

CS201 – Homework 4 Overview

RAOUL RIVAS

PORTLAND STATE UNIVERSITY

A solid green horizontal bar spanning the width of the slide at the bottom.

Goals

- 1) Improve understanding on how buffer overflow works
- 2) Further practice debugging with gdb in both assembly and source mode

Development Setup

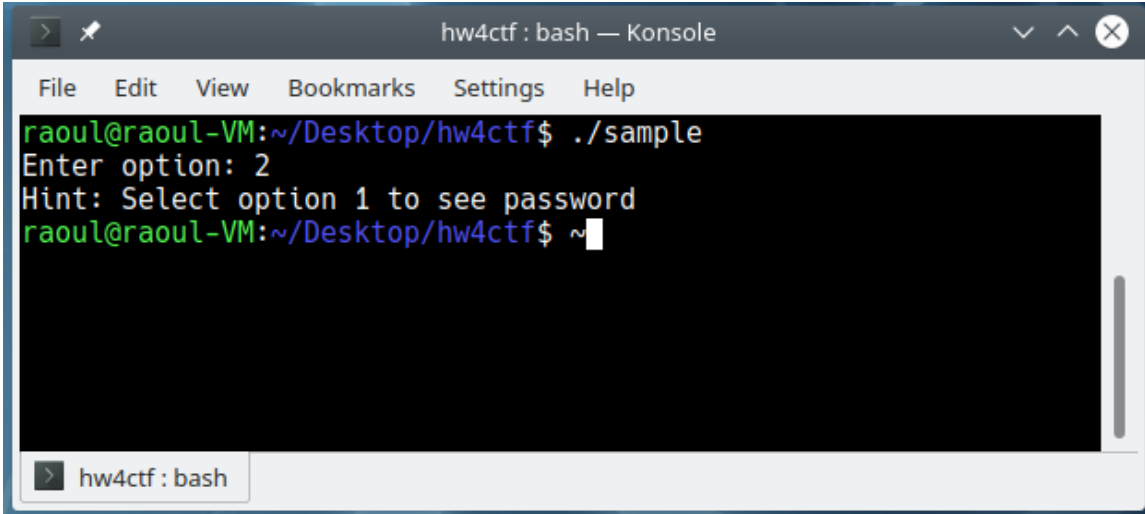
- **Individually!**
- Work in the CS Linux lab
 - `linuxlab.cs.pdx.edu`
 - FAB 88-09 and 88-10
- Use gdb in assembly and source mode
 - Executable files have been provided
 - Some problems include parts of the source files but not enough to recompile the executable
- Answer questions in quiz provided through D2L

Overview

- Assignment is composed of 2 problems
- Objective is to obtain the password in each problem
- For each problem:
 - Use the debugger in assembly or source mode to obtain details about the structure of the program
 - Use the password printed by the program as answer in D2L HW4 Quiz

Sample Program

- After running the program we are asked for input
- Selecting option 2 does not print the password



The screenshot shows a terminal window titled "hw4ctf : bash — Konsole". The terminal has a menu bar with "File", "Edit", "View", "Bookmarks", "Settings", and "Help". The prompt is "raoul@raoul-VM:~/Desktop/hw4ctf\$". The user has entered the command "./sample". The program output is "Enter option: 2" followed by "Hint: Select option 1 to see password". The prompt is now "raoul@raoul-VM:~/Desktop/hw4ctf\$ ~" with a cursor. A tab at the bottom of the window is labeled "hw4ctf : bash".

```
raoul@raoul-VM:~/Desktop/hw4ctf$ ./sample
Enter option: 2
Hint: Select option 1 to see password
raoul@raoul-VM:~/Desktop/hw4ctf$ ~
```

Goal is to obtain the password!

Sample Problem

How do we obtain the password?

- Read the source
- Inspect the execution with the debugger in assembly
- Some exercises might also provide symbols so you can inspect the execution in source mode
- In the sample exercise selecting Option 1 will print the password!

The screenshot shows a GDB console window titled "hw4ctf: gdb — Konsole". The window has a menu bar with "File", "Edit", "View", "Bookmarks", "Settings", and "Help". The main content area is divided into two panes. The top pane, titled "Register group: general", displays the following register values:

Register	Value
rax	0x2 2
rbx	0x0 0
rcx	0x1999999999999999 1844674407370955161
rdx	0x0 0
rsi	0x7fffffffddde6 140737488346598
rdi	0x2 2
rbp	0x7fffffffdddc0 0x7fffffffdddc0
rsp	0x7fffffffddb0 0x7fffffffddb0
r8	0x7fffffffdde7 140737488346599

The bottom pane shows the source code of a function named "sample". The code is as follows:

