Prácticas módulo 5

Bypass de NX y ASLR

OBJETIVO

Conseguir entender el funcionamiento de la seguridad que implementa NX y ASLR en los entornos de Linux para conseguir reproducir una cadena ROP funcional para un entorno de Linux con las protecciones NX y ASLR activas.

EJERCICIOS

1. Se debe de desensamblar el binario ovrflw y localizar indicios de la existencia de la dependencia vulnerable **libc** y la vulnerabilidad existente de buffer overflow en el binario ovrflw.

2. Explica paso por paso la metodología que has seguido con el debugger para reproducir la vulnerabilidad existente en el binario ovrflw. Recuerda que este punto debe de tener ASLR activo en el entorno de Linux.

3. Construye el exploit para reproducir la vulnerabilidad existente en el binario ovrflw. Recuerda que este punto debe de tener ASLR activo en el entorno de Linux.

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