HW #1

Finding and Fixing Program Vulnerabilities

Computer Security

School of CSEE

Requirement

- 이 숙제에서는 ‘animal.c’ 의 취약점을 분석하고, 가능한 공격 방법을 제시한 후 실제 공격 과정에 대해 설명해야 합니다. 또한 취약점을 극복할 수 있는 방안을 제시하고, 그에 따라 수정된 animal_adv.c를 제출하세요.

- animal.c가 컴파일하고 실행되는 환경은 아래와 같습니다.

```
[10/16/24]seed@VM:~/hw1$ sudo sysctl -w kernel.randomize_va_space=0
kernel.randomize_va_space = 0
[10/16/24]seed@VM:~/hw1$ gcc animal.c -o animal -g
[10/16/24]seed@VM:~/hw1$ sudo chown root animal
[10/16/24]seed@VM:~/hw1$ sudo chmod 4755 animal
[10/16/24]seed@VM:~/hw1$ ./animal db.txt
[DOG] Buddy says: Woof Woof!
[CAT] Whiskers says: Meow!
[COW] Daisy says: Moo!
[DOG] Max says: Woof Woof!
[CAT] Tiger says: Meow!
```

Requirement

- 취약점 공격을 위해 animal.c 소스 코드를 수정할 수는 없습니다. 그러나 공격을 위해 필요한 다양한 exploit은 직접 작성하여 사용할 수 있습니다.
- 취약점 공격 과정은 제3자가 쉽게 재현 가능하도록 화면 캡처 및 설명을 통해 상세하게 제시되어야 합니다.
- Intel CPU 사용자의 경우 Seed VM에서 실행되어야 하며, Arm CPU 사용자는 Arm 버전 Ubuntu 22.04에서 실행 가능해야 합니다.
- animal.c 의 취약점을 해결한 소스 코드는 animal_adv.c 로 이름을 변경하여 제출하세요.
  - animal_adv.c 역시 animal.c 와 동일한 옵션으로만 컴파일 해야 합니다.

Requirement

- 보고서에는 취약점 분석 및 공격 방법, 취약점 해결 방안 등에 관한 내용이 포함되어야 하며, 평가자가 쉽게 이해할 수 있도록 잘 정리되어야 합니다.
  - 보고서는 word로 작성 후 pdf로 변환하여 제출하세요.

- 제출하는 파일들은 아래와 같은 형태로 ZIP으로 압축하여 LMS에 제출하세요.
  - 파일 이름: hw01_student id.zip (ex: hw01_20400022.zip)
  - ZIP 파일 안에 포함되어야 하는 파일들: 보고서 pdf, animal.c 및 공격에 필요한 모든 파일, animal_adv.c 등

- ChatGPT 등 AI Tool에 대해 직접적인 사용이 적발될 경우 0점 처리됩니다.

- Due date: 11:59pm, 10/25 (Fri)