Bypass: ROP to Evade ASLR

Author: Harshal Harekar
Date: 28/10/2025

Use Return-Oriented Programming to bypass ASLR in a local binary.

Summary:

Analyzed binary with Ghidra to identify ROP gadgets. Crafted a ROP chain using to call without relying on fixed addresses. Used stack pivoting and leaked libc base to dynamically resolve function addresses. Successfully bypassed ASLR and executed shellcode in randomized memory space.