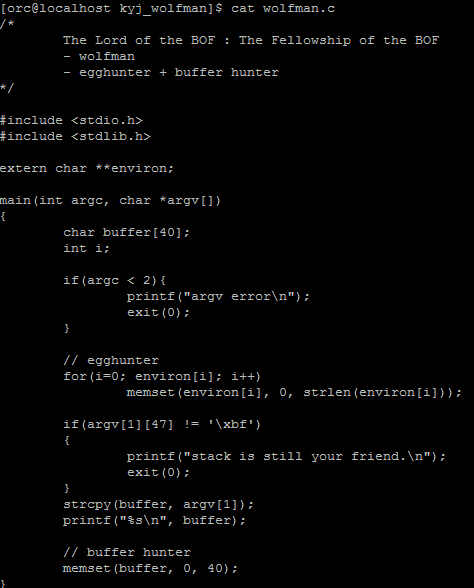
|  |
| --- |
| LOB wolfman |
| 동아리마크  2018. 01. 24 (wed)  Dong-a .univ  COLONY  Young jin kim |

목차

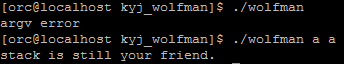
1. 소스코드 이해
2. 소스코드 분석
3. 공격
4. **소스코드 이해**



[ wolfman.c의 소스코드 ]

|  |  |
| --- | --- |
| 외부변수 extern선언  buffer 배열 선언[40byte]  I 변수 선언  인자값이 1개 이하이면 에러출력 후  프로그램 종료  memset함수로 2차원 배열 한줄 씩 초기화  argv[1][47]의 값이‘\xbf’와 다르면 프로그램 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**



[예외 종료 이미지]

첫번째, 인자값이 없는경우 에러

두번째, 인자값 2번째배열 48번째칸에 ‘\xbf’ 값이 있지 않아 오류 출력



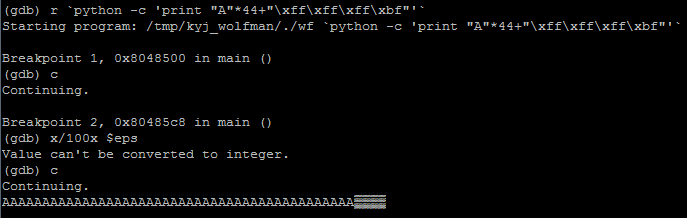
[환경변수 초기화]

첫번째, 환경변수 값을 초기화해서 쉘코드를 넣어두는 것을 막음



[디버깅]

첫번째, buffer[40]+int i[4]를 합쳐 44바이트가 할당 됨

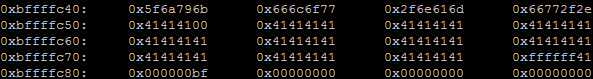


[디버깅(주소값 찾기)]

첫번째, 48번째 인자에 “\xbf”가 들어가야 한다.

(bf를 강제함으로써 다른 메모리에 쉘 코드를 넣는 것을 방지) [ ex)eggshell ]

1. **소스코드 분석**



[디버깅(주소값 찾기2)]

|  |  |  |  |
| --- | --- | --- | --- |
| Int i[4] | Buffer[40] | Ebp[4] | Ret[4] |
|  | “A”\*44 | | “\xbf………” |

첫번째, 위 내용을 종합하면 우리의 소스코드는 인자값이 2개 이상이고

두번째, 환경변수 사용 불가하며

세번째, ebp포함 44바이트 만큼 데이터를 채우고,

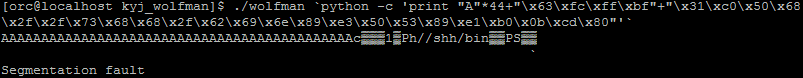
네번째, ret첫번째 값은 \xbf(쉘코드의 위치 강제함)가 들어가야 함

다섯째, 쉘코드가 들어갈 자리는 0xbffffc81



[코어파일 디버깅]

첫번째, 코어파일 분석결과 주소값은 \xbffffc59



[원본과 사본의 스택 주소차이로 인한 오류]

첫번째, 사본은 쉘 따는데 성공을 했다.

두번째, 원본은 쉘 따는데 실패 했다.

세번째, 문제의 길이 차이로 인해 메모리 값이 다를 수 있다.

네번째, 앞의 orc에서는 놉을 넣어 대충의 주소값을 가지고 익스플로잇을 시도했다.

다섯번째, 이번wolfman은 사본의 파일명을 wolfman으로 맞춰주어서 시도해 보았다.

1. **소스코드 분석**



[orc소스와의 차이점]

첫번째, orc소스에서와의 차이점은 이 코드 두줄이다.

두번째, buffer hunter는 memset함수를 이용해서 buffer 변수의 메모리 값을 초기화 함

세번째, 우리의 공격 방법은 ret보다 주소값이 높은 지역(즉, 버퍼와는 상관 없는)메모리에

쉘코드를 삽입하여 공격 중이다.

네번째, 따라서 orc와 똑 같은 문제다.

**+함수명, 경로가 해킹할 때 메모리에 영향을 주는가?**

1. /tmp/kyj\_wolfman/wf의 ret주소값 : bffffc63
2. /tmp/kyj\_wolfman/wolfman의 ret 주소값 : bffffc59
3. /tmp/AAAAAAAAAAAAAAAAAA(18개)/wf의 ret 주소값 : bffffc5d
4. /tmp/AAAAAAAAAAAAAAAAAA(18개)/wolfman의 ret 주소값 : bffffc53

파일명이 wf(2개) -> wolfman(7개)으로 바뀌었을 때 : 메모리 10칸 늘어남

경로명이 kyj\_wolfman(11개) -> A(18개)로 바뀌었을 때 : 메모리 6칸 줄어듬

**결론1 파일명은 메모리값에 영향을 미침**

**결론2 파일경로는 메모리값에 영향을 미침**

**결론3 파일명이 늘은 길이가 같으면 늘어나는 메모리값도 같다**

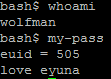
**결론4 파일경로가 늘은 길이가 같으면 늘어나는 메모리값도 같다**

**결론5 파일명, 경로의 길이 변화로 인해 메모리값이 변경되지만**

**얼마나 늘고 줄 것인지 예측불가**

1. **공격**





[파일 명 wf->wolfman 변경 후 익스플로잇]

Pw : love eyuna