

2020-2 임을규 교수님 컴퓨터보안

Assignment #3. Buffer Overflow

과제 제출: 모델 구현 중 작성한 소스코드 또는 보고서를 본인의 Git repository에 업로드

제출 기한: 12월 8일 화요일 23:59까지. 제출 기한에서 한 시간 단위로 10%씩 감점, 최소 0점

문의 사항: 장준영 조교, lartist@hanyang.ac.kr (제출 관련 문의 등)

과제 내용

"10. Buffer Overflow.pdf" 강의자료의 6페이지를 참고하여
12주차 강의에서 소개된 버퍼 오버플로우 실습 코드를 작성하고 실습하시오.
(헤더파일, next_tag 함수 및 TRUE/FALSE 값은 본인이 추가해야 함)

실습에 성공한 경우 소스코드 및 실행 캡처 화면만 Git에 업로드

본인의 실습 환경때문에 실습이 어려운 경우 6페이지 강의자료에서 소스코드 및 실행 커맨드
에 대한 내용을 한 줄씩 정리한 보고서로 대체 가능 (자유 양식, 2페이지 이상)

캡처 화면 예시

```
lartist@DESKTOP-C73L80G: /mnt/c/Users/bassist/Desktop/CLASS/CS/assignment/3$ gcc buffer1.c -o buffer1 -fno-stack-protector
buffer1.c: In function 'main':
buffer1.c:17:2: warning: implicit declaration of function 'gets'; did you mean 'fgets'? [-Wimplicit-function-declaration]
   17 |     gets(str2);
      |     ~~~~
      |     fgets
/usr/bin/ld: /tmp/cc1mqvr3.o: in function `main':
buffer1.c:(.text+0x52): warning: the `gets' function is dangerous and should not be used.
lartist@DESKTOP-C73L80G: /mnt/c/Users/bassist/Desktop/CLASS/CS/assignment/3$ ./buffer1
START
buffer1: str1(START), str2(START), valid(1)
lartist@DESKTOP-C73L80G: /mnt/c/Users/bassist/Desktop/CLASS/CS/assignment/3$ ./buffer1
EVILINPUTVALUE
buffer1: str1(TVALUE), str2(EVILINPUTVALUE), valid(0)
lartist@DESKTOP-C73L80G: /mnt/c/Users/bassist/Desktop/CLASS/CS/assignment/3$ ./buffer1
BADINPUTBADINPUT
buffer1: str1(BADINPUT), str2(BADINPUTBADINPUT), valid(1)
```

Windows10의 wsl을 활용한 실습

```
lartist@lartistui-MacBookAir practice % ./buffer1
warning: this program uses gets(), which is unsafe.
START
buffer1: str1(START), str2(START), valid(1)
lartist@lartistui-MacBookAir practice % ./buffer1
warning: this program uses gets(), which is unsafe.
EVILINPUTVALUE
buffer1: str1(TVALUE), str2(EVILINPUTVALUE), valid(0)
lartist@lartistui-MacBookAir practice % ./buffer1
warning: this program uses gets(), which is unsafe.
BADINPUTBADINPUT
buffer1: str1(BADINPUT), str2(BADINPUTBADINPUT), valid(1)
zsh: abort ./buffer1
```

mac에서 실습

참고사항

윈도우의 wsl(Windows Subsystem for Linux)를 활용하여 Ubuntu 설치가 가능함

1.

윈도우10의 wsl을 활용하여 Ubuntu 20.04.1 에서 gcc 9.3.0 으로 컴파일하는 경우
gcc 컴파일 시 옵션은 -fno-stack-protector (스택 오버플로우 경고 무시)

2.

macOS Catalina에서 clang 12.0.0 으로 컴파일하는 경우
경고 메시지만 뜨고 정상 실행