**REPORT**

**[어셈블리 실습 04]**

원, 폰트, 동전이(가) 표시된 사진

자동 생성된 설명

**과 목 : 시스템소프트웨어**

**담당교수 : 석문기 교수님**

**학 과 : 컴퓨터공학과**

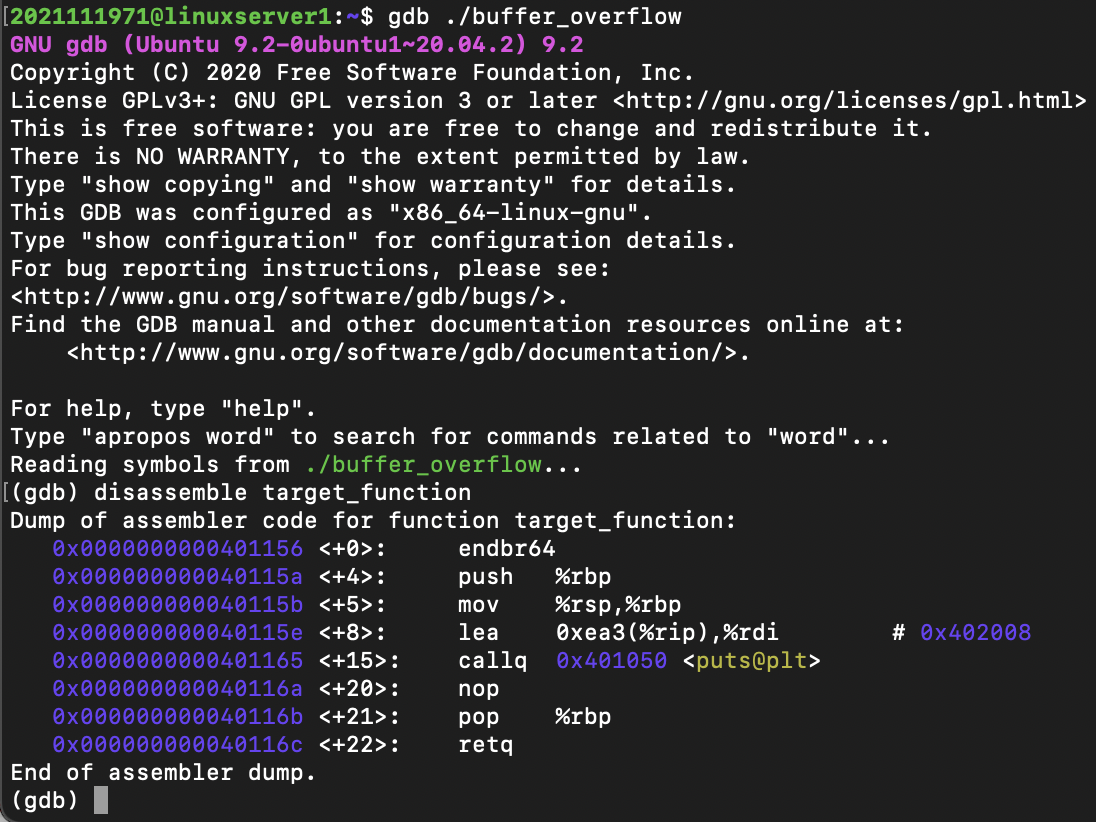
**학 번 : 2021111971**

**이 름 : 이재혁**

텍스트, 클립아트이(가) 표시된 사진

자동 생성된 설명

**1. target\_function 주소**

****

target\_function 시작주소 : 0x401156

**2. echo return address 확인**

텍스트, 스크린샷, 폰트이(가) 표시된 사진

자동 생성된 설명

x/16x $rsp 명령어로 스택 상단부의 명령어 주소를 조회합니다.

disassemble main 명령어로 echo함수 이후의 주소, 즉 echo의 반환 주소를 확인합니다.

callq 다음 주소는 0x004011ab입니다. 이 주소를 스택 상단부에서 찾아보면

echo함수의 반환주소는 0x7fffffffe2d8에 존재하는 것을 알 수 있습니다.

**3. Buffer Overflow 확인**

텍스트, 스크린샷, 폰트이(가) 표시된 사진

자동 생성된 설명

call 명령어 주소 : 0x00401185

|  |  |
| --- | --- |
| 텍스트, 스크린샷, 멀티미디어 소프트웨어, 소프트웨어이(가) 표시된 사진  자동 생성된 설명 | AAAAAAA 입력 후 rsp + 16주소에 0x41('A')가 7개 저장 된 것을 확인할 수 있습니다. |

python 스크립트 작성

텍스트, 폰트, 스크린샷, 그래픽이(가) 표시된 사진

자동 생성된 설명 서버 파이썬 버전 확인

텍스트, 스크린샷, 폰트이(가) 표시된 사진

자동 생성된 설명 exploit.py (타겟 함수 주소 반영)

텍스트, 스크린샷, 폰트, 라인이(가) 표시된 사진

자동 생성된 설명

텍스트, 스크린샷, 폰트, 그래픽이(가) 표시된 사진

자동 생성된 설명 exploit.py 실행 후 생성파일 확인

**실행결과**

텍스트, 스크린샷, 폰트이(가) 표시된 사진

자동 생성된 설명

exploit\_input파일을 입력으로 사용, target함수가 호출됩니다.