Prácticas módulo 3

Sobre escritura de SEH

OBJETIVO

Conseguir entender el funcionamiento de los depuradores que contiene el laboratorio de Windows 10 y las bases necesarias para construir un fuzzer funcional para la función vulnerable GMON del binario de vulnserver.

EJERCICIOS

1. Se debe de analizar el código fuente del binario vulnserver. Explica en qué parte se encuentra la vulnerabilidad de la función GMON y en qué consiste su vulnerabilidad.

2. Analiza el binario desensamblado e intenta localizar indicios de la vulnerabilidad existente en la función GMON.

3. Explica paso por paso la metodología que has seguido con el debugger para reproducir la vulnerabilidad existente en la función GMON de vulnserver.

4. Construye el exploit para reproducir la vulnerabilidad existente en la función GMON de vulnserver.

El formato de presentación de los ejercicios debe de ser cómo si estuvierais escribiendo un informe a vuestro cliente.

Hack by Security

We attack for your safety