2016년 시스템 프로그래밍

-Buffer Over Flow 과제-

제출일자	2016.11.14.
이　　름	정 윤 수
학　　번	201302482
분　　반	00

Buffer Over Flow 과제

```
a201302482@localhost:~$ ./bufdemo-nsp3 < bin
Type a 1 string:Type a 2 string:Type a 3 string:Type a 4 string:Type a 5 string:
Type a 6 string:Type a 7 string:Type a 8 string:Type a 9 string:Type a 10 string
:abcdabcdabcdabcdcdabcdabcdabcdabcdabcdabcdabcdabcdabbd_@
Type a 2 string:Type a 3 string:Type a 4 string:Type a 5 string:Type a 6 string:
Type a 7 string:Type a 8 string:Type a 9 string:Type a 10 string:
```

1. echo함수의 return주소는 call_echo함수에서 call echo의 다음 명령어인 add명령어의 어의 주소가 될 것이다. 그럼으로 0x40072a의 주소를 갖는다.

2.echo 함수의 return address의 저장위치는 gdb명령어로 스택을 살펴 본 결과 0x7fffffffe558 위치에 있다는 것을 알 수 있다.

3. buf와 buf2의 시작주소는 echo함수에서 값을 입력받기 전 %rsi와 %rdi에 스택 안에 있던 값을 저장을 한다. 이것은 buf1과 buf2의 시작주소이다. gdb명령어로 %rsi와 %rdi의 값을 살펴보면 buf1 과 buf2의 시작 주소는 0x7fffffffe3c0 과 0x7fffffffe3d0 이라는 것을 알 수 있다.