



OpenWebinars certifica que

Zebenzui Lorenzo Díaz

Ha superado con éxito

**Análisis forense en entornos
Windows: Registro y log de
eventos**

Duración del curso

7 horas

Fecha de expedición

13 mayo 2024

A handwritten signature in black ink, appearing to read 'Manuel Agudo', positioned over a large, light gray watermark of the OpenWebinars logo.

CEO de OpenWebinars

Manuel Agudo

Contenido

Análisis forense en entornos Windows: Registro y log de eventos

1. INTRODUCCIÓN

Presentación

2. EL REGISTRO DE WINDOWS

Introducción al registro de Windows

Localización y obtención de los Hives de registro

Hives de registro de usuario

Shellbags

Hives de registro: SAM y SECURITY

Hive de registro: SOFTWARE y SYSTEM

Test de Autoevaluación

3. PROCESAMIENTO Y ANÁLISIS DEL REGISTRO DE EVENTOS

Procesamiento y análisis de los hives de registro

Test de Autoevaluación

4. EL LOG DE EVENTOS DE WINDOWS

Introducción al log de eventos de Windows

Localización y obtención de los ficheros de eventos

Logs de eventos de seguridad

Logs de eventos de sistema

Logs de eventos de PowerShell

Logs de eventos de Terminal Services

Otros logs de eventos relevantes

Test de Autoevaluación



5. PROCESAMIENTO Y ANÁLISIS DE LOS LOGS DE EVENTOS DE WINDOWS

Procesamiento y análisis de los logs de eventos

Test de Autoevaluación

6. EJERCICIO PRÁCTICO

Planteamiento del ejercicio práctico

Resolución del ejercicio práctico

Test de Autoevaluación

7. CONCLUSIONES

Conclusiones y próximos pasos