**Homework Assignment #3**

Q> 다음 C 코드를 이용하여 컴파일하고 실행 파일을 만든 후에 Buffer overflow 원리를 이용하여 해킹하세요.

<OS> Debian Jessy OS 사용

<Compile> –fno-stack-protector –mpreferred-stack-boundary=2 옵션 사용

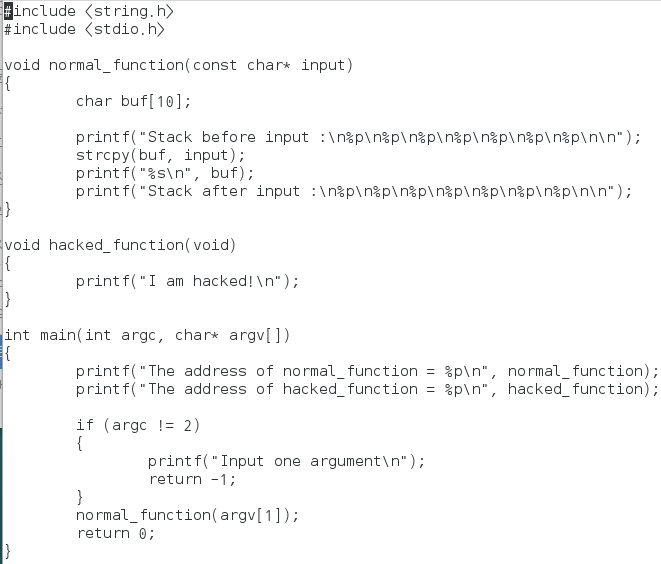
<String input> ./bof `perl –e ‘print “0123\xcc\xff”’` 형태를 이용하여 문자열 입력

<Hacking 성공 여부> 성공할 경우 I am hacked! 라는 문장이 출력됨

<Stack 내용보기> Stack before input 에 esp register에 저장된 메모리 주소부터 6개의 내용이 출력됨 (이중에 return address 포함되어 있음)

<함수 포인터> normal\_function과 hacked\_function의 함수 포인터가 출력됨

bof.c



보고서에 포함될 내용

1. Source Code
2. 해킹에 성공한 문자열과 그 문자열이 만들어진 이유 자세히 설명
3. 해킹에 성공한 화면 내용 출력
4. (보너스) printf(“Stack before Input : \n%p\n%p\n%p\n%p\n%p\n%p\n\n”); 문장이 스택의 내용을 출력한 이유

과제 기한

5월 2일 수업시간에 제출