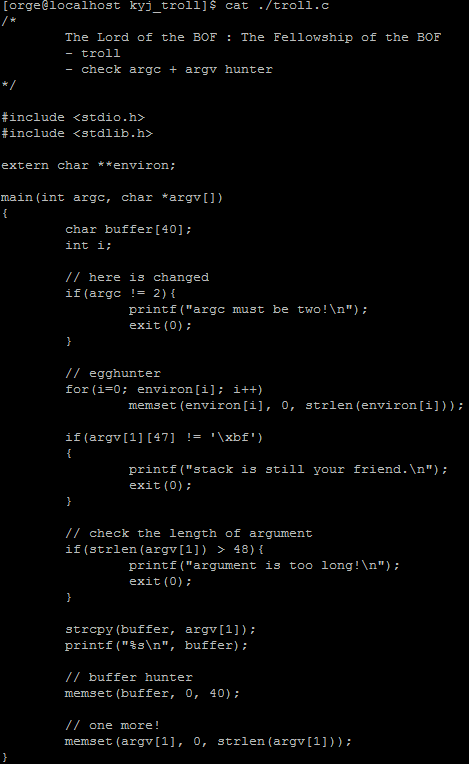
|  |
| --- |
| LOB Troll |
| 동아리마크  2018. 01. 29 (mon)  Dong-a .univ  COLONY  Young jin kim |

목차

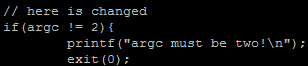
1. 소스코드 이해
2. 소스코드 분석
3. 공격
4. **소스코드 이해**



[ Troll.c의 소스코드 ]

|  |  |
| --- | --- |
| 외부변수 extern선언  buffer 배열 선언[40byte]  I 변수 선언  인자값이 2개가 아니면 프로그램 종료  memset함수로 2차원 배열 한줄 씩 초기화  argv[1][47]의 값이‘\xbf’와 다르면 프로그램 종료  argv[1](첫번째인자)의 길이가 48보다 크면 종료  buffer배열에 첫번째 인자값 복사  버퍼 값 출력  memset함수로 버퍼 초기화  memset함수로 argv[1] 초기화 | memset : (초기화할 변수, 초기화 값, 변수의 길이)  extern : 다른소스파일에 선언된 변수를  사용하기위한 코드  environ : unistd.h에 속한 변수지만 프로그램 만들 때,  자동으로 라이브러리에 포함됨 |

1. **소스코드 분석**



[인자 2개로 강제]

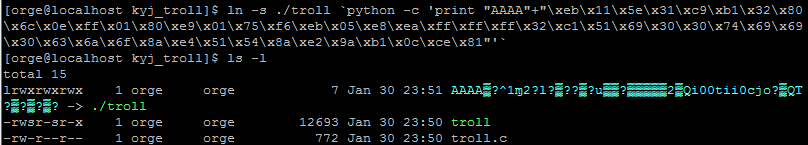
첫번째, 인자는 무조건 2개만 넣을 수 있다. (프로그램명도 1개를 차지함)



[argv[1] 초기화]

첫번째, 첫번째 인자값 argv[1]이 초기화 된다.

두번째, argv[1]에 쉘코드 삽입 불가능

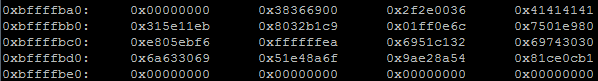


[심볼릭 링크를 통한 쉘코드 삽입]

첫번째, 우리는 argv[1], argv[2]에 쉘코드 삽입 불가

두번째, 남아있는 argv[0] 즉,함수명을 이용한다.

세번째, 함수명에 심볼릭 링크를 걸어 쉘코드를 삽입한다.

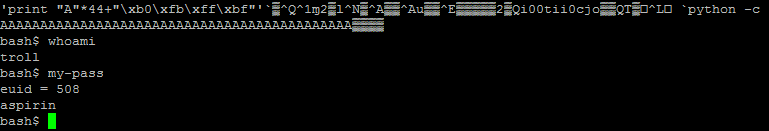


[코어파일 디버깅]

첫번쩨, 우리가 심볼릭 링크를 걸기 전 “A”개를 넣었던 것이 들어가 있다.

두번재, 쉘코드가 들어간 자리는 0xbffffbb0

1. **공격**



[익스플로잇]

Pw : aspirin