Prácticas módulo 4

Bypass de DEP

OBJETIVO

Conseguir entender el funcionamiento de la seguridad que implementa DEP en Windows para construir una cadena ROP funcional que evite dicha medida de seguridad y reproduzca la vulnerabilidad existente en la función TRUN.

EJERCICIOS

1. Se debe de analizar el código fuente del binario vulnserver. Explica en qué parte se encuentra la vulnerabilidad de la función TRUN y en qué consiste su vulnerabilidad. Recuerda que este punto debe de tener DEP activo para **todas las aplicaciones que se ejecuten en Windows.**

2. Explica paso por paso la metodología que has seguido con el debugger para reproducir la vulnerabilidad existente en la función TRUN de vulnserver. Recuerda que este punto debe de tener DEP activo para **todas las aplicaciones que se ejecuten en Windows.**

3. Construye el exploit para reproducir la vulnerabilidad existente en la función TRUN de vulnserver. Recuerda que este punto debe de tener DEP activo para **todas las aplicaciones que se ejecuten en Windows.**

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