CS6570 : Secure Systems Engineering
Lab 3 : Format String Vulnerability

Problem 1 (Log in if you can) : 40 points

A security-check program runs at the entrance of SSB-420, which asks for a password and allows entry into the lab only if the user provides the correct password. All the authorized members of the lab know the password (except a few who are crediting the course :)). You want to enter the lab but don't know the password and the lab members won't give you the password. So, you decide to credit the Secure Systems Engineering course to learn some hacking. Based on what you learned in class, you have already figured out that there is a format string vulnerability in the program. You also overheard some of the lab members talking about the password and got a hint that the password is alphanumeric and is exactly 30 bytes long. Now your job is to exploit this vulnerability, leak the password, and use the password to successfully log in.

You can run the security-check program using the following command:

```
ncat 10.21.235.155 1023
```

Problem 2 (Overwrite arbitrary memory) : 60 points

You are provided with an executable vulnerable to format string attacks. The code contains a variable called flag which is initialized to zero. Your job is to exploit the format string vulnerability in the code to overwrite the value of the flag with a specific value such that the statement *"The system is compromised"* gets printed.
Note: You can only use format string vulnerability to overwrite the value of the flag, using other approaches will not yield any marks.

What you need to submit:

1. Report in PDF format explaining your approach for both problems.
2. Python script and exploit string used in both problems.
3. Password found for Problem 1.
4. Screenshot of successful login for Problem 1.
5. Screenshot of the required statement being printed for Problem 2.

Note:

1. All the files should be submitted in a zipped folder through Microsoft Teams.
2. The schedule for viva will be communicated through Teams.

Happy Hacking :)