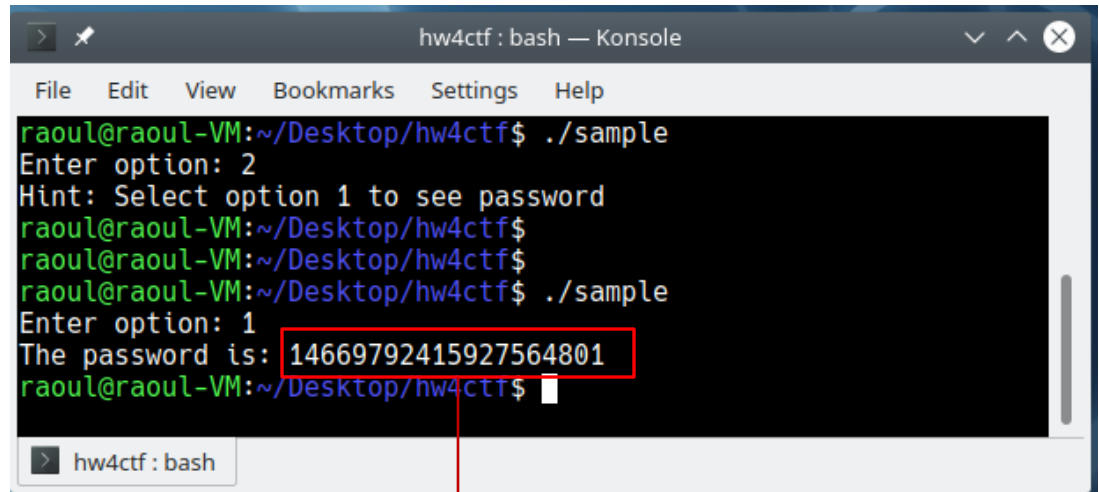
```
10 void sample(long value)
11 {
12     if (value == 1)
13     {
14         getpassword();
15     }
16     else
17     {
18         printf("Hint: Select option 1 to see password\n");
19     }
20 }
```

The GDB prompt shows the current state: "native process 16826 In: sample L12 PC: 0x5555555548cb". Below the source code, the GDB command history is visible:

```
(gdb) break sample
Breakpoint 1 at 0x8cb: file sample.c, line 12.
(gdb) run
Starting program: /home/raoul/Desktop/hw4ctf/sample
Breakpoint 1, sample (value=2) at sample.c:12
(gdb) layout src
```

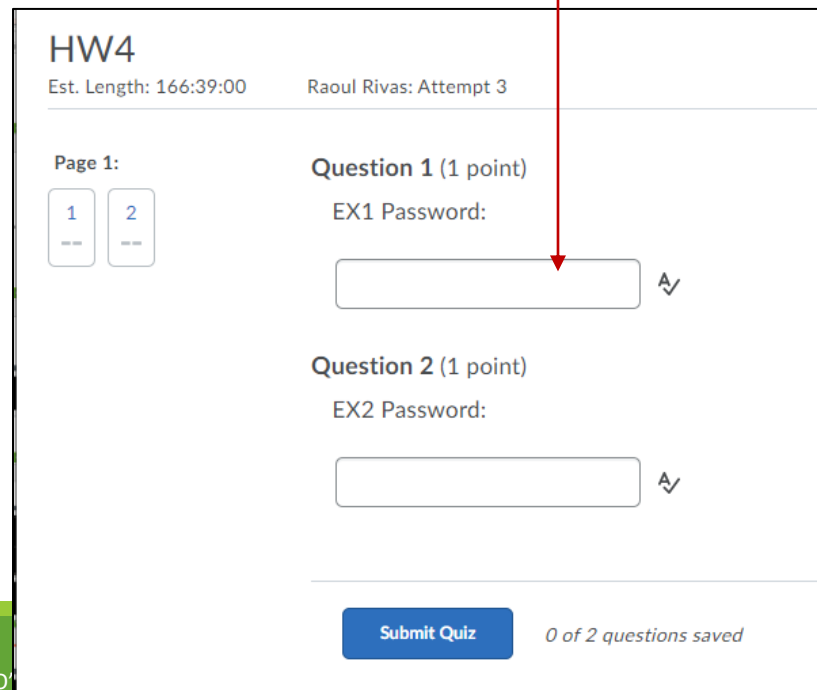
Sample Problem

- Use the password as answer in D2L HW4 Quiz
- Quizzes are located under Activities -> Quizzes
- You can try unlimited number of times



A terminal window titled 'hw4ctf : bash — Konsole' showing a series of commands and outputs. The user runs './sample', which prompts 'Enter option: 2'. A hint is shown: 'Hint: Select option 1 to see password'. The user then runs './sample' again, prompts 'Enter option: 1', and receives the output 'The password is: 14669792415927564801'. The password is highlighted with a red box. A red arrow points from this box down to the first input field in the quiz interface below.

```
raoul@raoul-VM:~/Desktop/hw4ctf$ ./sample
Enter option: 2
Hint: Select option 1 to see password
raoul@raoul-VM:~/Desktop/hw4ctf$
raoul@raoul-VM:~/Desktop/hw4ctf$
raoul@raoul-VM:~/Desktop/hw4ctf$ ./sample
Enter option: 1
The password is: 14669792415927564801
raoul@raoul-VM:~/Desktop/hw4ctf$
```



The image shows a quiz interface for 'HW4'. At the top, it says 'Est. Length: 166:39:00' and 'Raoul Rivas: Attempt 3'. Below this, 'Page 1:' is indicated with two buttons labeled '1' and '2'. The first question, 'Question 1 (1 point)', asks for the 'EX1 Password:'. A red arrow from the terminal above points to the input field for this question. Below it is 'Question 2 (1 point)' asking for the 'EX2 Password:'. At the bottom, there is a 'Submit Quiz' button and a status '0 of 2 questions saved'.