Laboratorio 4.1

Estudiante: Isaac Vásquez Valenciano

Cedula: 1-1711-0637

Descargamos Splunk

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

Configuramos el usuario y password

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Se accede a la herramienta web en 127.0.0.1:8080

Texto

Descripción generada automáticamente

Se modifica la zona horaria

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Se configura el email

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Se procede en agregar events logs de security

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Se realiza la búsqueda global “\*”

Interfaz de usuario gráfica

Descripción generada automáticamente con confianza media

Aquí buscamos intentos fallidos de inicio de sesión por 4625

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Configuramos una alerta de login fallidos:

Captura de pantalla de computadora

Descripción generada automáticamente

Configuramos el throttle y el trigger de correo

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Ahora analizamos el archivo Log.rtf del laboratorio para responder la pregunta 35

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica

Descripción generada automáticamente

Preguntas y respuestas:

1. ¿Cuántos eventos se generaron el 09 de febrero del 2022?

El archivo no presenta logs de Febrero del 2022, sin embargo, se generaron 380 en febrero del 2023.

1. ¿A qué hora se presentó la mayor generación de eventos el 09 de febrero del 2022?

A las 4:20 am.