Root-me

ELF C++ – 0 Protection Write Up

Author : hideroot(M.O.K)

Data : 2017/11/20

문제를 받아보면 elf 파일로 하나를 던져 준다. IDA로 열어 보면 C++ 클래스들이 몇 개 보인다. 일단 ELF니까 리눅스에서 실행을 해보면 USAGE 라고하면서 argv[1] 에 passwd를 입력하라고 한다. Passwd 입력하면 당연히 틀렸다고 나온다. 자 그럼 쉬운 문제니까 생각을 해보자 분명히 스트링을 비교를 하는 함수가 어딘가에 존재 할 것이다. IDA로 삽질하면서 ANGR까지 동원해서 찾아보는데 도저히 static으로는 도저히 안보이길래 attach 상태로 뜯어보기로 했다.

```
Guessed arguments:
arg[0]: 0xffffd6e4 --> 0x8050b24 ("Here_you_have_to_understand_a_little_C++_stuffs")
arg[1]: 0xffffd8df ("abcd")
```

Peda DBG로 돌리면서 언제 비교하나 한줄한줄 따라가보니 답이 나왔다....

만약 큰 프로그램이였다면 이런식으로는 안풀릴 것 같다. 일단 기초적인 문제라서 금방금방 풀리는 것 같다.