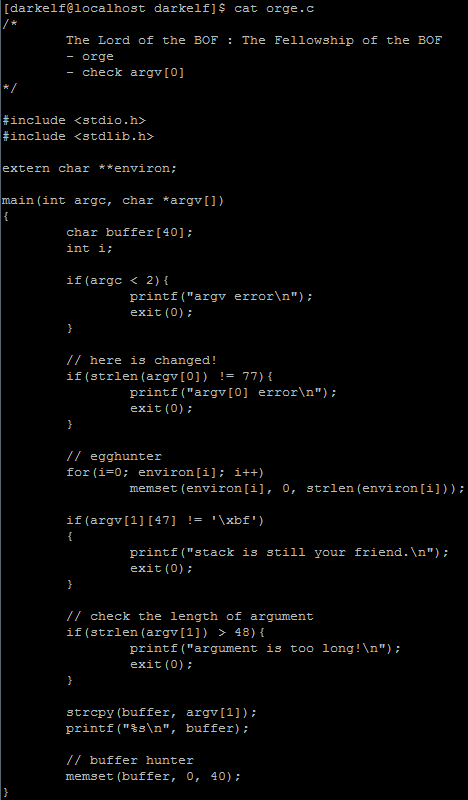
|  |
| --- |
| LOB orge |
| 동아리마크  2018. 01. 28 (sun)  Dong-a .univ  COLONY  Young jin kim |

목차

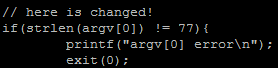
1. 소스코드 이해
2. 소스코드 분석
3. 공격
4. **소스코드 이해**



[ Orge.c의 소스코드 ]

|  |  |
| --- | --- |
| 외부변수 extern선언  buffer 배열 선언[40byte]  I 변수 선언  인자값이 1개 이하이면 프로그램 종료  파일명길이가 77이 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 | 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**



[darkelf와의 차이점]

첫번째, 파일길이가 77이 아니면 프로그램을 종료시킨다.

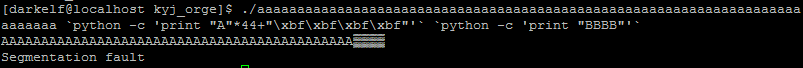


[파일명 A77개로 수정]

첫번째, 파일명을 요구한대로 77개로 맞추었다.

두번째, 원본파일명은 수정이 안되지만 파일명은 메모리값과 상관이 있어서 이렇게 변경함.

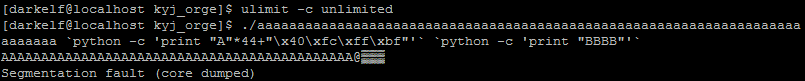
세번째, 디버깅 불가. 이유는 ./(현재 디렉터리)라는 명령어를 포함해야 한다고 함



[파일명 a75개로 수정]

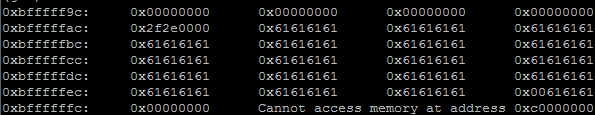
첫번째, argv[0]에러 없이 프로그램이 실행 되었다.

두번째, 코어파일을 생성하려 했으니 코어파일이 생성되지 않았다.



[코어파일 생성]

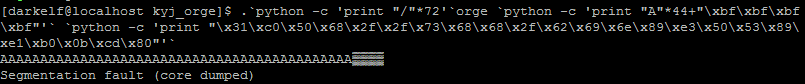
첫번째, ulimit -c unlimited 로 코어파일이 생성되도록 하였다.



[메모리 접근 불가]

첫번째. 디버깅 시도하려 했으나, 메모리가 할당이 되어있지 않다.

1. **소스코드 분석**



[코어파일 생성]

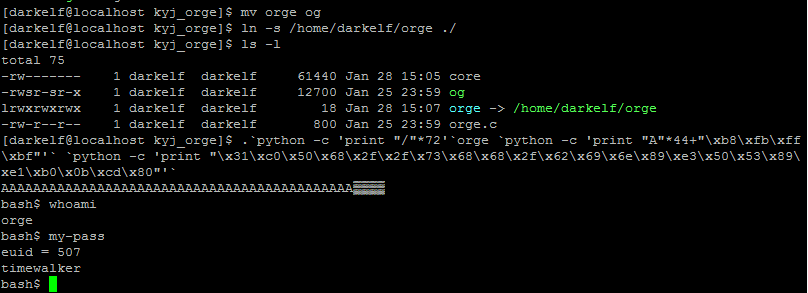
첫번째, orge가 실행되는 경로에서 영향력을 미치지 않는 “/” 72개 추가하여 익스플로잇



[코어파일 디버깅]

첫번째, 쉘코드 삽입 지점은 bffffbb8

1. **공격**



[익스플로잇]

Pw : timewalker