Pwnable.kr bof

텍스트이(가) 표시된 사진

자동 생성된 설명

Bof.c와 bof 파일 중 func부분을 gdb로 본 결과가 위의 사진이다.

<+40>을 보면 0xcafebabe와 [esp+0x8]을 비교하는 부분이 있다.

여기가 bof.c에서 key와 0xcafebabe를 비교하는 부분과 같다. 그러면 이곳 바로 위에 있는 함수 호출이 gets를 부르는 곳이고 gets에 들어가는 변수 주소가 [esp-0x2c]이다.

즉 key 값의 주소는 [esp+0x8] 입력하는 값이 저장되는 주소는 [esp-0x2c]가 된다.

둘 사이의 공간은 0x2c-(-0x8)이 되므로 (key는 esp+, 입력값은 esp-이므로 부호에 주의)

계산하면 총 52바이트의 공간이 남는다. 이 공간을 채우고 key값에 0xcafebabe를 덮어씌워주면 된다.

파이썬 pwntool을 사용해 익스플로잇 하면

텍스트이(가) 표시된 사진

자동 생성된 설명

이렇게 하면 성공적으로 문제가 풀린다.