SECURE SYSTEMS ENGINEERING (CS6570), IIT MADRAS

Assignment 4

Remote Format String Attack.

This is a remote attack to be done in-class in groups of atmost two.

Austin Powers is a determined and hardworking hacker. His best friend is gdb. However sometimes gdb may not be very helpful, in which case he would need to spend considerable amounts of time for trial and error before they succeed. His second best friend in this case is python.

In this mission, he is to hack into a remote server that requires a valid username and password to login. The username is 12345 and the password is exactly 30 bytes long and the password is alphanumeric.

Mr. Powers has figured out that there is a format string vulnerability in the server program that allows him to read arbitrary memory. Help Mr. Powers find the password.

To run the client:

```
$ gcc client.c -o client
$ ./client <IP address> <Port>
```

The IP address and port number will be provided in class.

When done, please upload the following to moodle.

1. Python script that will scrape the server's stack.
2. Script that would search the stack looking for potential passwords.
3. The password
4. Screen shot of successful log in

Happy Hacking !!!