Assignment 2

Buflab

Computer Security Lab

Name: Jaewon Hur

Email: hurjaewon@snu.ac.kr

Buflab Goal

- Understand IA-32 calling conventions of programs.

- Understand how to exploit security vulnerabilities.

Buflab Overview

- You need to enter the appropriate string by analyzing the bufbomb binary.
  - We don’t have penalty in this lab.

- bufbomb has 6 phases.

- Each phase expects you to type a particular string on stdin or file.

Downloading Your Bufbomb

- http://kayle.snu.ac.kr:18213
  - Type this into your address bar.

How to copy buflab-handout.tar into your container

- copy host file to the container

```
> docker cp buflab-handout.tar <CONTAINER_NAME>:<DESTINATION_PATH>
```

- In docker container, extract the bufbomb

```
(in docker) > tar xvf buflab-handout.tar
```

How to use buflab-handout

- buflab-handout contains 3 files
  - **bufbomb**: binary which you have to exploit.
  - **hex2raw**: convert hex representation of bytes into raw byte string
  - **makecookie**: generate cookie from your student number

1. Use your student number to generate cookie.

```
(in docker) > ./makecookie 2017-21214
0x30d0404d
```

How to use buflab-handout

2. Use your student number throughout exploiting bufbomb.

```
> cat <your solution>.txt | ./hex2raw | ./bufbomb -u 2017-21214
Userid: 2017-21214
Cookie: 0x30d0404d
Type string: Smoke!: you called smoke()
VALID
NICE JOB!
```

3. If you succeed, submit to the server

```
> cat <your solution>.txt | ./hex2raw | ./bufbomb -u 2017-21214 -s
```

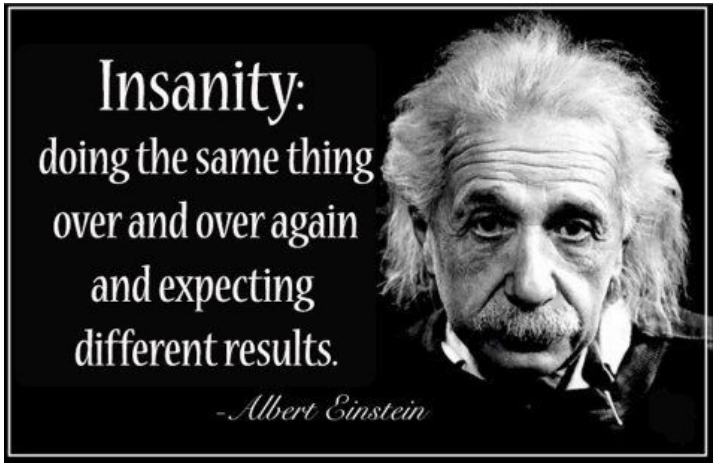
Useful Commands

- **gdb**

- objdump
  - -d: disassembles the binary
  - -t: print out the symbol of the binary

Tips

- Please read the **buflab-readme.pdf** carefully.
- Don’t forget to set up the breakpoints!
- If you have any questions, feel free to ask TAs via eTL.



Evaluation

- Total Score : 75 pts
  - Phase 0 - 1 : 10 pts
  - Phase 2 : 15 pts
  - Phase 3 : 20 pts
  - Phase 4 - 5 : 10 pts
- Due: 2022-10-10 (Monday) 23:59
- You can check your score at http://kayle.snu.ac.kr:18213/scoreboard

Buflab Demo