Buffer Overflow-Part A

As discussed in class, buffer overflow is a widely used technique, for instance in viruses and worms, to exploit systems. The overflow of a buffer can overwrite return pointers on the stack, and if the overwritten return pointer is carefully selected it can trigger the execution of code that the intruder can use to exploit the system at hand.

Here are some references on buffer overflow that we recommend:

- [http://insecure.org/stf/smashstack.html](http://insecure.org/stf/smashstack.html)
- [http://www.securiteam.com/securityreviews/5OP0B006UQ.html](http://www.securiteam.com/securityreviews/5OP0B006UQ.html)

Your assignment:

You need to exploit the following program that takes in a serial number. Your task is to make the program output the "serial is correct" message without having to enter a valid serial number.

```c
#include <stdio.h>
#include <string.h>

main() {
    char in[10];
    scanf("%s", in);
    if (!strncmp(in, "S123n456", 8))
    {
        printf("Serial number is correct \n");
    }
}
```
Submission instructions (For each part)

- Detailed Log of your attack describing all the commands used as well as any intermediate values found.
- Screenshots that show you have succeeded.
- Use ’script’ to record your session. Submit your files via Carmen all at once.