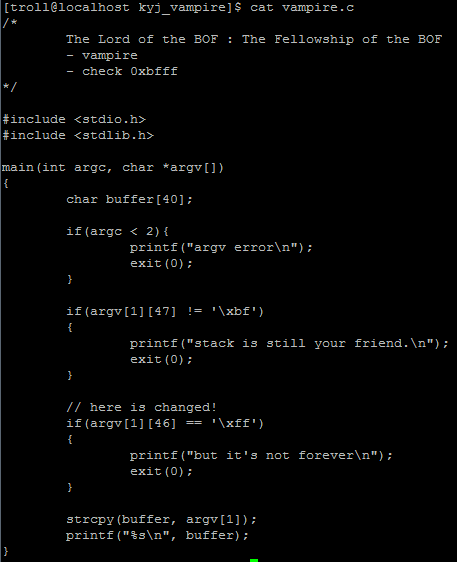
|  |
| --- |
| LOB vampire |
| 동아리마크  2018. 01. 31 (wed)  Dong-a .univ  COLONY  Young jin kim |

목차

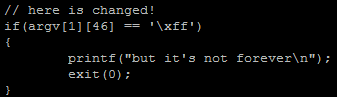
1. 소스코드 이해
2. 소스코드 분석
3. 공격
4. **소스코드 이해**



[ vampire.c의 소스코드 ]

|  |  |
| --- | --- |
| buffer 배열 선언[40byte]  인자값이 1개 이하이면 프로그램 종료  argv[1][47]의 값이‘\xbf’와 다르면 종료  argv[1][46]의 값이 ‘\xff’이면 종료  buffer배열에 첫번째 인자값 복사  버퍼 값 출력 |  |

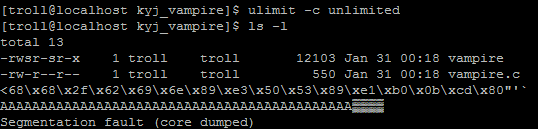
1. **소스코드 분석**



[ret두번째 주소값을 ff로 사용 못하게 함]

첫번째, 이부분에서 우리는 ret주소값을 0xbfff…으로 사용 할 수 없다..

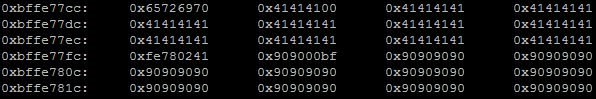
두번째, 우리는 익스플로잇 할 때 이 메모리대역을 사용 해 왔다.



[코어파일 생성]

첫번쩨, 함수명, ‘A’\*44개 \xbf\xbf\xbf\xbf를 넣었다

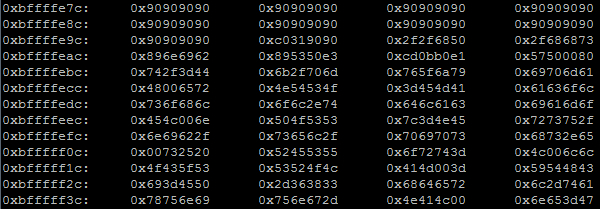
두번재, 두번째 인자에 놉10만개와 쉘코드를 삽입 했다.



[첫번째 인자 값]

첫번째, 우리가 넣은 첫번째 인자값이 있다.

1. **소스코드 분석**



[두번째 인자 값]

첫번째, 놉10만개의 끝나는 지점이다,

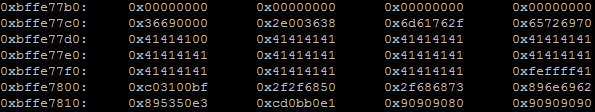
두번째, 놉 뒤에 쉘코드가 들어 가 있는 것이 보인다.

세번째, 첫번째 인자 값 사진과 두번째 인자 값 사이의 메모리중 적당한 값을 찾아 ret로 사용

네번째, 우리가 사용 할 주소는 \xbffeffff

다섯번째, 익스플로잇을 진행 해 보았으니 세폴이 떳다.(이유는 잘 모르겠음)

여섯번째, 놉+쉘코드 구조에서 쉘코드+놉 구조로 바꿔 보았다.

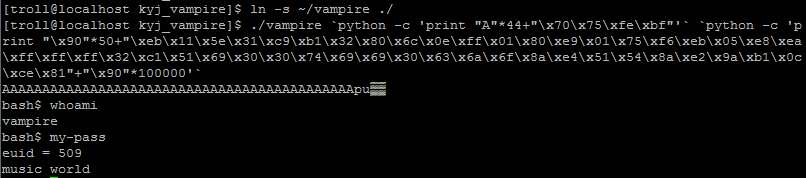


[쉘코드+놉구조 코어파일 디버깅]

첫번째, 쉘코드가 들어간 위치가 바뀐 것을 확인

두번재, 우리가 사용할 ret주소는 \xbffe7802

1. **공격**



[익스플로잇]

Pw : music world