Secure Systems Engineering (CS6570)

Lab-1

For this assignment we expect the following from each team :

- A single report that describes your approach for **both parts** of the assignment (PDF format)
  - The report should contain a snapshot of the stack for both the binaries while they are executing (this can be a screenshot of a debugger like gdb or you can illustrate it) with the addresses being visible.
  - Highlight why the binaries could be exploited, what can be done to make them secure?
- Exploit string for each binary (**tested on the provided VM**)
- Honesty

Lab1_1 (20 Marks)

Teams are provided a binary (lab1_1) and the corresponding source (lab1_2.c) file

- Teams can view the source file and identify vulnerabilities in the program.
- Teams need to come up with an exploit string input such that they are able to call the function `exploit()` present in the program.

Expected Output

```
root@osboxes:/Lab1# ./lab1_1 $(cat exploit_string)
Welcome group <something>
Exploit succesfull...
```

Lab1_2 (50 Marks)

Teams are provided a binary (lab1_2) and the corresponding source (lab1_2.c) file

- Teams can view the source file and identify vulnerabilities in the program.
- Teams need to come up with an exploit string input such that they are able to spawn a shell (the binary calls `/bin/sh`).
- In the report highlight any important addresses (like the base address of libc) you find or use.

Expected Output

```
root@osboxes:/Lab1# ./lab1_2 $(cat exploit_string)
exploit_string    lab1_2    lab1_2.c
Welcome group <something>
# whoami
root
#
```

Viva (30 Marks)

- Schedule will be communicated after assignment deadline.