$15213, 20xx$년 가을
실습 2 : 이진 폭탄 해체하기
출시일: x월 x일, 마감일: x월 x일(수) 오후 xx시 xx분

Harry Bovik(bovik@cs.cmu.edu) 이 이 과제의 책임자입니다.

1 소개

사악한 닥터 이블이 우리 수업용 컴퓨터에 수많은 '이진 폭탄'을 설치했습니다. 이진 폭탄은 일련의 단계로 구성된 프로그램입니다. 각 단계는 사용자가 특정 문자열을 stdin에 입력하도록 요구합니다. 올바른 문자열을 입력하면 해당 단계가 해제되고 폭탄은 다음 단계로 진행됩니다. 그렇지 않으면 "B00M!!!"을 출력한 후 폭탄이 폭발하고 종료됩니다. 폭탄은 모든 단계가 해체되었을때 해체됩니다.

우리가 처리하기에는 폭탄이 너무 많아서 각 학생에게 폭탄을 해체할 수 있는 폭탄을 주고 있습니다. 여러분의 임무는 마감일 전에 폭탄을 해체하는 것입니다. 행운을 빌며 폭탄 제거반이 된 것을 환영합니다!

1단계: 해체할 폭탄을 가져가세요

웹 브라우저에 다음 주소를 입력해서 폭탄을 가져갈 수 있습니다.

http://$Bomblab: : SERVER_NAME : $Bomblab : :REQUESTD_PORT/

그러면 바이너리 폭탄 요청 양식이 표시되어 작성할 수 있습니다. 사용자 이름과 이메일 주소를 입력하고 제출 버튼을 누릅니다. 서버가 폭탄을 빌드하여 브라우저에 bombk.tar(여기서 k는 폭탄의 고유 번호)라는 이름의 tar 파일로 반환합니다.

tar 파일을 작업을 수행할 (보호된) 디렉터리에 저장합니다. 그런 다음 다음과 같은 명령을 실행합니다: tar −xvf bombk.tar. 이렇게 하면 다음 파일이 있는 ./bombk라는 디렉터리가 생성됩니다:

- README: 폭탄과 그 소유자를 식별합니다.
- bomb: 실행 가능한 바이너리 폭탄입니다.
- bomb.c: 폭탄의 main 함수와 닥터 이블의 친근한 인사말이 포함된 소스 파일.
- writeup. { pdf, ps } : 실습 설명서.

어떤 이유로 여러 개의 폭탄을 요청하더라도 문제가 되지 않습니다. 작업할 폭탄 하나를 선택하고 나머지는 삭제하면 됩니다.

Step 2: 폭탄을 해체하세요

이 실험실에서 여러분의 임무는 폭탄을 해체하는 것입니다. 수업용 컴퓨터중 하나에서 과제를 수행해야 합니다. 사실 닥터 이블은 정말 사악해서 폭탄을 다른 곳에서 작동시키면 항상 폭발한다는 소문이 있습니다. 폭탄에는 몇가지 다른 조작 방지 장치도 내장되어 있다고 합니다. 폭탄을 해체하는 데 도움이 되는 여러 도구를 사용할 수 있습니다. 힌트 섹션에서 몇 가지 팁과 아이디어를 확인하세요. 가장 좋은 방법은 gdb와 같은 디버거를 사용하여 역어셈블된 바이너리 파일을 살펴보는 것입니다.

폭탄이 폭발할 때마다 폭탄실험실 서버에 알림이 전송되며, 실습의 최종 점수에서 1/2점(최대 20점)을 잃게 됩니다. 따라서 폭탄을 폭발시키는것에는 책임이 따릅니다. 조심해야 합니다!

처음 네 단계는 각각 10점씩 입니다. 5단계와 6단계는 조금 더 어렵기 때문에 각각 15점입니다. 따라서 획득할 수 있는 최대 점수는 70점입니다.

단계가 진행될수록 해체하기가 점점 더 어려워지지만, 단계를 거치면서 쌓은 전문 지식이 이 어려움을 상쇄할 수 있습니다. 그러나 마지막 단계는 최고의 학생들도 어려워하므로 마지막 순간까지 미루지 마세요.

폭탄은 빈 입력 줄을 무시합니다. 예를 들어 명령행 인자를 사용하여 폭탄을 실행하면,

```
linux> ./bomb psol.txt
```

폭탄은 EOF(파일 끝)에 도달할 때까지 psol.txt의 입력 줄을 읽은 다음 stdin으로 전환합니다. 닥터 이블은 이미 해제한 단계에 대한 솔루션을 계속 다시 입력할 필요가 없도록 이 기능을 추가했습니다.

실수로 폭탄을 터뜨리지 않으려면 어셈블리 코드를 한 단계씩 진행하는 방법과 중단점을 설정하는 방법을 배워야 합니다. 또한 레지스터와 메모리 상태를 모두 검사하는 방법도 배워야 합니다.

메모리 상태를 검사하는 방법도 배워야 합니다. 실습을 하면 좋은 점 중 하나는 디버거를 매우 능숙하게 사용하는법을 알게 된다는 것입니다. 이는 여러분의 커리어에 큰 도움이 될 중요한 기술입니다.

2 구성

이것은 개별 프로젝트입니다. 모든 제출은 전자식입니다. 설명 및 수정 사항은 수업 게시판에 게시됩니다.

