[Hack CTF] Basic\_BOF #2

텍스트이(가) 표시된 사진

자동 생성된 설명

Gdb로 문제 파일을 분석해보자

Fgets 함수를 보면 [ebp-0x8c]에 133바이트를 표준입력으로 받는다.

그리고 위쪽에 [ebp-0xc]에 어떤 값이 들어간 것을 볼 수 있다. 좀만 더 내려보면 eax에 이 주소를 넣고 eax를 call하는 부분이 있다. 즉 eax에 있는 주소값에 있는 함수를 실행시키는 것이다.

[ebp-0x8c]와 [ebp-0xc] 사이에는 128바이트의 공간이 있고 fgets로는 133바이트를 입력받으니 128바이트를 채우고 5바이트만큼 [ebp-0xc]에 덧씌울 수 있다.

덧씌울 때는 함수의 주소를 넣어야 하는데 info func함수로 덧씌울 함수 주소를 볼 수 있다.

텍스트이(가) 표시된 사진

자동 생성된 설명텍스트, 칠판이(가) 표시된 사진

자동 생성된 설명

Shell이란 함수가 있어 봤더니 system함수를 실행한다.

아마 쉘을 실행시키는 함수인 듯 하다. 그러면 덧씌우는 함수의 주소는 shell 함수의 주소 0x0804849b로 하면 될 것 같다.

Python pwntools라이브러리로 익스플로잇하면

텍스트이(가) 표시된 사진

자동 생성된 설명