Overview:

Buffer overflow is defined as the condition in which a program attempts to write data beyond the boundary of a buffer. This vulnerability can be used by a malicious user to alter the flow control of the program, leading to the execution of malicious code. The objective of this lab is for students to gain practical insights into this type of vulnerability, and learn how to exploit the vulnerability in attacks.

Setup:

```
$ cd buffer-overflow-exercise/
$ make
```

Task:

1. Find out buffer start address
2. Find the number of bytes needed to start overwriting the return address

Hint:

1. Use command: `python -c "print('A'*10)"` to print 10 As
2. Locate the special character “A” in stack memory to find the buffer start address

You need to submit a detailed lab report in PDF, with screenshots, to describe what you have done for each task.