3 유인물 지침

명시적인 핸드인이 없습니다. 폭탄은 작업하는 동안 진행 상황을 강사에게 자동으로 알려줍니다. 다음 링크에서 수업 점수판을 확인하여 진행 상황을 추적할 수 있습니다:

http://$Bomblab: : SERVER_NAME: $Bomblab : :REQUESTD_PORT/scoreboard

이 웹 페이지는 각 폭탄의 진행 상황을 보여주기 위해 지속적으로 업데이트됩니다.

4 힌트 (제발 읽으세요!)

폭탄을 해체하는 방법에는 여러 가지가 있습니다. 프로그램을 실행하지 않고도 폭탄을 자세히 살펴보고 정확히 어떤 기능을 하는지 파악할 수 있습니다. 이것은 유용한 기술이지만 항상 쉬운 것은 아닙니다. 디버거에서 폭탄을 실행하여 단계별로 작업을 관찰하고 이 정보를 사용하여 폭탄을 해체할 수도 있습니다. 이것이 아마도 가장 빠른 방법일 것입니다.

한 가지 부탁드리자면, 무차별 대입을 사용하지 마세요! 올바른 키를 찾기 위해 가능한 모든 키를 시도하는 프로그램을 작성할 수도 있습니다. 하지만 이는 여러 가지 이유로 좋지 않습니다:

- 틀릴 때마다 1/2점(최대 20점)을 잃고 폭탄이 폭발합니다.
- 틀릴 때마다 폭탄실험 서버로 메시지가 전송됩니다. 이러한 메시지로 인해 네트워크가 매우 빠르게 포화 상태가 되어 시스템 관리자가 사용자의 컴퓨터 액세스 권한을 취소할 수 있습니다.
- 우리는 문자열의 길이가 얼마나 되는지, 어떤 문자가 들어 있는지 알려주지 않았습니다. 문자열의 길이가 모두 80자 미만이고 문자만 포함되어 있다는 (잘못된) 가정을 하더라도 각 단계마다 26^{80}의 추측을 하게 됩니다. 이렇게 하면 실행 시간이 매우 오래 걸리고 과제 마감일 전에 답을 얻을 수 없습니다.

프로그램이 작동하는 방식과 작동하지 않을 때 무엇이 문제인지 파악하는 데 도움이 되는 많은 도구가 있습니다. 다음은 폭탄을 분석하는 데 유용할 수 있는 몇 가지 도구 목록과 사용 방법에 대한 힌트입니다.

gdb

GNU 디버거는 거의 모든 플랫폼에서 사용할 수 있는 명령줄 디버거 도구입니다. 프로그램을 한 줄씩 추적하고, 메모리와 레지스터를 검사하고, 소스 코드와 어셈블리 코드를 모두 살펴보고(대부분의 폭탄의 소스 코드는 제공하지 않습니다), 중단점을 설정하고, 메모리 감시점을 설정하고, 스크립트를 작성할 수 있습니다.

CS:APP 웹 사이트

http://csapp.cs.cmu.edu/public/students.html

에는 인쇄하여 참고 자료로 사용할 수 있는 매우 편리한 한 페이지짜리 gdb 요약이 있습니다. 다음은 gdb를 사용하기 위한 몇 가지 다른 팁입니다.

잘못된 입력값을 넣을 때마다 폭탄이 터지는 것을 방지하려면 중단점을 설정하는 방법을 배워야 합니다.

온라인 설명서를 보려면 gdb 명령 프롬프트에 "help"를 입력하거나, 유닉스 프롬프트에 "man gdb" 또는 "info gdb"를 입력합니다. 어떤 사람들은 emacs에서 gdb-mode로 gdb를 실행하기도 합니다.

objdump - t

이 명령은 폭탄의 심볼 테이블을 출력합니다. 심볼 테이블에는 폭탄에 있는 모든 함수와 전역 변수의 이름, 폭탄이 호출하는 모든 함수의 이름과 주소가 포함됩니다. 함수 이름을 보고 무언가를 배울 수 있습니다!

objdump - d

폭탄의 모든 코드를 분해하는 데 사용합니다. 개별 함수만 살펴볼 수도 있습니다. 어셈블러 코드를 읽으면 폭탄이 어떻게 작동하는지 알 수 있습니다.

objdump - d는 많은 정보를 제공하지만, 모든 것을 알려주지는 않습니다. 시스템 수준 함수에 대한 호출은 암호화된 형태로 표시됩니다. 예를 들어, sscanf에 대한 호출은 다음과 같이 표시될 수 있습니다:

8048C36: E8 99 FC FF FF 호출 80488D4 <_INIT+0X1A0>

호출이 sscanf에 대한 호출인지 확인하려면 gdb 내에서 역어셈블해야 합니다.

strings

이 유틸리티는 폭탄에 인쇄 가능한 문자열을 표시합니다.

특정 도구를 찾고 계신가요? 문서는 어때요? apropos, man, info 명령은 여러분의 친구라는 것을 잊지 마세요. 특히 man ascii가 유용할 수 있습니다. info gas는 GNU 어셈블러에 대해 알고 싶었던 것보다 더 많은 것을 알려줄 것입니다. 또한 인터넷도 정보의 보고가 될 수 있습니다. 막히는 부분이 있으면 언제든지 강사에게 도움을 요청하세요.