



Hack by Security

Prácticas módulo 1

Conceptos de debugging y fuzzing

OBJETIVO

Conseguir entender la importancia del análisis estático del código de un binario y el manejo de herramientas de desensamblado, lo que permitirá el desarrollo del código exploit que reproduzca la vulnerabilidad existente en el binario.

EJERCICIOS

1. Se debe de analizar el código fuente del binario stack2. Explica en qué parte se encuentra la vulnerabilidad del código y en qué consiste su vulnerabilidad.
2. Construye el exploit para reproducir la vulnerabilidad existente en stack2.
3. Se debe de desensamblar el binario stack3. Explica en qué parte se encuentra la vulnerabilidad del código (binario desensamblado) y en qué consiste su vulnerabilidad.
4. Construye el exploit para reproducir la vulnerabilidad existente en stack3.

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