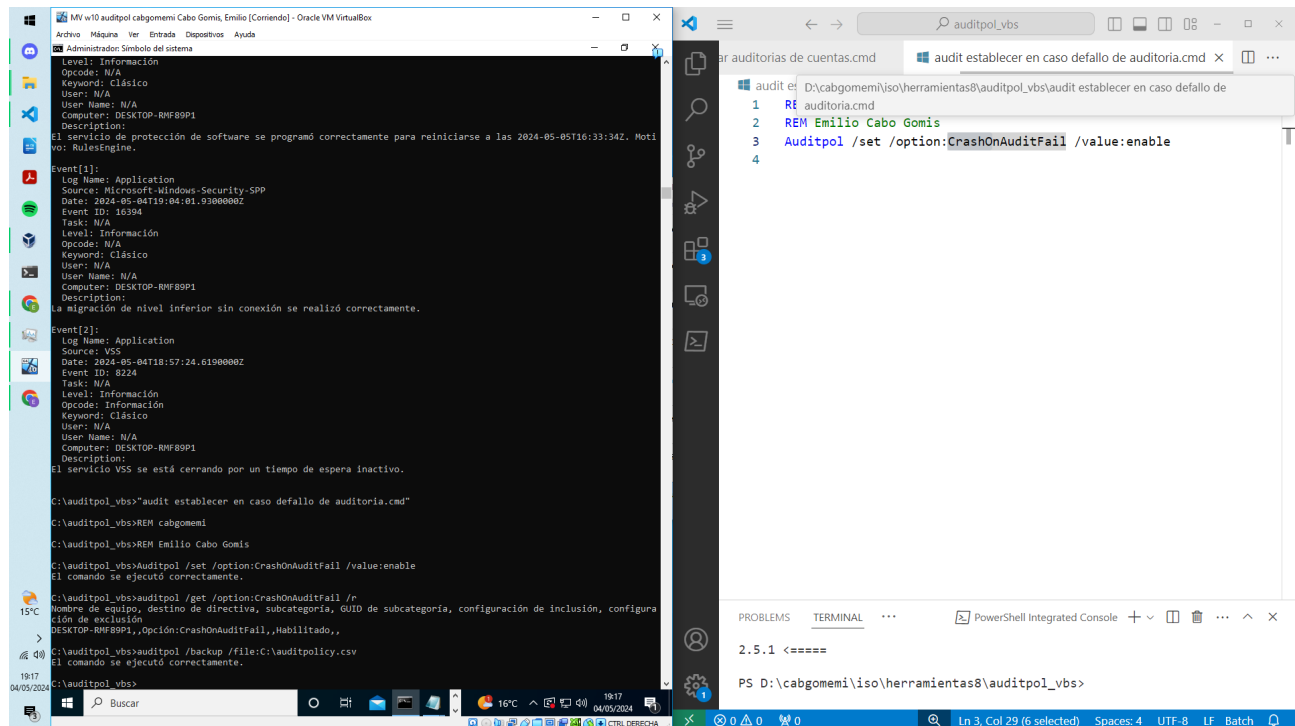
Comprobación de la ejecución mediante el comando.

auditpol /get /option:CrashOnAuditFail /r



auditpol /backup /file:C:\auditpolicy.csv

Copia de seguridad de las configuraciones de auditoría del ordenador.



Restablecido de las configuraciones de auditoría a partir del archivo CSV

auditpol /restore /file:C:\auditpolicy.csv

