

15213 - Recitation 4 - Attack Lab

September 20th, 2024

To download the activity, enter into a Shark machine:

```
$ wget https://www.cs.cmu.edu/~213/activities/rec5.tar
$ tar xvf rec5.tar
$ cd rec5
$ gdb activity
```

Activity 1

The goal of this activity is to input a string that causes the program to call `win(0x15213)`, and thereby win a cookie¹. Work with your group to fill in the stack diagram, and discuss:

1. Where is **long** before stored on the stack? What about **long** after?
2. How many bytes can `Gets()` copy before overwriting something?
3. If the user types "12345678\n", what will the resulting stack look like? (Fill in the stack diagram on the back.) What will the corresponding value read from `%rdx` be?
4. How can you use GDB to check if your buffer overflow worked as intended?

Activity 2

We've upped the stakes! Can you figure out how to call `win(0x18213)` for two cookies?

1. Which lines of assembly correspond to `win(0x15213)` and `win(0x18213)`?
2. Which value will the `retq` instruction read off of the stack? Can it be overwritten?

Activity 3

If you finished the other activities early, see if you can manage to call `win(0x18613)`!

1. Note the suspiciously named function `gadget1`. Does it obey calling conventions by preserving the stack pointer when it returns? What value will it place into `%rdi`?

¹Actual availability of cookies is neither guaranteed or implied. However, there are always plenty of [stack cookies](#) available for you to choose from!

