



**Hack by Security**

## Prácticas módulo 6

Buffer overflow en entornos de 64 bits

## 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 classic. 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 classic.
3. Se debe de desensamblar el binario ret2libc. 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 ret2libc.

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